IX

АПИНО

ICAIT

9TH INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2020

IX МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ
И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ
«АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ
В НАУКЕ И ОБРАЗОВАНИИ»

СБОРНИК НАУЧНЫХ СТАТЕЙ

26–27 ФЕВРАЛЯ 2020 ГОДА

APINO.SPBGUT.RU

СПбГУТ))) 90 ЛЕТ

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

АПИНО

ICAIT

9TH INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2020

IX МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ «АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ В НАУКЕ И ОБРАЗОВАНИИ»

Научные направления:

– Радиотехнологии в связи
– Инфокоммуникационные сети и системы
– Информационные системы и технологии
– Теоретические основы радиоэлектроники
– Цифровая экономика и управление в связи
– Гуманитарные проблемы информационного пространства
– Сети связи специального назначения

Генеральный партнёр:

технологии бесконечности ®
КОМПАНИЯ «Т8»

ООО «Т8»

Партнёры:

Ростелеком

ПАО «Ростелеком»

МегаФон

ПАО «МегаФон»

SERTEK

ООО «Сертек»

АРГУС НТЦ

ООО «НТЦ АРГУС»

специальные системы ФОТОНИКА

ООО «Специальные Системы. Фотоника»

Информационные партнёры:

ТУЗС

журнал
«Труды учебных заведений связи»

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ ИНФОРМАЦИЯ КОСМОС

журнал
«Информация и космос»

Информационная поддержка:

www.iit.sut.ru

электронный журнал «Информационные технологии и телекоммуникации»

26–27 ФЕВРАЛЯ 2020

APINO.SPBGUT.RU

УДК 001:061.3(082)
ББК 72 А43

Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С. В. Бачевского; сост. А. Г. Владыко, Е. А. Аникевич. СПб. : СПбГУТ, 2020. Т. 2. 748 с.

ПРОГРАММНЫЙ КОМИТЕТ

Председатель

Бачевский С. В., доктор технических наук, профессор, ректор СПбГУТ (Россия)

Заместитель председателя

Шестаков А. В., доктор технических наук, ст. науч. сотрудник, проректор по научной работе СПбГУТ (Россия)

Ответственный секретарь

Владыко А. Г., кандидат технических наук, member IEEE, директор научно-исследовательского института технологий связи СПбГУТ (Россия)

Члены программного комитета

Yevgeni Koucheryavy, professor, Ph. D., Senior member IEEE, Department of Electronics and Communication Engineering Tampere University of Technology (Finland)
Tina Tsou, Liaison rapporteur Huawei Technologies, editor positions in ITU-T, IETF and ETSI, Huawei (China)
Matthias Schnöll, professor, Ph. D., Fachbereich Elektro-technik, Anhalt University of Applied Sciences (Germany)
Hyeong Ho Lee, Ph. D. in Electrical Engineering, Vice President of IEEK (Institute of Electronics Engineers of Korea), ETRI (Korea)
Edison Pignaton de Freitas, rofessor adjunto, Ph. D., Federal University of Rio Grande do Sul (Brasil)
Andrej Kos, professor, Ph. D., University of Ljubljana (Slovenia)
Janusz Pieczerak, M. Sc., Orange Labs (Poland)
Сеилов Ш. Ж., доктор технических наук, президент Казахской Академии Инфокоммуникации (Казахстан)
Кирик Д. И., кандидат технических наук, доцент, декан факультета радиотехнологий связи СПбГУТ
Бузюков Л. Б., кандидат технических наук, профессор, декан факультета инфокоммуникационных сетей и систем СПбГУТ
Зикратов И. А., доктор технических наук, профессор, декан факультета информационных систем и технологий СПбГУТ
Колгатин С. Н., доктор технических наук, профессор, декан факультета фундаментальной подготовки СПбГУТ
Сотников А. Д., доктор технических наук, доцент, декан факультета цифровой экономики, управления и бизнес-информатики СПбГУТ
Шутман Д. В., кандидат политических наук, доцент, декан гуманитарного факультета СПбГУТ
Гирш В. А., полковник, начальник военного учебного центра СПбГУТ

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ СПбГУТ, Россия

Председатель

Машков Г. М., доктор технических наук, профессор, первый проректор–проректор по учебной работе

Сопредседатель

Алексеенко И. А., кандидат педагогических наук, проректор по воспитательной работе и связям с общественностью СПбГУТ (Россия)

Ответственный секретарь

Аникевич Е. А., кандидат технических наук, начальник отдела организации научно-исследовательской работы и интеллектуальной собственности

Члены организационного комитета

Ивасишин С. И., директор департамента организации и качества образовательной деятельности
Петров Н. М., директор административно-хозяйственного департамента
Чистова Н. А., директор финансово-правового департамента
Елагин В. С., кандидат технических наук, начальник управления организации научной работы и подготовки научных кадров
Казаков Д. Б., начальник управления информатизации – заместитель проректора по информатизации
Григорян Г. Т., начальник управления маркетинга и рекламы
Зыкова Н. В., начальник управления информационно-образовательных ресурсов
Карташова Н. И., главный специалист отдела организации научно-исследовательской работы и интеллектуальной собственности

В научных статьях участников конференции исследуются состояние и перспективы развития мирового и отечественного уровня IT и телекоммуникаций. Предлагаются методы и модели совершенствования научно-методического обеспечения отрасли связи и массовых коммуникаций.

Предназначено научным работникам, аспирантам и студентам старших курсов телекоммуникационных и политехнических вузов, инженерно-техническому персоналу и специалистам отрасли связи.

Научное издание
Литературное редактирование,
корректура Е. А. Аникевич
Оформление Г. И. Юрьев
Верстка Е. М. Аникевич
Подписано в печать 01.09.2020.
Вышло в свет 30.09.2020. Формат 60×90 1/8.
Уст. печ. л. 46,75. Заказ № 063-ИТТ-2020.
пр. Большевиков, д. 22, корп. 1.
Россия, Санкт-Петербург, 193232

ISBN 978-5-89160-198-7

© СПбГУТ, 2020

СОДЕРЖАНИЕ

Информационные системы и технологии	**5**	Information Technology and Telecommunications
Цифровая экономика, управление и бизнес-информатика	**601**	Digital Economy, Governance and Business Informatics
Аннотации	**687**	Annotations
Авторы статей	**723**	Authors of Articles
Авторский указатель	**746**	The Author’s Index

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

UDC 02.026 (681.3)
SCSTI 20.53.01

QUALITY ANALYSIS OF ELECTRONIC LIBRARIES AS ELEMENTS OF A TELECOMMUNICATION MEDIA

E. S. Kryukova, I. B. Parashchuk, N. V. Mikhaylichenko

Military Telecommunications Academy

The questions of the analysis of the quality of electronic libraries as the basic elements of the modern educational information and telecommunication infrastructure (media) are considered. The advantages, functions and tasks of electronic libraries are analyzed. The study was conducted to identify and analyze their significant properties. The analysis of approaches to assessing the quality of electronic libraries is carried out, the potential possibilities of quality analysis using well-known principles of the theory of interval means are considered.

electronic library, quality, indicator, infrastructure, attribute, document, information resource.

Modern studies for the analysis and construction of educational information and telecommunications infrastructure (media) show that the importance of electronic libraries (EL) for the information society is growing. This is confirmed by the fact that the problem of creating EL rises to the level of state policy not only in individual High Schools (HSs) and organizations, but also in educational and research organizations of various ministries and departments of the Russian Federation [1, 2, 3].

Electronic (digital) libraries today occupy a special place among modern and promising information systems deployed in the interests of the educational system of the Russian Federation as part of the «Electronic High School» project [4]. An electronic library is a distributed information system that allows you to reliably store and efficiently use heterogeneous collections of electronic documents through common, departmental (and if necessary closed) data networks in a form convenient for the end user [2, 3].

The main objectives of the electronic library is the integration of information resources and effective navigation in them. Integration of information resources

is understood as their integration in order to use (using convenient and unified interfaces) various information while preserving its properties, presentation features and user-specific manipulation capabilities [2, 5].

Common tasks of the electronic library:

– an electronic library should be a collection of electronic resources organized on the basis of the library on the basis of automated library technologies, including the formation, processing, systematization, storage and access to electronic documents and databases;

– increasing the availability of books of the educational process in HSs (universities);

– improving the efficiency and quality of library-information services for users;

– introduction of modern information technologies in the practice of library-information services;

– ensuring the efficiency of library-information services;

– providing users with qualitatively new opportunities for working with large volumes of information;

– increasing the availability of books and other documents and long-term storage of electronic documents.

Like any holistic fund, EL contributes to the following basic functions:

– information function, aimed at satisfying the need for information;

– educational function, implemented, inter alia, through the popularization of electronic documents related to history and culture;

– a research function, focused on promoting in-depth study of a topic (subject) by specialists;

– educational function, within the framework of which support is provided for basic and additional education by providing multimedia educational material and the necessary literature;

– help function that allows you to get reliable information reflected in documents of a certain type.

The advantages of electronic libraries (in comparison with traditional libraries):

– the user receives information regardless of time and location, his or library;

– significantly increases the efficiency of providing users with the necessary literature, documents and data;

– the user has the ability to access diverse electronic resources;

– facilitated the implementation of new forms of library and information services to users;

– documents available in libraries in a limited number become available to a significantly larger number of users;

– work with electronic documents may go beyond reading text or viewing an image (combining, adding, editing materials are available);

– a quick and high-quality search for certain fragments of a document, its semantic analysis, other types of software processing, and saving space are possible compared to a conventional library [2, 5].

In addition, an important advantage of electronic libraries is the fact that they allow the widespread introduction of the latest technologies, that provide access to a large amount of information resources at a qualitatively new level; their deployment does not require significant time and cost.

It is assumed that the EL is a telecommunication and information center, providing quick and controlled access to information, professional databases, information reference and search systems, as well as other information resources.

Along with the emergence, development, and active implementation of complex automated information systems, the elements of which are hardware (technical) tools, software, and maintenance personnel, the question arose of developing new approaches to assessing their quality.

The existing difficulties in the implementation of projects, the difficulties in solving the problem of multi-criteria analysis of the quality of electronic libraries are due, inter alia, to the lack of universal methods that take into account a number of properties and features of electronic libraries, the incompleteness and heterogeneity of the initial information about the quality of hardware and software platforms for systems of this class.

Therefore, the development of a modern, rigorous mathematical approach that allows you to combine the incoming and available information to obtain common interval quality assessments of the entire system, the task of creating a new, convenient methodological tool for decision support on the construction and management of EL – methods of multi-criteria analysis (assessment) of the quality of electronic libraries of educational and research organizations is relevant [6, 7].

Most modern EL-systems of this class are dynamic systems. This is due to the fact that the functioning parameters of hardware, software and officials, as components of EL, are constantly changing. In other words, even with the necessary amount of statistical data on the values of quality indicators (QIs) of elements and processes implemented by EL, the stability of these values in time is rarely observed.

These indicators of quality of EL include numerical values of parameters, for example, characterizing efficiency (timeliness) – average access times of authorized users to the electronic resource of EL, average search times of requested content, or parameters, characterizing reliability – average operating time of EL to failure [7].

The signs of the analysis (assessment) of EL quality can be considered: the object of analysis; assessment criteria; type of rating scale; nature of assess-

ment; assessment methods; type of EL quality ratings obtained; the time dependence of the EL quality assessment, as well as the type of a priori uncertainty of the observational data, which determines the choice of the method (method) for analyzing the quality of the electronic library.

According to the object of the analysis (assessment), the distinction is made between assessing EL parameters (state) EL and assessing EL quality (quality indicators) based on parameter values, and assessing the state and (or) quality of the electronic library by three criteria: suitability, optimality, and superiority.

In such cases, for multi-criteria quality analysis (assessment), it is advisable, in our opinion, to use interval statistical models, which requires the development of new methods of quality analysis and their justification.

Existing methods for analyzing the quality of complex systems with incomplete information, based on the use of the theory of possibilities and the theory of fuzzy sets, are scattered and solve limited classes of problems.

The lack of common, unified approaches to their application based on mathematical rigor, the lack of a justified and practical interpretation of the entire variety of QIs of systems of this class makes it difficult for them to be applied by EL officials and engineers in the field of quality control and management.

Therefore, the urgent task is not only to develop new, modern, unconventional approaches to the analysis of quality, but also a clear and rigorous argumentation of their application, to establish a connection with the traditional probabilistic QIs of complex information systems.

The solution to these problems is relevant at the present time when expanding the scope and geography of the application of EL, in the construction of new highly reliable and effective elements that must satisfy modern requirements.

Thus, the essence and content of the features of the development of modern electronic libraries as the basic elements of the modern educational information and telecommunication infrastructure are considered. The analysis of approaches to assessing the quality of electronic libraries is carried out, the potential possibilities of quality analysis using well-known principles of the theory of interval means are considered.

References

1. Antopolsky A. B., Markarova T. S., Kryukova O. P., Kharlamov A. A. Electronic libraries in education / Edited by O. P. Kryukova, A. A. Kharlamov. M.: 2009. 94 p. [in Russian].

2. National standard of the Russian Federation GOST R 7.0.96-2016. Electronic libraries. The main types. Structure. Formation technology. M.: Standardinform, 2016. 13 p. [in Russian].

3. Zuykina K. L., Sokolova D. V., Skalaban A. V. Electronic Libraries in Russia. Current status and development prospects. M.: Your format, 2017. 120 p. [in Russian]

4. Electronic Library of the Ministry of Defense of the Russian Federation (2019) [Electronic resource]. URL: http://mil.ru/departament_informashion_system/activity/ellib.htm (accessed 11.12.2019). [in Russian].

5. Kryukova E. S., Parashchuk I. B. Features of the development of modern electronic libraries and analysis of approaches to assessing their quality // Modern technologies: pressing

issues, achievements and innovations: Collection of articles of the XXXI International scientific and practical conference. Penza: Science and Enlightenment. 2019. 54 p., pp. 34–36. [in Russian].

6. Sazonov V. V., Parashchuk I. B., Loginov V. A., Elizarov V. V. Mathematical support of ACS troops. SPb.: VAS. 2018. 256 p. [in Russian].

7. Gurov S. V., Utkin L.V. Reliability of systems with incomplete information. SPb.: Lyubavich, 1999. 160 p. [in Russian].

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ К РЕАГИРОВАНИЮ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

В. С. Авраменко, Д. А. Бочкарев, А. В. Маликов

Военная академия связи

В статье проведен анализ современных подходов к организации реагирования на компьютерные инциденты. Рассмотрены основные этапы реагирования, реализуемые организационные и технические мероприятия. Выделены основные недостатки существующих подходов к управлению инцидентами. Предлагается подход к автоматизации функции анализа инцидентов на основе методов машинного обучения.

анализ, нарушение безопасности, компьютерный инцидент, реагирование, машинное обучение.

Реагирование является одним из этапов управления компьютерными инцидентами (КИ) и осуществляется после обнаружения, анализа событий безопасности и регистрации инцидентов.

Для объектов информационной инфраструктуры за последние годы в России разработано достаточное большое количество федеральных и ведомственных нормативно-правовых документов, в том числе и регламентирующих мероприятия по реагированию на компьютерные инциденты. Общие рекомендации по менеджменту инцидентов информационной безопасности в организациях изложены в [1].

Меры по реагированию на КИ в организациях, не связанных с объектами критической информационной инфраструктуры, могут отражаться в локальных нормативных актах (например, в положениях «О порядке выявления и реагирования на инциденты информационной безопасности»), но зачастую такие положения разрабатываются формально, без учета требо-

ваний к реагированию по результативности, оперативности и ресурсоемкости), особенностей конкретных информационных систем, а их содержание в основном раскрывает порядок проведения служебного расследования с целью привлечения к ответственности должностных лиц.

Из зарубежных источников по вопросам регулирования управления компьютерными инцидентами следует выделить стандарт NIST (*National Information Standardization Institute*) SP 800-61 «Computer security incident handling guide» – полноценное руководство по обработке компьютерных инцидентов, описывающее различные подходы к реагированию на инциденты и их обработке. Данное руководство определяет следующие этапы жизненного цикла процесса управления инцидентами:

– подготовительный этап;
– обнаружение и анализ инцидентов;
– сдерживание, ликвидация и восстановление;
– постинцидентные мероприятия.

Начальная фаза включает назначение и обучение команды реагирования на инциденты, обеспечение её необходимыми средствами и ресурсами. Во время подготовки организация также пытается ограничить число потенциальных инцидентов, выбирая и реализуя ряд мер безопасности на основе результатов оценок степени риска. Однако риск возникновения инцидента неизбежно сохраняется после реализации мер безопасности, поэтому необходимо проводить мероприятия по обнаружению нарушений защиты.

В соответствии со степенью опасности инцидента организация может смягчить воздействие инцидента, ограничивая его и устраняя его последствия. Во время этой фазы действия часто возвращаются назад к обнаружению и анализу, например, чтобы определить, не заражены ли дополнительные хосты вредоносным программным обеспечением после ликвидации инцидента.

Сдерживание необходимо, чтобы предотвратить ущерб. Сдерживание необходимо начинать как можно раньше при выявлении инцидента, так как сдерживание предоставляет время для разработки адаптированной стратегии устранения. Основная часть сдерживания – принятие решения о конкретных мерах реагирования (например, выключить систему, разъединить ее от сети, отключить некоторые функции). Такие решения намного легче принять, если существуют предопределенные стратегии и процедуры сдерживания инцидента. Организации должны определять приемлемые риски при обращении с инцидентами и разрабатывать соответствующие стратегии.

Стратегии сдерживания варьируются на основе типа инцидента. Например, стратегия сдерживания вредоносных программных средств, распространяемых электронной почтой, существенно отличается от стратегии сдерживания сетевой DDoS-атаки. Организации должны создать отдельные

стратегии сдерживания для каждого основного типа инцидента с ясно определёнными критериями, чтобы облегчить принятие решения.

Критерии определения стратегии включают:

– потенциальный ущерб ресурсам и хищение ресурсов;

– потребность в сохранении свидетельств;

– доступность сервиса (например, сетевое соединение, услуги, предоставленные третьим сторонам);

– время и ресурсы, необходимые для реализации стратегии;

– эффективность стратегии (например, частичное сдерживание, полное сдерживание);

– длительность решения (например, чрезвычайная работа, которая будет завершена через четыре часа, временная работа, которая будет завершена через две недели, постоянное решение).

После того, как инцидент ликвидирован, организация выпускает отчет, который детализирует причину и ущерб от инцидента, а также шаги, которые организация должна предпринять в целях предотвращения будущих инцидентов. Такой отчет подробно описывает действия, происходившие на основных этапах.

Похожие требования к реагированию отражены в руководстве Правительства Австралии по реагированию на инциденты кибербезопасности. В данном документе реагирование на инциденты предусматривает обнаружение инцидентов, управление ими и составление отчета об инциденте.

Положительной стороной данных документов является признание необходимости классификации потенциальных компьютерных инцидентов по различным признакам (в первую очередь, по степени возможного ущерба), их приоритезации и формирования различных стратегий реагирования. Это позволяет оптимально распределить ресурсы подразделения информационной безопасности, обеспечить высокую результативность и оперативность реагирования с минимальными затратами.

Резюмируя вышесказанное, необходимо подчеркнуть важность осуществления реагирования на инциденты по следующим причинам.

Во-первых, приведенные выше меры реагирования на КИ позволяют своевременно локализовать инцидент, минимизировать ущерб от инцидентов и предотвратить их возникновение в будущем за счет превентивных и проактивных действий.

Во-вторых, осуществление сбора информации о прошедших инцидентах в статистических целях позволяет проводить прогнозирование и оценку рисков информационной безопасности, а также улучшать имеющиеся инструменты информационной безопасности (например, создавать датасеты для обучения программного обеспечения, функционирующего на основе искусственных нейронных сетей).

В-третьих, ведение постоянного мониторинга множества событий и их последующий анализ (в том числе с использованием методов корреляции) позволяет выявить и предотвратить инциденты, на первый взгляд неочевидные и незначительные.

Осуществление полноценного процесса реагирования на компьютерные инциденты без автоматизации процессов и использования соответствующих инструментов в современных условиях невозможно. Однако, прежде всего следует определить порядок управления инцидентами, и только потом – какие технические решения применять.

Ключевой задачей управления КИ является анализ обнаруженных инцидентов с целью идентификации характеристик нарушений безопасности, существенных для принятия решения по первоочередным мерам реагирования, то есть по сдерживанию. К таким характеристикам относятся источник, цель, причины нарушения, способ его реализации и другие. Оперативный анализ инцидентов в интересах решения задачи сдерживания является частной задачей анализа состояния защиты, поэтому для ее выделения в качестве отдельной задачи целесообразно использовать термин диагностирование инцидентов [2, 3].

Основные диагностические данные об инциденте могут предоставить средства защиты информации и средства автоматизации (например, в сообщении от системы обнаружения атак содержится имя атаки, адрес источника и другие первичные диагностические признаки). В SIEM-системах сосредотачивается первичная диагностическая информация и информация об обнаруженных инцидентах, но этих данных не всегда достаточно для принятия адекватного решения, особенно в сложных ситуациях, например, при одновременном возникновении нескольких инцидентов. В основном диагностирование в современных инфокоммуникационных системах осуществляется в автоматизированном режиме, требует высокой квалификации администраторов безопасности, занимает длительное время.

Таким образом, к основным недостаткам существующих подходов к реагированию на КИ следует отнести низкую оперативность анализа (диагностирования) выявленных инцидентов, а также неполноту и низкую достоверность результатов диагностирования, обуславливающих, в свою очередь, неадекватность принимаемых решений на реагирование. Также решение на реагирование и непосредственно сами мероприятия по реализации выбранной стратегии реагирования главным образом реализуются в «ручном» режиме, занимают в сложных ситуациях недопустимо длительное время. Особенно критичны данные недостатки в условиях жестких требований по оперативности реагирования и высокой степени неопределенности априорной информации об угрозах, что требует реализации адаптивного подхода к защите информации, и в частности – к реализации функции обнаружения и диагностирования [4].

Основным путем повышения эффектности реагирования, и, в первую очередь – оперативности и адекватности, является повышение уровня автоматизации выполнения таких функций как диагностирование выявленных компьютерных инцидентов и выработка решения на мероприятия по сдерживанию. Перспективным направлением решения данной задачи является применение технологий искусственного интеллекта, в частности искусственных нейронных сетей. Например, предложенные в [5] модель и методика диагностирования компьютерных инцидентов безопасности, на основе комбинированной искусственной нейронной сети, позволяют в близком к реальному масштабу времени и с достаточно высокой достоверностью определять значения характеристик нарушений безопасности.

Список используемых источников

1. ГОСТ РИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М. : Стандартинформ, 2009.

2. Авраменко В. С. Модели защищенности информации от несанкционированного доступа в многорежимных автоматизированных системах и методы ее контроля в условиях неопределенности угроз // Информация и космос. 2008. № 2. С. 87–94.

3. Авраменко В. С., Маликов А. В. Диагностирование нарушений безопасности информации в инфокоммуникационных системах на основе искусственных нейронных сетей // Сборник трудов конференции «Региональная информатика и информационная безопасность». Выпуск 4. СПб. : Изд-во СПОИСУ, 2017. С. 24–26.

4. Авраменко В. С. Адаптивный контроль защищенности информации от несанкционированного доступа // Информация и космос. 2010. № 3. С. 116–119.

5. Авраменко В. С., Маликов А. В. Диагностирование компьютерных инцидентов безопасности на основе комбинированной искусственной нейронной сети // Защита информации. Инсайд. 2019. № 6. С. 72–77.

УДК 004.056
ГРНТИ 28.23.37

ПОДХОД К АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ С ПРИМЕНЕНИЕМ МАШИННОГО ОБУЧЕНИЯ

В. С. Авраменко, А. В. Маликов

Военная академия связи

В статье предлагается подход к аутентификации пользователей в ходе сеанса их работы на средствах автоматизации на основе комбинированной искусственной

нейронной сети. В результате обучения искусственной нейронной сети формируется эталонный информационный почерк для каждого пользователя. В ходе функционирования инфокоммуникационной системы осуществляется определение степени соответствия текущих значений характеристик действий пользователя его эталонному информационному почерку.

аутентификация, информационный почерк, искусственные нейронные сети, автоэнкодер, журнал событий.

Аутентификация субъектов доступа является одной из ключевых функций системы защиты информации от несанкционированного доступа. В инфокоммуникационных системах с высокими требованиями к защищенности информации кроме традиционных паролей используются дополнительные средства аутентификации (токены, биометрические средства и др.). Основным недостатком существующих технологий аутентификации является возможность использования аутентификатора другими лицами или его подмены при входе в систему, а также возможность подмены пользователя в ходе сеанса работы. Особенно актуальна данная проблема в системах с удаленными пользователями. В [1] предложен метод постоянной аутентификации по информационному почерку на основе методов статической теории распознавания образов и теории нечетких множеств. Данный метод в качестве признаков использует ограниченный набор явных индивидуальных характеристик работы пользователя на средствах автоматизации, но для повышения точности аутентификации целесообразно расширить данный перечень, используя для этого методы машинного обучения.

Потенциально большой набор признаков содержит операционный стиль работы пользователя – составляющая психомоторного компонента информационного почерка [1], отражающая содержание и привычный порядок выполнения работы пользователем на средствах автоматизации. Например, к явным признакам операционного стиля работы пользователя относится множество программных средств и информационных ресурсов, используемых при выполнении задач на средствах автоматизации, перечень приемов выполнения отдельных задач при работе с отдельным программным средством или с набором программных средств и др.

Исходные данные для формализации и расчета значений признаков операционного стиля содержатся в журналах событий, также могут использоваться программные сенсоры для регистрации действий пользователя на уровне системных вызовов, драйверов устройств ввода-вывода и других источников данных о действиях пользователей.

Одним из широко применяемых методов машинного обучения при наличии наборов обучающих данных являются искусственные нейронные сети, применяемые во многих областях научных знаний, где исследуются модели с неопределенной зависимостью выходных результирующих значений от имеющихся входных данных [2, 3, 4].

В решаемой задаче аутентификации пользователей по их информационному почерку в ходе сеанса их работы в качестве обучающих наборов для искусственных нейронных сетей в первую очередь могут быть использованы события, формируемые и фиксируемые в журналах по результатам действий пользователей.

Известны работы, в которых применяются искусственные нейронные сети в задачах анализа журналов событий. Так, в [5] приведен подход к изучению поведения пользователя для выявления вторжений уровня узла. Однако количество нейронов входного слоя создаваемой искусственной нейронной сети не оптимизируется в интересах снижения времени обучения.

В целях снижения «шумов» данных из журналов событий при извлечении информативных событий, а также уменьшения количества нейронов входного слоя классификатора, предлагается использовать комбинированную искусственную нейронную сеть, предложенную в [6]. Структура комбинированной искусственной нейронной сети включает кодирующую часть автоэнкодера и многослойный персептрон. Автоэнкодер позволяет снизить размерность вектора входных данных, а многослойный персептрон осуществляет классификацию полученных признаков.

Сбор данных для формирования эталонного информационного почерка пользователя необходимо осуществлять в течение достаточно длительного времени. Например, в течение рабочего дня для журналов событий рабочей станции пользователя и других элементов сети, формируется матрица признаков, включающая события, обозначаемые как $x_i \in X, i = \overline{1, N_{\text{тип}}}$, где $N_{\text{тип}}$ – количество типов событий. На рис. 1 (см. ниже) приведен пример формирования матрицы признаков.

Сформированная матрица признаков подается на вход автоэнкодера (рис. 2, см. ниже) – вариант многослойного персептрона с числом нейронов скрытого слоя меньшим, чем число нейронов входного слоя и обучающийся по методу глубокого обучения. Для достижения высокого качества обучения такая процедура может повторяться на основе данных нескольких сеансов работы. В итоге автоэнкодер формирует в скрытом слое компактные признаки почерка, которые используются для обучения многослойного персептрона.

В результате обучения персептрона формируются эталонные информационные почерки всех пользователей. На этапе функционирования системы выборки текущих пользовательских событий по мере их формирования подаются на вход комбинированной сети, затем проверяется соответствие идентификатора входной выборки идентификатору, полученному на выходе. В случае несоответствия подается сигнал тревоги. Следует заметить, что для учета возможности реализации угрозы неизвестным системе защиты

нарушителем необходим дополнительный класс «неизвестный нарушитель».

Рис. 1. Пример формирования матрицы признаков

Таким образом, все действия пользователя в ходе сеанса его работы подвергаются процедуре проверки его подлинности.

Также данный подход может применяться и для решения задачи определения личности нарушителя, решаемой в ходе диагностирования компьютерных инцидентов [7].

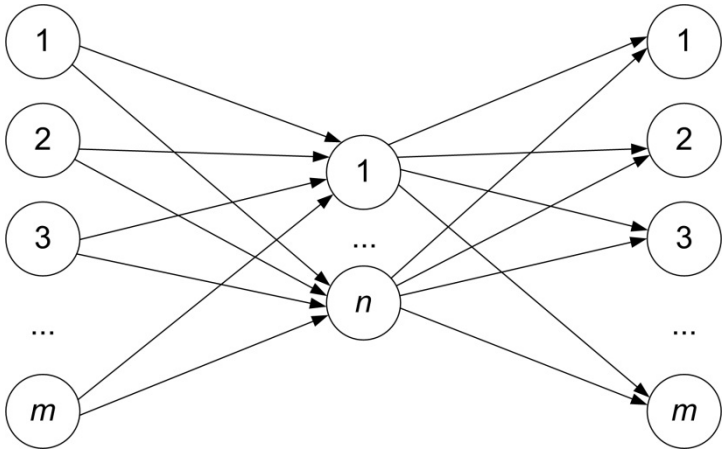


Рис. 2. Пример автоэнкодера для обработки матрицы диагностических признаков

Список используемых источников

1. Авраменко В. С. Способ постоянной аутентификации пользователей в автоматизированных системах на основе информационного почерка // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 2. С. 4–9.
2. Паращук И. Б., Башкирцев А. С., Михайличенко Н. В. Анализ уровней и видов неопределенности, влияющей на принятие решений по управлению информационными системами // Информация и космос. 2017. № 1. С. 112–120.
3. Паращук И. Б., Михайличенко Н. В. Нейро-нечеткие модели в интересах управления данными в ЦОД и интеллектуального анализа информации в региональных телекоммуникационных сетях // Региональная информатика (РИ-2016): Юбилейная XV Санкт-Петербургская межрегиональная конференция «Региональная информатика (РИ-2016)». СПб., 26–28 октября 2016 г.: материалы конференции. СПб.: Изд-во СПОИСУ, 2016. 599 с. С. 117.
4. Михайличенко Н. В. Вероятностно-временная модель для анализа динамики изменения состояний центров обработки данных // Системы управления, связи и безопасности. 2019. № 1. С. 54–66.
5. Зуев В. Н., Ефимов А. Ю. Нейросетевой поведенческий анализ действий пользователя в целях обнаружения вторжений уровня узла // Программные продукты и системы. 2019. Т. 32. № 2. С. 268–272.
6. Маликов А. В., Авраменко В. С., Саенко И. Б. Модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационных системах, основанные на глубоком машинном обучении // Информационно-управляющие системы. 2019. № 6. С. 32–42.
7. Авраменко В. С. Способы идентификации нарушителя безопасности информации в автоматизированных системах на основе информационного почерка // Проблемы технического обеспечения войск в современных условиях. II межвузовская конференция: сб. тр. СПб. : ВАС, 2017. С. 36–40.

УДК 004.021
ГРНТИ 28.17.27

МОДЕЛЬ РАСПРЕДЕЛЕННОЙ LMS НОВОГО ПОКОЛЕНИЯ

А. М. Адуевский, Г. В. Верхова, К. В. Кучеревский

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящий момент времени системы управления учебным процессом находят все более широкое применение в системе высшего и среднего образования. Такие системы обеспечивают комплексную автоматизацию и информатизацию учебного процесса, существенно повышая качество подготовки специалистов. Концепция цифрового университета предъявляет новые, более жесткие требования к данному классу систем.

Представлены результаты анализа современного состояния и перспектив развития LMS. Проанализированы достоинства и недостатки, существующих систем управления учебным процессом. Показано, что для соответствия требованиям концепции цифрового университета LMS должны строиться по принципу распределенных систем.

LMS, цифровой университет, система управления учебным процессом, распределенная система.

В настоящий момент времени системы управления учебным процессом (англ. LMS – *Learning Management System*) находят все более широкое применение в системе высшего и среднего образования [1, 2]. Такие системы обеспечивают комплексную автоматизацию и информатизацию учебного процесса, существенно повышая качество подготовки специалистов. Основной целью внедрения LMS является улучшения качества процесса обучения. LMS представляет собой цифровую платформу, на базе которой осуществляется управление учебным процессом. Системы управления учебным процессом обеспечивают размещение электронных образовательных ресурсов, выполнение измерений результатов освоения учащимися учебного материала, сохранение данных об учащихся, информационное взаимодействие всех участников учебного процесса. Концепция цифрового университета предъявляет новые, более жесткие требования к данному классу систем [3].

На современном рынке представлено большое количество LMS от разных производителей, обеспечивающих автоматизацию широкого спектра задач. Однако современные LMS не лишены недостатков, основным из которых является отсутствие возможности глубокой интеграции отдельных блоков и инструментов от разных производителей в единую систему. Так как не все LMS являются кроссплатформенными, существует существенное ограничение на использование современных мобильных устройств в образовательном процессе. Кроме того, современные LMS не обеспечивают достаточную кастомизацию образовательной среду под отдельных пользователей.

Параметры наиболее распространенных LMS представлены в таблице (см. ниже).

Как видно из таблицы, современные LMS обладают сходной функциональностью, хотя могут существенно отличаться дизайном пользовательского интерфейса, эргономикой и уровнем поддержки. Хотя на базе существующих систем можно создать достаточно развитые и качественные электронные курсы, они не подходят для внедрения в единую образовательную среду цифрового университета. Перспективные LMS должны строиться по принципу открытых распределенных систем, обладать интероперабельностью и возможностью глубокой кастомизации, чтобы обеспечить формирование единой образовательной среды, отвечающей потребностям каждого университета.

ТАБЛИЦА. Сравнительный анализ параметров, наиболее распространенных LMS

Параметр	Moodle	iSpring	WebTutor
Создание контента	+	+	+
Продажа курсов	+	–	–
Мобильное обучение	+	+	+
Вебинары	+	+	+
Поддержка SCORM	+	+	+
Геймификация	+	+	+
Брендирование	+	+	+
Облачная версия	+	+	–
Коробочная версия	+	+	+

Исходя из сформулированных выше требований, распределенные LMS нового поколения должны:

– иметь сервисно-ориентированную архитектуру;

– обладать интероперабельностью;

– состоять из отдельных модулей, выполняющих ограниченный набор функций, реализованных в виде микросервисов;

– допускать глубокую интеграцию в единую информационную среду цифрового университета, а также в глобальную образовательную киберсреду;

– допускать использование модулей от различных производителей;

– быть кроссплатформенными;

– обеспечивать доступ к образовательным ресурсам с любых вычислительных устройств;

– допускать развертывание на внешних серверах или на серверах конкретного учебного заведения.

В общем виде перспективная LMS может быть представлена в виде выражения:

$$LMS \stackrel{\text{def}}{=} < EER, ILP, SQM, ILPSh >, \quad (1)$$

где *EER* – электронные образовательные ресурсы основной образовательной программы, сгруппированные по интерактивным учебно-методическим комплексам (2); *ILP* – индивидуальная траектория обучения; *SQM* – квалиметрическая модель учащегося; *ILPSh* – планировщик индивидуальных траекторий обучения.

Интерактивный учебно-методический комплекс *EMC* представляет собой основу LMS:

$$EMC \stackrel{\text{def}}{=} < E, Q, R, Eval, Config >, \quad (2)$$

где E – электронные образовательные ресурсы; Q = < Q_1, Q_2 > – квалиметрическая модель, состоящая из фонда оценочных средств Q_1,

позволяющего оценить уровень усвоения материала, содержащегося в учебно-методическом комплексе, и квалиметрической модели Q_2, дающей возможность оценить качество материалов, содержащихся в модуле; *R* – связи между элементами учебно-методического комплекса; *Eval* – алгоритмы управления курсом; *Config* – механизм конфигурации электронного учебно-методического комплекса, обеспечивающий возможность адаптации электронных образовательных ресурсов под индивидуальную траекторию обучения.

Внедрение LMS нового поколения обеспечит:

– существенное повышение качества учебного процесса и общей культуры высшего образования;

– поддержку интерактивных форм обучения;

– поддержку всех видов и форм занятий (теоретические, практические, самостоятельные, индивидуальные, групповые, фронтальные);

– глубокую интеграцию в информационную среду цифрового университета и глобальную образовательную киберсерду;

– глубокую кастомизацию и адаптацию под индивидуальные особенности учащихся;

– возможность тиражирования опыта ведущих преподавателей;

– модульность (возможность использования одних и тех же модулей в курсах различных дисциплин);

– поддержку все видов современных вычислительных устройств;

– непрерывный мониторинг уровня усвоения учебного материала [4, 5, 6] для текущей и промежуточной аттестации.

Список используемых источников

1. Kim M., Bergman L., Lau T., Notkin D. Ethnographic Study of Copy and Paste Programming Practices in OOPL // Proceedings. 2004 International Symposium on Empirical Software Engineering, 2004. ISESE'04. Pp. 83–92. DOI:10.1109/ISESE.2004.1334896

2. Юрловская И. А. Исследование теоретико-методических интерактивных форм высшей школы // Мир науки. 2014. № 1. С. 13.

3. Verkhova G. V., Akimov S. V. The Role of the Unified Educational Cyber Environment in Improving the Quality of Training of Engineer Personnel // Proceedings of 2018 17th Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region, PTES 2018. PP. 70–74. (SCOPUS, IEEE) DOI: 10.1109/PTES.2018.8604190.

4. Гребенюк Т. Б., Панюшкина М. А. Моделирование квалиметрической компетентности на основе концепции индивидуальности // Вестник Балтийского федерального университета им. И. Канта. 2016. Сер.: Филология, педагогика, психология. № 2. С. 81–91.

5. Васильева Н. О. Оценка образовательных результатов студентов на основе модели компетенций // Современные проблемы науки и образования. 2017. № 6. С. 177.

6. Tkhagapsoyev K. G., Robert K. K., Martin M. Y. // To Problems of Qualimetric Estimation of Quality in Education and Science // IEEE International Conference "Quality

Management, Transport and Information Security, Information Technologies" (IT&QM&IS). 2018. Pp. 692–695. DOI: 10.1109/ITMQIS.2017.8085918.

УДК 004.946
ГРНТИ 28.23.39

ПРОТОТИП ПРОГРАММНОГО МОДУЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ СВЯЗЯМИ МЕЖДУ АГЕНТАМИ КИБЕРФИЗИЧЕСКОЙ СРЕДЫ

С. В. Акимов, М. А. Гордеев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлен прототип программного модуля, реализующего управление информационными связями между агентами, формирующими киберфизическую среду. Агентами киберфизической среды являются физические лица, группы физических лиц и техногенные объекты, представляющие собой оборудование и программное обеспечение. Программный модуль позволяет устанавливать между агентами информационно нагруженные связи следующих типов: P2P, B2B, M2M, P2B, P2M, B2M. В результате установления данных связей формируется семантическая сеть, отражающая отношения между агентами. На основании информации, содержащейся в семантической сети, может быть реализовано управление информационными процессами, участниками которых являются упомянутые выше агенты, в частности, управление правами доступа. Программный модуль, реализующий управление информационными связями, может быть использован при формировании единой информационной среды постиндустриального общества.

киберфизическая среда, информационные связи, постиндустриальное общество, агенты, P2P, B2B, M2M, P2B, P2M, B2M.

На современном этапе развития общества существует потребность в создании единой киберфизической среды, которая объединит всех участников, представленных в данной среде агентами или цифровыми двойниками (*digital twins*) [1]. Агенты киберфизической среды представляют физических лиц, группы физических лиц и техногенные объекты (оборудование и программное обеспечение).

Сеть участников киберфизической среды NET_{KE} может быть представлена в следующем виде:

$$NET_{KE} \stackrel{\text{def}}{=} \langle \mathrm{P}, \mathrm{B}, \mathrm{M}, \mathrm{R} \rangle, \quad (1)$$

где P – физические лица (*Peers*); B – группы физических лиц (*Business*); M – техногенные объекты (*Machines*); R – связи, устанавливаемые между участниками сети:

$$R \in \{R_{P2P}, R_{B2B}, R_{M2M}, R_{P2B}\ R_{P2M}\ R_{B2M}\}. \quad (2)$$

В результате установления данных связей формируется семантическая сеть, отражающая отношения между агентами (рис. 1). На основании информации, содержащейся в семантической сети, может быть реализовано управление информационными процессами, участниками которых являются упомянутые выше агенты, в частности, управление правами доступа.

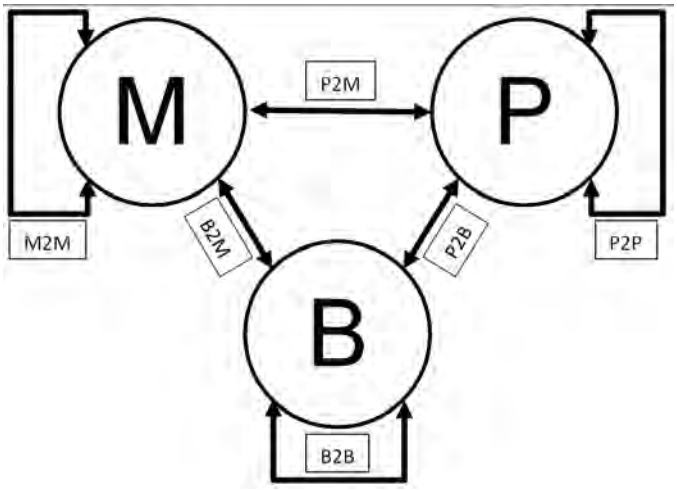


Рис. 1. Информационные связи между агентами киберфизической среды

Одним из важнейших элементов киберфизической среды является менеджер связей, представляющий собой программный модуль, позволяющий устанавливать между агентами информационно нагруженные связи. Программный модуль, реализующий управление информационными связями, может быть использован при формировании единой информационной среды постиндустриального общества или для поддержки интеллектуальных технологий «Индустрии 4.0». Объектная модель менеджера связей представлена на рис. 2 (см. ниже). Диаграмма классов репозиториев, выполняющих CRUD-операции (создания, чтения, обновления и удаления), представлена на рис. 3 (см. ниже).

В настоящий момент на кафедре автоматизации предприятий связи разработан прототип менеджера связей для киберфизической среды, которую предполагается положить в основу программных продуктов, построенных с использованием технологий, поддерживающих интероперабельность. Программный прототип создан на языке объектно-ориентированного программирования C# с использованием принципов предметно-ориентированного проектирования (DDD – *Domain Driven Design*) и имеет микросервисную архитектуру [2, 3].

Список используемых источников

1. Акимов С. В., Верхова Г. В., Меткин Н. П. Теоретические основы CALS. СПб. : Изд-во СПбГУТ, 2018. 263 с.

2. Microsoft Corporation, Microsoft Docs. Документация по C#, ASP.NET и .NET [Электронный ресурс]. UML: https://docs.microsoft.com/ (дата обращения 29.03.2020)

3. Эванс Э. Предметно-ориентированное проектирование (DDD): структуризация сложных программных систем. М. : Вильямс, 2011. 448 с. ISBN 978-5-8459-1597-9.

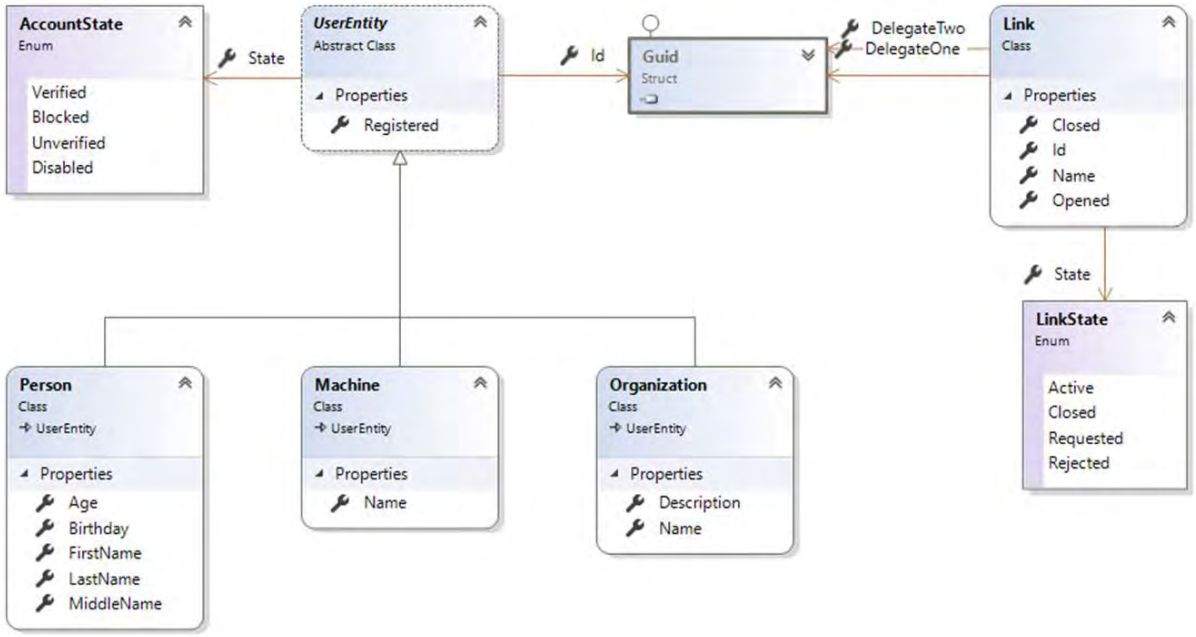


Рис. 2. Объектная модель менеджера связей

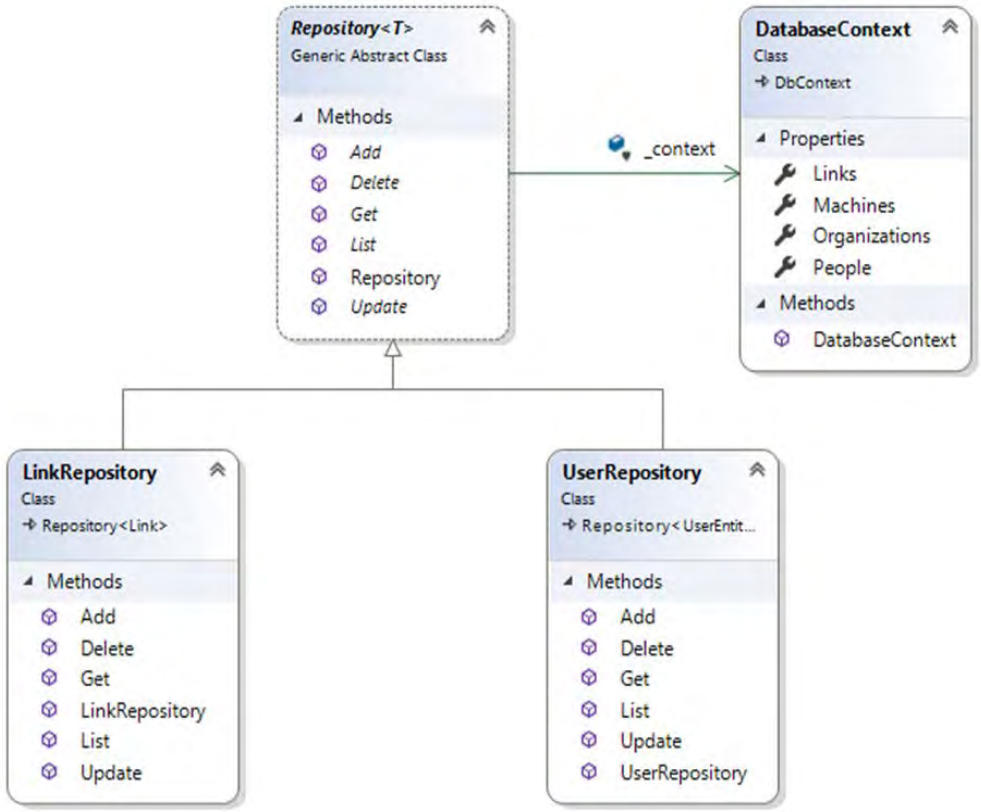


Рис. 3. Диаграмма классов репозитория менеджера связей

УДК 004.045
ГРНТИ 50.41.25

МОДЕЛИ И АЛГОРИТМЫ АВТОМАТИЧЕСКОГО ВЫЧИСЛЕНИЯ РЕЙТИНГОВ ДЛЯ РАСПРЕДЕЛЁННЫХ КИБЕРСРЕД ВИРТУАЛЬНЫХ ПРЕДПРИЯТИЙ

С. В. Акимов, Э. Р. Давлетшина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлены результаты анализа проблемы автоматического вычисления рейтингов субъектов виртуальных предприятий. Предложена модель вычисления индивидуальных многокритериальных рейтингов физических лиц и групп физических лиц, выполняемого в режиме реального времени. Рейтинги групп вычисляются на основе рейтингов физических лиц, составляющих данные группы. В роли групп могут выступать структурные подразделения и юридические лица. Группы могут образовывать иерархические структуры. Рейтинги вышестоящих групп вычисляются на основе групп, входящих в их состав. Рассмотренные модели и алгоритмы призваны обеспечить сокращение рутинных процедур, повышение уровня прозрачности и объективности результатов непрерывного мониторинга.

киберсреда, электронное портфолио, автоматизация, виртуальные предприятия.

В условиях внедрения технологий «Индустрии 4.0» и переходу к постиндустриальному обществу существует потребность в разработке методов и технологий эффективного управления трудовыми коллективами в рамках единой киберсреды виртуальных предприятий. Одной из особенностей постиндустриального общества и «Индустрии 4.0» является формирование временных трудовых коллективов, нацеленных на решение определенных задач. При этом требуется подобрать коллектив исполнителей, который максимально эффективно, в кратчайшие сроки будет способен решить поставленную задачу. Традиционные методы уже не удовлетворяют данным требованиям.

В статье изложена концепция автоматического вычисления рейтингов участников распределённых киберсред виртуальных предприятий, на основе которых возможно оценить качественный уровень физических лиц и трудовых коллективов, а также реализовать алгоритмы формирования временных трудовых коллективов. Приведенные результаты исследований полностью находятся в рамках концепции формирования единого информационного пространства, снижения рутинных операций, повышения качества

информационной поддержки субъектов, повышения уровня прозрачности, полноты и актуальности информации.

Основная идея заключается в создании электронного профиля и портфолио, которое является частью цифрового двойника участника киберфизической среды [1]. На базе портфолио формируется электронная репутация участника (физического или юридического лица). Профиль, или электронное портфолио, субъекта является сложной информационной структурой, которая отражает различные аспекты: личную информацию о субъекте, личные достижения, образование, результаты публикационной активности и регистрации интеллектуальной деятельности, информацию об участие в проектах, опыте работы, навыках и научных интересах.

Научная значимость исследования заключается в разработке многоаспектной модели электронного портфолио, на основе которого может быть создана система электронных репутаций и рейтингов. Практическая ценность заключается в повышении качества управления кадровыми ресурсами в рамках цифровой экономики и в процессе формирования постиндустриального общества, повышении значимости института электронной репутации, а также автоматизации процесса управления временными трудовыми коллективами.

Электронный профиль физического лица (*e-profile*) представляет собой открытую информационную систему, способную к взаимодействию с другими информационными системами (рис. 1).

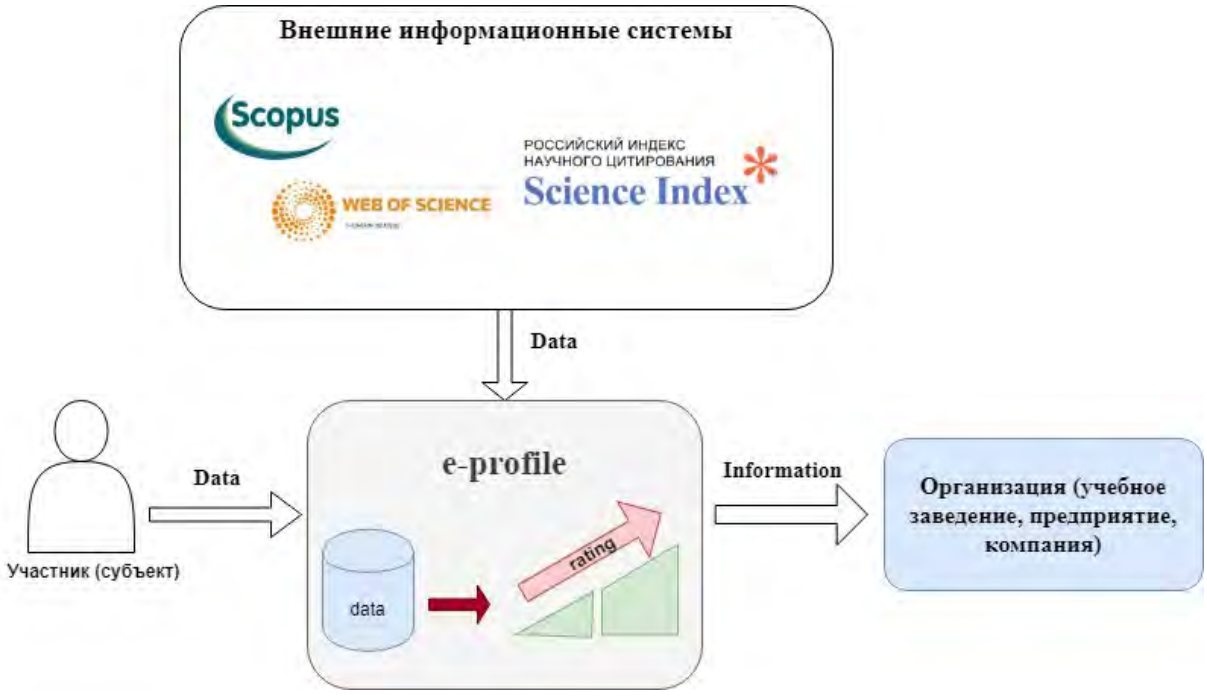


Рис. 1. Схема взаимодействия электронного профиля субъекта с внешними информационными ресурсами

Модель электронного портфолио (рис. 2) состоит из ряда сущностных классов, которые являются «каркасом» для представления данных по каждому из аспектов электронного профиля субъекта [2].

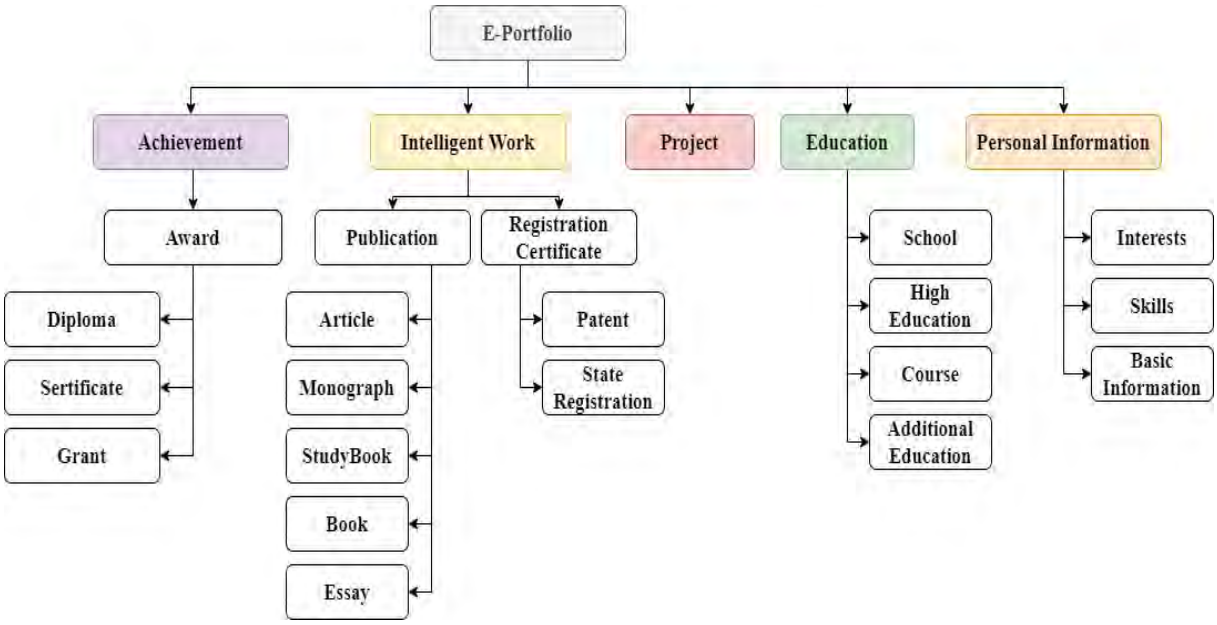


Рис. 2. Модель представления электронного портфолио

Система электронных портфолио должна автоматизировать выполнение следующих функций:

– аккумулирование многоаспектной информации о субъекте на протяжении всей профессиональной карьеры;

– обеспечение двустороннего информационного обмена между различными информационными системами по методу «одной кнопки» (система электронных портфолио должна допускать глубокую интеграцию с научными информационными системами, таким как РИНЦ, *Scopus, World of Science*);

– обеспечивать автоматическую подготовку информации для конкретных информационных систем по стандартным информационным шаблонам (например, автоматическая отправка информации для поступления в высшее учебное заведение);

– учет и подтверждение компетенций участников киберсреды;

– автоматическое вычисление рейтингов;

– автоматизированное формирование оптимальных временных трудовых коллективов для решения поставленных задач.

Авторы убеждены, что в условиях перехода к постиндустриальному обществу необходимо исключить все рутинные операции, поддающиеся формализации и автоматизации. Система электронных портфолио позволит осуществлять автоматическую генерацию по принципу нажатия одной

кнопки комплектов документов установленного образца, включая электронное портфолио и резюме. Система сама подберет целевой комплект документов, причем, при отсутствии какой-либо информации или электронных версий документов, пользователю будут сформированы соответствующие рекомендации. Следует заметить, что автоматическая генерация комплекта документов не исключает возможность ручной коррекции.

По информации, содержащейся в электронном профиле, система сможет автоматически вычислять его рейтинг, используя определенные формулы и алгоритмы. При вычислении рейтинга могут учитываться и рейтинги других участников киберсреды (так, рейтинг преподавателя высшего учебного заведения будет зависеть также от рейтингов его выпускников, у которых он является научным руководителем, а также от успеваемости студентов).

В качестве примера рассмотрим вычисления итогового рейтинга учащегося высшего учебного заведения [3]:

$$R_y = R_{\text{а}} + R_{\text{н}} + R_{\text{о}}, \quad (1)$$

где $R_{\text{а}}$ – оценка успеваемости учащегося; $R_{\text{н}}$ – суммарный рейтинг за награды (призы) за результаты проектной деятельности и (или) опытно-конструкторской работы; $R_{\text{о}}$ – суммарный рейтинг за участие в олимпиадах, конкурсах, соревнованиях, состязаниях и иных мероприятиях.

Расчет рейтингов, определяющий суммарный рейтинг субъекта в области учебной деятельности можно определить, например, по методике, разработанной в СПбГУТ по формулам (2)–(4) [3]:

$$R_{\text{а}} = 10a_1 + 8a_2 + 5a_3 \quad (1)$$

$$R_{\text{н}} = 6n_1^1 + 4n_2^1 + 9m_1^1 + 6m_2^1 + 12z_1^1 + 8z_2^1 + 15k_1^1 + 10k_2^1 \quad (2)$$

$$R_{\text{о}} = 6n_1^2 + 4n_2^2 + 9m_1^2 + 6m_2^2 + 12z_1^2 + 8z_2^2 + 15k_1^2 + 10k_2^2 \quad (3)$$

где коэффициенты $a^i, m_j^i, n_j^i, k_j^i, z_j^i$, отражающие различные аспекты учебной деятельности, вычисляются по методике, представленной в [3].

Участники системы могут образовывать трудовые коллективы (группы физических лиц, юридические лица), рейтинг которых будет зависеть от рейтингов участников, входящих в ее состав. Трудовые коллективы могут образовывать иерархические структуры, рейтинги которых вычисляются на основе рейтингов групп, входящих в их состав.

Иерархическая структура высшего учебного заведения представлена на рис. 3. Рейтинг образовательной группы зависит от рейтингов всех студентов, входящие в ее состав; рейтинг кафедры – от рейтингов групп, относящиеся к данной кафедре и преподавательского состава кафедры; рейтинг

факультета – от кафедр; рейтинг университета – от рейтингов факультетов. Таким же образом, можно вычислить рейтинги на более высоких уровнях: городском, региональном, всероссийском, международном уровнях.

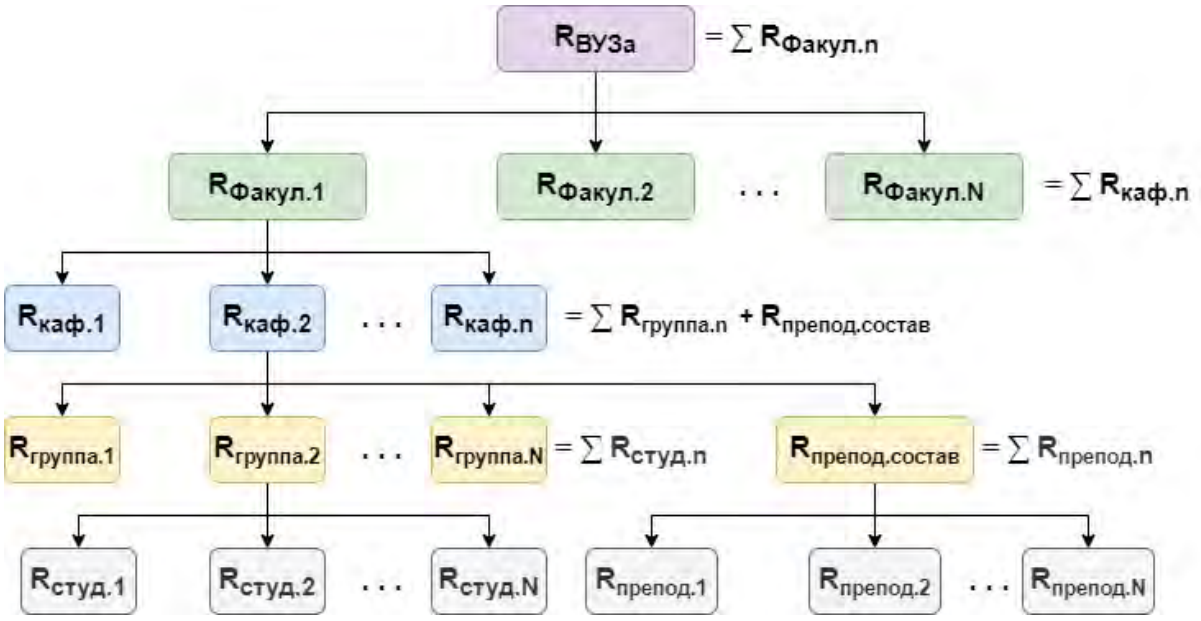


Рис. 3. Иерархическое представление вычисления рейтингов на уровне учебного заведения

Список используемых источников

1. Акимов С. В., Верхова Г. В., Меткин Н. П. Теоретические основы CALS. СПб.: Изд-во СПбГУТ, 2018. 263 с. ISBN 978-5-89160-172-7.

2. ГОСТ Р 7.0.100–2018 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления».

3. Положение о стипендиальном обеспечении обучающихся СПБГУТ, утвержденное приказом ректора СПбГУТ от 05.05.2017 г.

УДК 004.045
ГРНТИ 50.41.25

ПРИМЕНЕНИЕ ДЕЛЬТА-КОДИРОВАНИЯ ДЛЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

С. В. Акимов, В. Ю. Юплов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлены результаты исследования в области использования методов и алгоритмов дельта-кодирования для автоматизированных систем управления. Дельта-кодирование является одним из предпочтительных методов при формировании электронных документов, так как основано на принципах представления данных в виде разницы (дельты) между последовательными наборами данных, вместо самих данных. Дельта-кодирование обеспечивает сокращение трафика передачи данных, а также уменьшения требуемых объемов хранения версий документа. Одним из перспективных путей применения дельта-кодирования в распределенных автоматизированных системах управления является применение форматов документов, реализующих данный принцип. Рассмотрены возможные пути применения дельта-кодирования в автоматизации управления электронными документами путем создания соответствующих микросервисов и стандартных клиентских веб-технологий (HTML, CSS, JavaScript).

дельта-кодирование, VCDIFF, Quill Rich Text Editor.

Дельта-кодирование представляет собой способ представления данных в виде разницы (дельты) между последовательными данными вместо самих данных. Дельта-кодирование нашло широкое применение в радиосвязи, так как обеспечивало достаточно простой и эффективный способ передачи сигнала. Дельта-кодирование применяется в звуковом формате IFF 8SVX на стадии, предшествующей компрессии.

Другое применение дельта-кодирование нашло в представлении символьной (в частности, текстовой) информации. Разновидностью дельта-кодирования является инкрементное кодирование, при котором кодированию подвергается различие в префиксах и постфиксах текстовых строк. Инкрементное кодирование особенно эффективно для отсортированных списков с малыми различиями между строками, такими как список слов в словаре.

В случае использования дельта-кодирования при передаче данных по сети, необходимо использовать специальные коды коррекции ошибок. Дельта-кодирование применяется на предварительном этапе многих алгоритмов сжатия информации, а также в инвертированных индексах поисковых программ. Эффективность применения дельта-кодирования существенно зависит от типа кодируемой информации. Дельта-кодирование

значительно повышает коэффициент сжатия в случае, когда данные имеют небольшую или постоянную вариацию (например, градиент на изображении).

Учитывая специфику автоматизированных систем управления, построенных на базе киберсред виртуальных предприятий, дельта-кодирование может быть успешно использовано при формировании пользовательских данных, хранящихся в записях реляционных баз данных, а также в базах данных NoSQL [1, 2, 3]. Это полностью соответствует стратегии работы с данными в киберфизических средах. Применение дельта-кодирования обеспечит механизм рационального хранения информации с возможностью создания большого числа точек восстановления.

Реализация представления информации может быть реализовано с помощью Quill, который представляет собой свободно распространяемый продукт с открытым исходным кодом. В рамках Quill реализован WYSIWYG редактор (*What You See Is What You Get* – свойство прикладных программ отображать содержимое в процессе редактирования максимально похожим на представление конечного документа). Данный редактор может быть использован в современных web-приложениях, имеющих модульную архитектуру и развитый интерфейс прикладного программирования.

В Quill используется дельта-кодирование для хранения версий документов. «Дельты» представляют собой простой формат, который можно использовать для описания содержимого и его изменений в Quill. Формат является строгим подмножеством JSON, достаточно удобочитаем, а также прост в использовании. С помощью «Дельт» можно представить любой текстовый документ, включая содержимое и информацию о логическом и визуальном форматировании.

Управление «Дельтами» реализовано в виде отдельной автономной библиотеки, что позволяет использовать ее вне Quill. Функционал может быть использован в режиме реального времени. Основные параметры Quill представлены в таблице (см. ниже).

Архитектура приложения, использующего методы дельта-кодирования для управления текстовой информацией, и его связь с киберсредой виртуальных предприятий, представлена на рис.

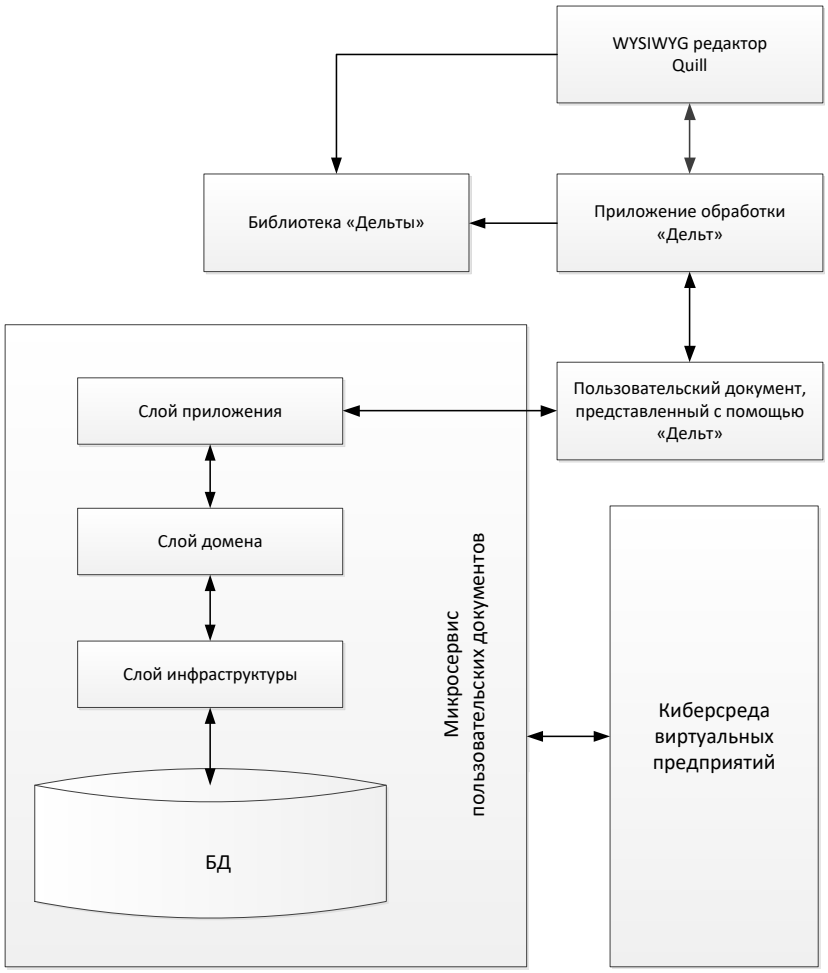


Рис. Приложение, использующее методы дельта-кодирования для управления текстовой информацией, в рамках киберсреды виртуальных предприятий

ТАБЛИЦА. Основные параметры Quill

Параметр	Описание
bounds	Элемент DOM или CSS-селектор для элемента DOM, внутри которого должны быть ограничены элементы пользовательского интерфейса редактора
debug	Свойство для отладки. Отладка реализована в виде статического метода, который влияет на все экземпляры редакторов Quill на веб-странице
formats	Управление разращёнными форматами данных. По умолчанию все форматы разрешены
modules	Коллекция модулей, обеспечивающих включение соответствующих опций
scrollingContainer	Элемент DOM или селектор CSS для элемента DOM, указывающий, какой контейнер должен иметь полосы прокрутки

Список используемых источников

1. Дуглас Ф., Хеллерштейн Д. Дельта-кодирование в HTTP. RFC 3229, 2002. 49 с.
2. Акимов С. В., Верхова Г. В., Меткин Н. П. Теоретические основы CALS. СПб. : Изд-во СПбГУТ, 2018. 263 с.

2. Официальный сайт проекта Quill [Электронный ресурс]. URL: https://quilljs.com/ (дата обращения: 30.03.2020)

УДК 004.93
ГРНТИ 28.23.15

АНАЛИЗ ПРИМЕНЕНИЯ КОМПЬЮТЕРНОГО ЗРЕНИЯ В ПРОМЫШЛЕННОСТИ

Д. Р. Акчурина, М. П. Белов, И. В. Грищенко, Ю. А. Шолухо

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье приведен анализ современных систем компьютерного зрения, применяемых в промышленности. Рассмотрены типы систем технического зрения и методы обработки изображений. Выявлены факторы, способствующие росту использования технологий компьютерного видения в Российской Федерации.

компьютерное зрение, обработка изображений, техническое зрение, промышленность.

Компьютерное зрение (*Computer Vision* – CV) – это автофиксация и обработка изображений, как движущихся, так и недвижимых объектов при помощи технических средств [1]. В РФ также применяется термин «техническое зрение».

Современное высокотехнологичное производство требует особых подходов к контролю качества выпускаемой продукции. Компьютерное зрение совершило настоящий технологический прорыв и значительно расширило возможности дефектоскопии в промышленности, перевела ее на новый, более высокий уровень. Теперь технологии позволяют отслеживать качество не только после изготовления изделия или продукта, но и непосредственно во время производственного процесса. Кроме того, системы CV способны значительно упростить и ускорить дефектоскопию производственного оборудования, агрегатов и коммуникаций, находящихся в эксплуатации [2].

Выделяют три основных типа систем технического зрения [3]:

– одномерные (1D-системы);
– двумерные (2D-системы);
– объёмные (3D-системы).

Существуют особые виды систем CV: панорамные многокамерные системы (массивы) и системы «рыбий глаз» (от англ. *fish-eye*). В зависимости

от их конструкции, количества видеокамер и расположению такие системы относят к одному из перечисленных выше типов.

Панорамные (сферические) системы «рыбий глаз», работающие с приложениями обработки изображений, применяются, например, при мониторинге больших промышленных пространств и подсчёте количества работников.

Массивы применяются с целью отслеживания передвижения отдельных людей внутри помещений или в участках с ограниченной видимостью (промышленные базы, заводские территории, склады и пр.).

В простых системах обработки компьютерного видения, как правило, необходимо получить количественную и качественную информацию из визуальных данных (изображений): такие параметры, как размер, тональность цветовой палитры, количество, направление и характер движения, а также контрастные переходы в окрестностях пикселя изображения, из которых получают характерные черты (ХЧ). На их основе производится исследование изображения для извлечения полезных данных [4].

В системах обработки изображений технического зрения используются такие методы, как:

– системы, основывающиеся на нейросетевых технологиях;
– системы глубокого обучения;
– машинное обучение.

Данные подходы имитируют деятельность анализа и идентификации объектов, которая проходит в мозге человека.

Существуют основные методы решения задач CV:

1. Контурный анализ.

Суть этого метода заключается в анализе не полноценного изображения объекта, а только его контура [5]. Данный подход позволяет существенно снизить сложность вычислений и алгоритмов при обработке. Ограничения, применимые к анализу контуров:

– при одинаковой яркости с фоном объект может не иметь чёткой границы на изображении или оно может быть «зашумлено» помехами, что приводит к невозможности выделения контура;
– перекрытие объектов или их группировка приводят к тому, что контур выделяется неправильно и не соответствует границе объекта;
– слабая устойчивость к помехам, приводящая к тому, что любое нарушение целостности контура или плохая видимость объекта приводят либо к невозможности детектирования, либо к ложным срабатываниям.

2. Поиск по шаблону.

Наиболее распространённый метод идентификации объектов в CV – поиск соответствия по шаблонам изображений. Для того, чтобы установить однозначно, есть ли заданный объект на изображении, и, если есть,

где он находится на изображении. Приложения данной категории: распознавание движущихся деталей на конвейерной ленте, прокладывание маршрутов для мобильных роботов, производственные приложения и др. Базовые типы поиска по шаблону представлены ниже:

– простое соответствие;
– соответствие на базе характерных черт;
– соответствие на базе областей;
– корреляция изображений;
– нейросети;
– глубокое обучение в системах технического зрения;
– калибровка камер по шаблону.

3. Поиск вне шаблонов, сопоставление по ключевым меткам.

Элементы изображения (точки, края, линии или границы объектов) представляют собой наборы характерных черт для обработки изображений. Ещё примером характерных черт может служить движение в последовательности изображений, или формы, представленные в виде кривых между областями изображений, или свойства этих областей [6]. Основные виды поиска вне шаблонов:

– обнаружение и распознавание объектов;
– фотограмметрия;
– детектирование препятствий;
– одновременная локализация и построение карты (*Simultaneous Localization And Mapping* – SLAM);
– дефектоскопия;
– идентификация объектов и локализация в заранее снятой сцене;
– локализация наблюдателя и фиксирование измерений;
– коррекция экспозиции и цвета.

4. Совмещение данных (*Data Fusion*).

Data Fusion – это совмещение данных от различных источников изображений (с видеокамер) с помощью компьютерного зрения, чтобы получить более точную и полезную информацию. В методе Data Fusion CV можно выделить следующие недостатки:

– из одного изображения можно выделить различные характерные черты;
– экземпляры одного класса объектов могут выглядеть по-разному;
– поведение экземпляров одного класса объектов может быть различно, по крайней мере, временами;
– один объект с разных ракурсов (или с разных камер) может выглядеть по-разному;
– разные комбинации вышеперечисленных факторов.

Совмещённый анализ изображений от системы CV и данных от комплекса датчиков значительно улучшает ценность информации, получаемой от системы CV и позволяет значительно улучшить работу приложения, её использующего.

Системы компьютерного зрения не ограничиваются только этими методами. Например, можно выделить методы на основе генетических алгоритмов, которые, в частности, находят применение для распознавания лиц.

К основным факторам роста использования CV технологий в России следует отнести следующие:

– развитие и продвижение национальной программы цифровой экономики, в которой компьютерное зрение вынесено в отдельный пункт раздела «Нейротехнологии и искусственный интеллект» [7];

– развитие таких решений, как «Безопасный город», «Умный город» и интеллектуальные транспортные системы;

– увеличение уровня автоматизации промышленного производства;

– потенциал отечественных разработок на рынке систем робототехники и автоматизации;

– развитие Интернета Вещей (*Internet of Things* – IoT) и промышленного интернета (*Industrial Internet of Things* – IIoT) и др.

Список используемых источников

1. Селянкин В. В. Компьютерное зрение. Анализ и обработка изображений: учебное пособие. СПб. : Лань, 2019. – 152 с.

2. Крупенников И. В. Разработка методов и алгоритмов обработки данных систем машинного зрения в реальном масштабе времени : дис. … канд. техн. наук : 05.14.15 / Крупенников Илья Владимирович. Москва, 2011. 134 с.

3. Лапан М. Глубокое обучение с подкреплением. AlphaGo и другие технологии. СПб.: 2019. 176 с.

4. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. СПб. : Питер, 2018. 480 с.

5. Жерон О. Прикладное машинное обучение с помощью Scikit-Learn и TensorFlow. Концепции, инструменты и техники для создания интеллектуальных систем. М. : Вильямс, 2018. 688 с.

6. Николенко С., Кадурин А., Архангельская А. Глубокое обучение. Погружение в мир нейронных сетей. СПб. : Питер, 2018. 480 с.

7. Национальная программа «Цифровая экономика Российской Федерации» от 28 июля 2017 г. № 1632-р // Сайт Правительства Российской Федерации [Электронный ресурс] URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yL VuPgu4bv R7M0. pdf (дата обращения: 06.02.2020).

УДК 004.418
ГРНТИ 20.15.05

АВТОМАТИЗИРОВАННАЯ ОБРАБОТКА ЗАЯВОК НА ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ ЮРИДИЧЕСКИХ ЛИЦ

Д. А. Андреев, В. А. Тарасов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлены результаты анализа helpdesk-систем, рассмотрены вопросы автоматизации процесса обслуживания клиентов, выявлены задачи, которые должна решать система автоматизации, на основе чего сформулированы требования к системе, предложены её концепция и общая структура.

аутсорсинг, автоматизация бизнес-процессов, helpdesk.

Проведенный анализ helpdesk-систем показал, что за высокой стоимостью решений стоит обширный функционал, часть которого так и остается невостребованной конечными пользователями, например, в системе OMNITRACKER, в которой наиболее удобны и эргономичны по графическому интерфейсу модуль автоматизации работы с заявками и модуль сопровождения клиентов, присутствует модуль call-центра и модуль мониторинга. Небольшой аутсорсинговой компании вряд ли в работе будет критически необходим модуль мониторинга, но система OMNITRACKER не предоставляет возможности миксования функциональных блоков, это «коробочное» решение, при покупке которого 40 % функций не будут использованы.

Предлагается рассмотреть рациональный набор функциональных требований к программной системе типа helpdesk, основной целью которой является усовершенствование работы аутсорсинг-фирм, в частности модернизация работы технической поддержки сотрудников аутсорсинга, путем внедрения новой автоматизированной информационной системы, которая сможет обеспечить решение ряда следующих задач [1]:

– создание и управление банком активов компании;
– организация работы с юридическими лицами в части предложения аутсорсинговых услуг на договорной основе;
– автоматизация работы с заявками от пользователей;
– управление работой сотрудников;
– планирование экономической эффективности аутсорсинговых услуг.

Исходя из поставленных задач, можно сформулировать минимальные функциональные требования к системе:

– единый интерфейс для всех пользователей;

– интуитивно понятный интерфейс для пользователей;

– стандартный способ регистрации и выдачи заданий инженерам;

– контроль за выполнением работ;

– возможность финансового сопровождения аутсорсинговых услуг.

Таким образом, система должна удовлетворять следующим требованиям:

– ручное заведение заявки – пользователю должна быть доступна функция самостоятельного составления заявки согласно шаблону;

– просмотр заявки – пользователь может просмотреть информацию своей заявки, статус, назначенного инженера и сроки выполнения;

– добавление комментариев к заявке – данная функция необходима пользователю для указания дополнительной информации по технической проблеме, что облегчит работу инженера;

– возможность отклонить заявку – данная функция позволит отклонить некорректно заполненные заявки с указанием необходимых поправок;

– возможность прикрепления файлов к заявке – зачастую пользователю необходимо подкрепить свои слова графическим описанием проблемы; для этого он создает скриншот и прикрепляет его к заявке;

– база знаний по возникавшим ранее ошибкам и проблемам – данный функционал необходим для инженеров;

– просмотр всех заявок;

– установление сроков выполнения заявки руководителем и др.

Более подробно функциональность системы автоматизации представлена на диаграмме (рис. 1). Код приведён на рис. 2 (см. ниже).

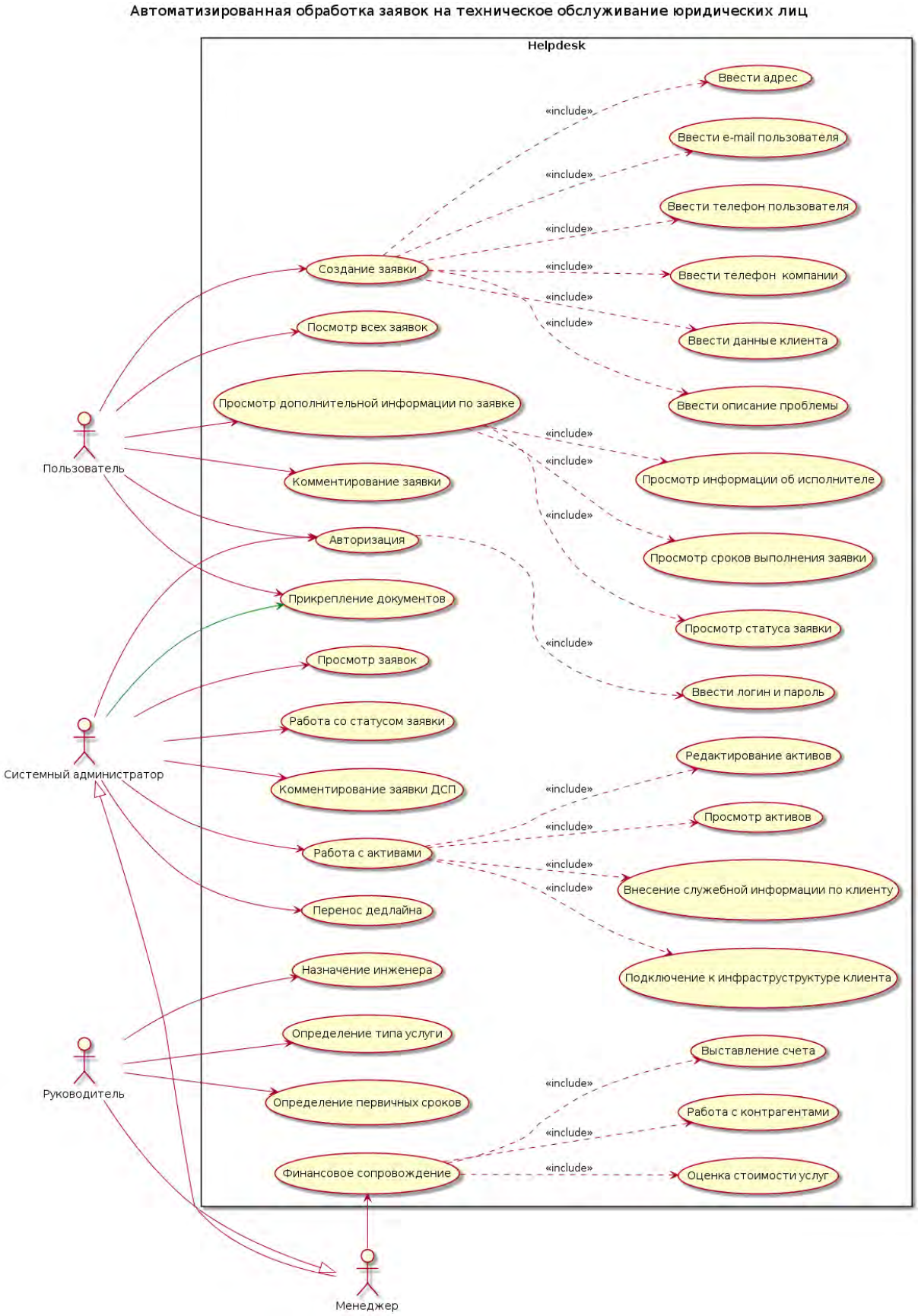


Рис. 1. Use-case-диаграмма системы автоматизации

Для реализации системы автоматизации обработки заявок на техническое обслуживание юридических лиц необходима разработка Web-приложения, что позволит упростить работу с заказчиками, так как для работы с системой заказчику необходим только браузер, а не специальное программное обеспечение, требующее дополнительной установки и ресурсов.

```
@startuml
title Автоматизированная обработка заявок на техническое обслуживание юридических лиц

left to right direction
actor "Пользователь" as A_user
actor "Системный администратор" as A_system
actor "Менеджер" as A_manager
actor "Руководитель" as A_director

rectangle Helpdesk {
A_user --> (Авторизация)
(Авторизация) ..> (Ввести логин и пароль) :<<include>>
A_user --> (Создание заявки)
(Создание заявки) ..> (Ввести описание проблемы) :<<include>>
(Создание заявки) ..> (Ввести данные клиента) :<<include>>
(Создание заявки) ..> (Ввести телефон  компании) :<<include>>
(Создание заявки) ..> (Ввести телефон пользователя) :<<include>>
(Создание заявки) ..> (Ввести e-mail пользователя) :<<include>>
(Создание заявки) ..> (Ввести адрес) :<<include>>
A_user --> (Посмотр всех заявок)
A_user --> (Просмотр дополнительной информации по заявке)
A_user --> (Комментирование заявки)
A_user --> (Прикрепление документов)
(Просмотр дополнительной информации по заявке) ..> (Просмотр статуса заявки):<<include>>
(Просмотр дополнительной информации по заявке) ..> (Просмотр сроков выполнения заявки):<<include>>
(Просмотр дополнительной информации по заявке) ..> (Просмотр информации об исполнителе):<<include>>
A_system <|-- A_manager

A_system --> (Авторизация)
A_system --> (Просмотр заявок)
A_system --> (Работа со статусом заявки)
A_system --> (Комментирование заявки ДСП)
A_system-[#green]-> (Прикрепление документов)
A_system --> (Работа с активами)
(Работа с активами) ..> (Просмотр активов):<<include>>
(Работа с активами) ..> (Редактирование активов):<<include>>
(Работа с активами) ..> (Подключение к инфраструктуре клиента):<<include>>
(Работа с активами) ..> (Внесение служебной информации по клиенту):<<include>>
A_director --> (Определение типа услуги)
A_director --> (Определение первичных сроков)
A_director --> (Назначение инженера)
A_director --|> A_manager
A_system --> (Перенос дедлайна)
A_manager --> (Финансовое сопровождение)
(Финансовое сопровождение)..> (Оценка стоимости услуг):<<include>>
(Финансовое сопровождение)..> (Работа с контрагентами):<<include>>
(Финансовое сопровождение)..> (Выставление счета):<<include>>
}
@enduml
```

Рис. 2. Код UML-диаграммы

Система должна быть представлена на основе трехзвенной клиент-серверной архитектуры: Web-клиент, API (логика) и база данных на сервере. В данном случае реализация архитектуры с помощью API решит две задачи: скорость работы программы и безопасность хранения данных на сервере. Двухзвенная архитектура с прямым подключением к базе данных крайне

не рекомендуется, так как это сделает программный продукт не защищенным от внешних вторжений.

База данных позволит хранить данные о заявках, заказчиках, активах заказчиков и базу знаний для инженеров. Финансовые операции будут проводиться через продукт «1С:Бухгалтерия», модуль интеграции с данной системой предполагается реализовать в дальнейшем [2].

Зачастую для автоматизации того же Help Desk используется электронная почта или Excel, совершенно для этого не предназначенные. Такой инструментарий работает неэффективно. Причем, чем больше масштабы бизнеса, тем серьёзнее на результате сказываются недостатки инструмента.

На старте достаточно сложно оценить экономический эффект от вложения в автоматизацию, тем более, если речь идет о системах клиентской поддержки. Чтобы оценить эффект, необходимо собрать статистику и сравнить её с текущими данными, но при этом текущие данные почти никто не собирает (сравнить не с чем). В данном случае поможет опыт коллег по рынку. Например, опыт внедрения системы службы поддержки в компании по автоматизации общепита и HoReCa [3].

Небольшим компаниям, особенно в начале развития, удобнее не тратить время на внедрение helpdesk-систем, не приносящих на данной стадии заметной пользы. Однако при масштабировании важно не упустить тот момент, когда отсутствие системы службы поддержки будет якорем, то есть когда заявки начнут теряться из-за того, что существующая система учета (будь то бумажный журнал, канал в Viber или цепочки писем в ящике электронной почты) перестанет справляться с нагрузкой.

Внедрение данной системы позволит автоматизировать обработку заявок на техническое обслуживание юридических лиц, что ускорит работу аутсорсинговой компании. Разработка собственной системы позволит сократить затраты на внедрение программы автоматизации обработки заявок.

Список используемых источников

1. Недякин М. Искренний сервис. М. : Манн, Иванов и Фербер, 2018. 180 с.

2. ГОСТ 34.601-90. Автоматизированные системы. Стадии создания. М. : Стандартинформ, 2009. 6 с.

2. Предпосылки, сложности и результаты внедрения Help Desk системы для партнёра IIKO [Электронный ресурс] // Рекомендации от экспертов. Блог Okdesk. URL: https://okdesk.ru/blog/restaudit (дата обращения: 21.03.2020).

Статья представлена заведующим кафедрой ИУС СПбГУТ, доктором технических наук, профессором Л. К. Птицыной.

УДК 004.4, 519.85
ГРНТИ 20.23.27

ИНФОРМАЦИОННАЯ СИСТЕМА АНАЛИЗА ДОРОЖНОЙ СИТУАЦИИ НА ОСНОВЕ ДАННЫХ СЕРВИСА YANDEX.MAPS

В. Ю. Аронов, М. А. Вержаковская

Поволжский государственный университет телекоммуникаций и информатики

Информационная система позволяет оперативно анализировать дорожную ситуацию и принимать решения о формировании и изменении маршрута передвижения. Результаты данной работы в дальнейшем могут быть внедрены в различных организациях, которые занимаются логистической деятельностью, а также применяться в домашних и личных целях пользователей.

информационная система, анализ, методы оптимизации, дорожная ситуация, Yandex.Maps.

В повседневной жизни все большую ценность приобретает такой ресурс, как время. Люди стараются свести к минимуму затраты времени на самые различные виды деятельности, непрерывно продолжая создавать всё больше автоматизированных информационных систем, позволяющих решать задачи по оптимизации всевозможных процессов любой сложности, в том числе анализ дорожной ситуации и построение оптимальных маршрутов передвижения.

В данной работе проведен обзор и анализ геосервисов для работы с маршрутами, описано проектирование системы анализа дорожной ситуации, разработка информационной системы анализа дорожной ситуации, функциональные возможности информационной системы анализа дорожной ситуации.

При проектировании информационной системы были выявлены следующие типы информации: требования к разрабатываемой информационной системе, анализ данных для обработки в информационной системе сервиса Yandex.Maps, выбор программных средств для разработки, общая постановка задачи анализа дорожной ситуации.

Для написания программного кода использовался кроссплатформенный текстовый редактор SublimeText 3. Для контроля версий и деплоймента на удаленный сервер – система git.

Готовое приложение загружается на удаленный виртуальный сервер хостера DigitalOcean с установленной операционной системой Ubuntu 12.04

x32 и сервером nginx в качестве HTTP-сервера. Доступ к серверу осуществляется по протоколу SSH, в качестве клиента используется программа-терминал iTerm.

Информационная система позволяет оперативно анализировать дорожную ситуацию и принимать решения о формировании и изменении маршрута передвижения.

Результаты данной работы в дальнейшем могут быть внедрены в различных организациях, которые занимаются логистической деятельностью, а также применяться в домашних и личных целях пользователей.

При разработке информационной системы в рамках данной научной работы в качестве основного источника данных используется картографический сервис Yandex.Maps (Яндекс-карты). Существует множество различных картографических гео-сервисов, предоставляющих доступ к собственным методам и данным, необходимых для работы разрабатываемой в рамках данной научной работы системы, таких как Yandex.Maps, Google.Maps, OSM, 2Gis и другие, однако Яндекс-карты для этого подходят наилучшим образом по следующим причинам:

– сервис представляет самые точные и актуальные данные о текущей дорожной ситуации;

– сервис имеет очень удобный и подробно документированный JavaScript API на русском языке, предназначенный для клиентских web-приложений;

– API сервиса предоставляет методы построения автомобильных маршрутов, возвращая детальную информацию о маршруте;

– возможность выбора удобного формата данных для работы с методами API, среди которых JSON и объекты JavaScript, работа с которыми по умолчанию поддерживается интерпретатором языка JavaScript.

Разрабатываемая система решает задачу поиска кратчайшего маршрута между заданными точками, что является одной из самых популярных задач в области комбинаторики, которая носит название задачи коммивояжера (*travelling salesman problem*), суть которой заключается в посещении географических точек [1].

Существует целый ряд алгоритмов решения задачи коммивояжера, имеющих те или иные недостатки, связанные со сложностью реализации, производительностью, точностью результата и так далее. Одним из самых точных методов решения задачи коммивояжера является метод полного перебора, то есть алгоритм, в котором подряд проверяются все возможные варианты маршрутов между всеми точками и на каждой итерации полученный результат сравнивается с найденным на данный момент оптимальным и принимается за оптимальный в случае, если оказывается короче, чем существующий [2, 3]. Этот алгоритм в противовес своей простоте и точности

имеет очень большой недостаток: количество вариантов, которые нужно перебрать при поиске решения равно факториалу количества заданных точек, что очень сильно ограничивает объемы обрабатываемых данных.

При построении маршрута обязательно учитывается актуальная дорожная ситуация, маршрут строится с учетом пробок на дорогах, возникших в результате интенсивного потока машин, ДТП или дорожных работ. Если пользователь предпочтет оптимизировать маршрут по времени, алгоритм должен учитывать время, исходя из актуальных данных о пробках, которые перед каждым новым пересчётом должны обновляться. В случае расчета времени перемещения пешком или на велосипеде, пробки учитываться не должны.

Ниже представлен общий алгоритм с коротким описанием каждого действия, необходимого для реализации функционала решения поставленной задачи:

1) Инициализация всех модулей приложения.

При загрузке приложения инициализируются модули путём последовательного подключения браузером. Подключаемые модули описаны в заглавном модуле, загружающимся в самом начале и выполняющим роль пользовательского интерфейса.

2) Получение геопозиции пользователя.

Выполняется с помощью дополнительного модуля, обращающегося к специальной службе браузера с запросом использования геопозиции. Полученный результат может использоваться в вычислениях в качестве стартовой точки.

3) Задание набора маршрутных точек.

Осуществляется с помощью собственных соответствующих методов разрабатываемой системы, которые в свою очередь вызываются обработчиками элементов пользовательского интерфейса. При добавлении точек вызывается метод геокодирования API Яндекса для получения адреса по координате и наоборот.

4) Получение данных от маршрутизатора Яндекса.

При последовательных запросах к API Яндекс-карт собираем информацию о маршрутах между каждой возможной парой точек. Данные передаются по HTTP-протоколу с помощью соответствующих JavaScript-методов API Яндекса.

5) Предварительная обработка данных.

Полученные данные итеративно собираются в объект в памяти в виде двумерного массива весов.

6) Поиск оптимального решения.

Используя заранее сформированный массив весов, итеративно перебираются все возможные комбинации путей между заданными маршрутными точками, найденный на каждой итерации путь сравнивается с запомненным

в результате работы предыдущих итераций и перезаписывается в случае, если является более оптимальным.

7) Визуализация полученного решения.

Полученный маршрут и информация по нему отображается на карте соответствующими методами карты и в интерфейсе приложения, не связанного с картой, с помощью соответствующих методов приложения.

Опираясь на постановку задачи и возможные варианты работы с данными, разработана простая модульная схема приложения, позволяющая легко подключать дополнительные модули и вносить изменения в существующие модули.

Обобщенная файловая структура информационной системы анализа дорожной ситуации на основе данных сервиса Yandex.Maps приведена в таблице.

ТАБЛИЦА. Обобщенная файловая структура информационной системы анализа дорожной ситуации на основе данных сервиса Yandex.Maps

Директория	Файл	Краткое описание
/	index.html	Выполняет функции пользовательского интерфейса
/scripts	main.js	Связующее звено между пользовательским интерфейсом и остальными модулями системы
/scripts	lib.js	Набор основных и вспомогательных функций приложения
/scripts	jquery-1.11.0.min.js	Библиотека, упрощающая работу с элементами пользовательского интерфейса
/scripts	geolocation-service.js	Библиотека для получения геопозиции пользователя от соответствующей службы браузера
/styles	style.css	Описание стилей пользовательского интерфейса
/images	—	Статичные изображения для пользовательского интерфейса

Центральной частью всего веб-приложения является файл index.html, расположенный в корне проекта. Он загружается первым и к нему подключаются все остальные модули и стили, как локальные, так и удалённые. Для пользователя играет роль пользовательского интерфейса.

В файле /scripts/main.js является центральным для части скриптов, в нём производятся обращения ко всем подчинённым модулям, и осуществляется их связь с пользовательским интерфейсом.

Файл /scripts/lib.js содержит основные и самые важные функции, разрабатываемые в рамках дипломной работу и предоставляющие основной функционал. Функции представлены в виде методов javascript-объектов, разбитых на три категории:

– функции работы с маршрутами (объект routes);

– функции работы с геоточками (объект points);
– вспомогательные функции (объект utils).

Файлы jquery-1.11.0.min.js и geolocation-service.js являются сторонними библиотеками и подключаются для расширения возможностей и упрощения доступа к геолокационному сервису Яндекса и службам браузера.

В файле /styles/style.css на языке CSS описаны стили элементов, представленных на заглавной web-странице index.html. В верстке элементов соблюдаются требования кроссбраузерности и мобильности, а также применены техники адаптивной вёрстки для разных разрешений экранов.

На рис. 1 представлена схема взаимодействия основных модулей информационной системы анализа дорожной ситуации на основе данных сервиса Yandex.Maps, описанных выше.

Рис. 1. Схема взаимодействия основных модулей информационной системы анализа дорожной ситуации на основе данных сервиса Yandex.Maps

Все необходимые для работы данные и объекты хранятся в памяти браузера, при необходимости обновляются или очищаются. При инициализации приложения объявляются и создаются все необходимые переменные и объекты в глобальной области видимости. Все остальные переменные объявляются внутри функций и доступны внутри них же только во время выполнения функции, после чего очищаются из памяти.

Приложение предназначено для работы в любой операционной среде с наличием доступа в интернет и современным браузеров, соответствующим последним стандартам W3C.

Приложение разработано с применением техники адаптивной верстки и с использованием универсальных кроссбраузерных возможностей языка JavaScript и библиотек, поэтому одинаково выглядит и работает, как на настольных компьютерах и ноутбуках, так и на планшетных компьютерах и телефонах с различными современными операционными системами.

Такая мобильность позволяет пользователю не быть привязанным к месту, и иметь возможность получить актуальные данные и при необходимости перестроить маршрут практически в любом месте, если у него под рукой есть мобильный телефон или планшетный компьютер с доступом в интернет.

На рис. 2 и рис. 3 приведены примеры запущенного приложения на мобильном устройстве. Интерфейс приложения состоит из двух основных частей: информационного блока слева и блока параметров и управления справа. Левая часть занимает две трети окна и имеет два режима отображения: графический в виде карты и текстовый в виде блока текста.

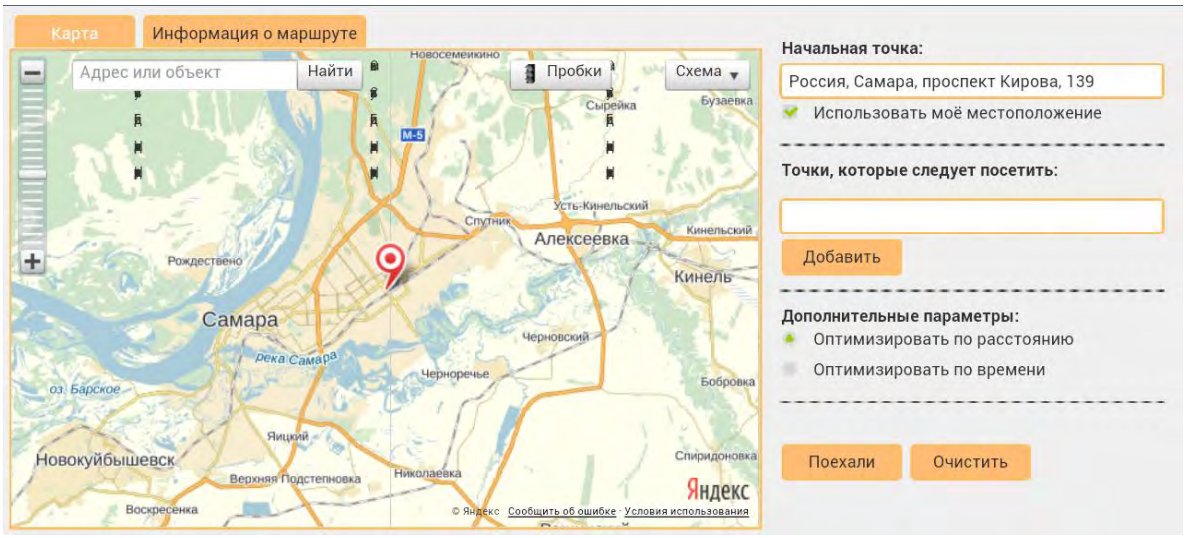


Рис. 2. Пример запущенного приложения на мобильном устройстве

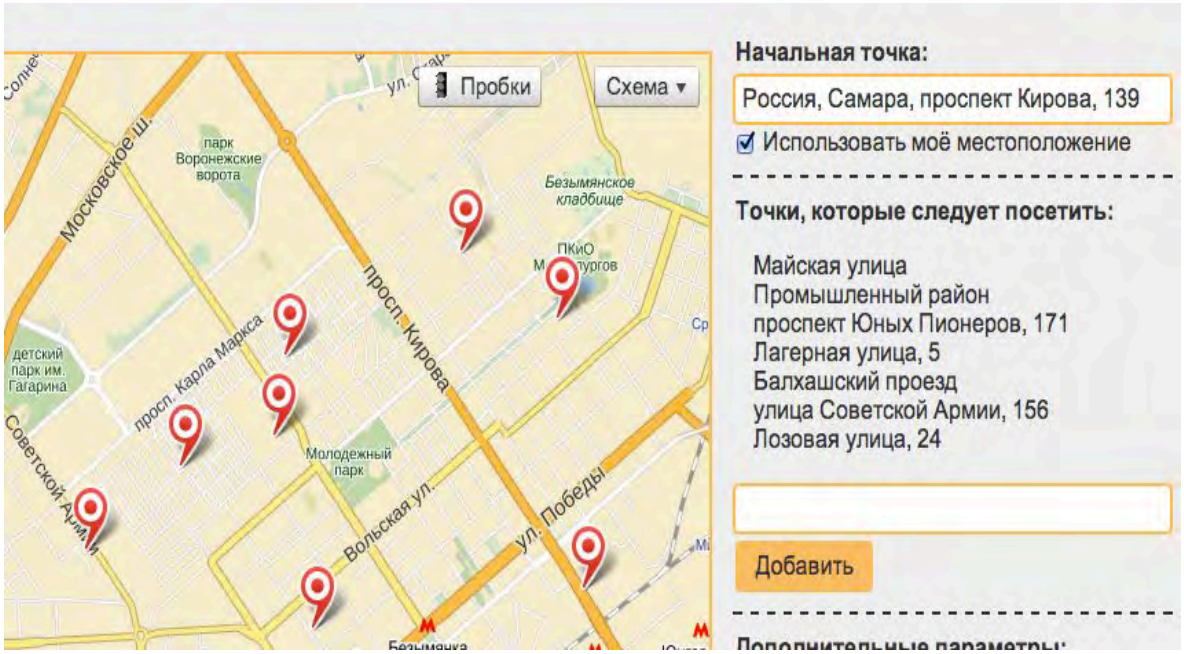


Рис. 3. Заполненный список маршрутных точек

Правая часть занимает оставшееся место и предоставляет пользователю следующие элементы интерфейса: поле для ввода стартовой точки, переключатель использования собственной геопозиции, список маршрутных точек (изначально пустой), поле ввода адреса и кнопка добавления новой маршрутной точки, дополнительные параметры маршрута, кнопки расчета и очистки данных маршрута.

Список используемых источников

1. Тарасов В. Н., Бахарева Н. Ф. Математическое программирование. Теория. Алгоритмы. Программы. Оренбург : ИПК ОГУ, 2007. 222 с.

2. Новиков Ф. А. Дискретная математика для программистов : учебник для вузов. 3-е изд. СПб. : Питер, 2009. 384 с.

3. Аттетков А. В., Зарубин В. С., Канатников А. Н. Методы оптимизации : учебное пособие. М. : ИЦ РИОР, НИЦ Инфра-М, 2013. 270 с.

УДК 004.451
ГРНТИ 81.93.29

СРАВНЕНИЕ МЕХАНИЗМОВ БЕЗОПАСНОСТИ РАЗЛИЧНЫХ ВЕРСИЙ ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID

В. Д. Атанов, А. В. Красов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматриваются возможности безопасности версии Андроид 7.0 относительно других версий операционной системы, а также рассмотрены и представлены возможные реализации некоторых уязвимостей.

*Linux kernel, applications, android framework, android runtime, Address Space Layout Randomization (ASLR), **A**pplication **P**rogramming **I**nterface (API), Transport Layer Security (TLS), Service Discovery Protocol (SDP), Bytecode Viewer, Manifest, Common Language Runtime (CLR).*

Android – это операционная система с открытым исходным кодом для мобильных устройств. Соответствующий проект с открытым исходным кодом возглавляет Google. Этот сайт – Android Open Source Project (AOSP) репозиторий предлагает информацию исходный код, необходимый для создания пользовательских вариантов ОС Android (рис. 1, 2), порт устройства и аксессуары для платформы Android, а также обеспечить соответствие

устройств требования к совместимости, которые сохраняют экосистему Android здоровой и стабильная среда для миллионов пользователей.

В мобильной платформе Google на сегодняшний день обнаружено множество ошибок. Некоторые из этих багов представляют собой полноценные уязвимости и могут использоваться как для несанкционированного доступа к файловой системе смартфона, так и для распространения вредоносного ПО [1].

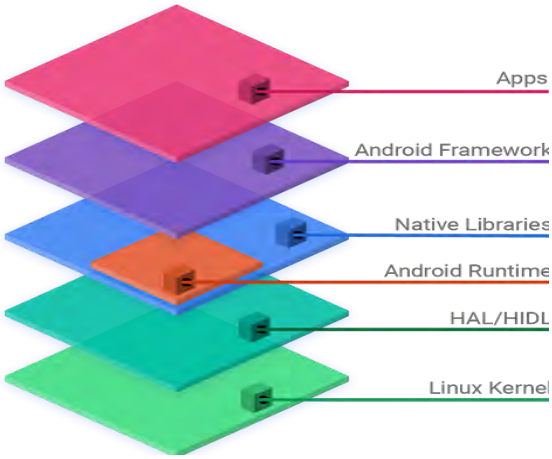


Рис. 1. Структура ОС Android

Рис. 2. Стек программного обеспечения для Android

Каждый выпуск Android включает в себя десятки улучшений безопасности для защиты пользователей. Вот некоторые из основных улучшений безопасности, доступных в Android 7.0:

- *Шифрование на основе файлов.* Шифрование на уровне файлов, вместо того, чтобы шифровать всю область хранения как один блок, лучше изолирует и защищает отдельных пользователей и профили на устройстве.
- *Прямая Загрузка.* Включено шифрованием на основе файлов, прямая загрузка позволяет некоторым приложениям, таким как будильник и специальные возможности, чтобы запустить, когда устройство включено, но не разблокировано.
- *Проверенная Загрузка.* Проверенная загрузка теперь строго применяется к предотвращению загрузке скомпрометированных устройств; она поддерживает исправление ошибок до повышения надежности защиты от несанкционированного повреждения данных.
- *SELinux.* Обновлена конфигурация SELinux, seccomp дополнительно блокирует изолированную программную среду приложения и уменьшает риск атаки.

• *Загрузка библиотеки-рандомизация порядка и улучшенный ASLR.* Повышенная случайность делает некоторые атаки повторного использования кода менее надежными.

• *Защита ядра.* Добавлена дополнительная защита памяти для более новых ядер путем маркирования части памяти ядра, как только для чтения, ограничивая доступ ядра к адресам userspace и дальнейшее предотвращение существующей атаки [2].

• *Схема подписи APK v2.* Введена подпись целого файла схема, которая улучшает скорость проверки и усиливает гарантии целостности.

• *Доверенный магазин CA.* Чтобы упростить управление приложениями, доступ к их защищенному сетевому трафику, установленным пользователем центром сертификации, которые установлены через API администратора устройства больше не доверяют по умолчанию для приложений, ориентированных на уровень API 24+. Кроме того, все новые устройства на Android должны загружать приложения с таким же доверенным магазином CA.

• *Конфигурация Сетевой Безопасности.* Настройка сетевой безопасности и протокола TLS через декларативный конфигурационный файл [3].

Согласно информации с сайта cvedetails.com, на сегодняшний день в Android насчитывается 2146 уязвимостей (рис. 3), при этом число выявленных багов начало экспоненциально расти примерно с 2014 года.

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2009	5	3								1					
2010	1	1	1												
2011	9	1	1		1					3	2	3			
2012	8	5	4	2							1				1
2013	7	1	2	2	2					1	1	3			
2014	13	2	4	1		1				1	2	2			1
2015	125	56	70	63	46					20	19	17			
2016	525	106	73	92	38					48	99	250			
2017	842	87	206	162	32			1		31	115	36			
2018	611	32	84	150	12	3	1	1		17	64	3			
Total	2146	294	445	472	131	4	1	2		122	303	314			2
% Of All		13.7	20.7	22.0	6.1	0.2	0.0	0.1	0.0	5.7	14.1	14.6	0.0	0.0	

Рис. 3. Уязвимости

Самая первая уязвимость Android была обнаружена еще в октябре 2008 года в прошивке коммуникатора HTC T-Mobile G1. При просмотре веб-страниц с определенным содержимым ошибка в ПО позволяла выполнить вредоносный код, отслеживающий использование клавиатуры гаджета (рис. 4). Теоретически таким образом можно было реализовать кейлоггер, фиксирующий нажатия кнопок, и собирать вводимую пользователем при веб-серфинге информацию. Эта уязвимость представляла опасность только для одной-единственной модели коммуникатора, но само ее наличие наглядно

показало: Android – не настолько безопасная и защищенная система, как считалось ранее [4].

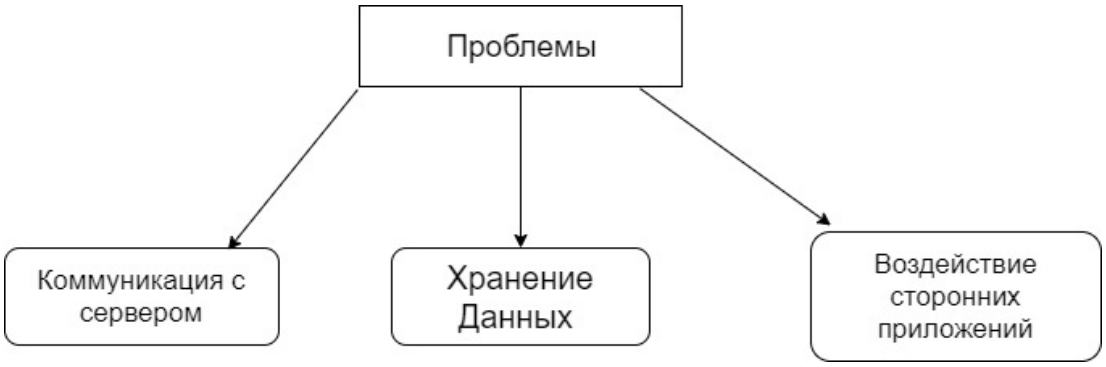


Рис. 4. Проблемы ОС

Вспомогательный софт отчасти помогает решать некоторые проблемы.

Bytecode Viewer – это расширенный облегченный Java-инструмент для обработки байтов, GUI Java Decompiler, GUI-редактор байт-кода, графический интерфейс пользователя Smali, GUI Baksmali, редактор GUI APK, редактор графического интерфейса GUI, графический пользовательский дескриптор GUI, графический интерфейс DEX Decompiler, графический интерфейс Procyon Java Decompiler, графический интерфейс пользователя Krakatau, GUI CFR Java Decompiler, GUI FernFlower Java Decompiler, GUI DEX2Jar, GUI Jar2DEX, GUI Jar-Jar, Hex Viewer, Code Searcher, Debugger и многое другое.

Файл MANIFEST – это XML-документ, который позволяет описывать манифест или содержимое пакета программного обеспечения Windows. Он используется различными технологиями Windows для настройки и развертывания программного обеспечения, включая ClickOnce и Common Language Runtime (CLR). Файлы MANIFEST часто видны с расширением файла .exe.manifest (рис. 5).

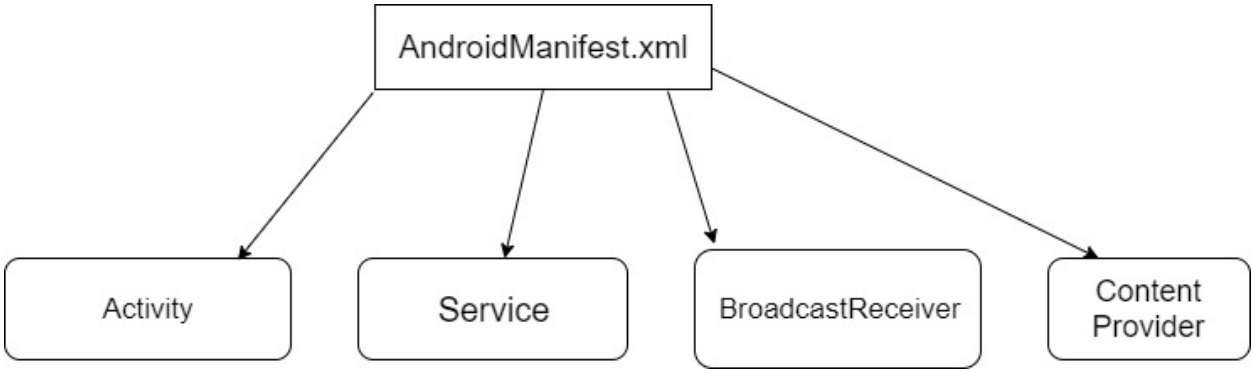


Рис. 5. Состав AndroidManifest.xml

Пример уязвимости Яндекс почты: использование публичного BroadcastReceiver, т. е. злоумышленник может послать любой broadcast, подобрать IP-адресс письма и, к примеру, удалить его (рис. 6).

```
<receiver android:name=«…NotificationBarBroadcastReceiver">
    <intent-filter android:priority="1">
        <action android:name=«…notification.create" />
        <action android:name=«…notification.delete" />
        <action android:name=«…notification.folder.delete" />
        <action android:name=«…notification.message.read" />
        <action android:name=«…notification…archive_delete» />
        <action android:name=«…notification.drop» />
        <action android:name=«…notification.restore» />
    </intent-filter>
</receiver>
```

Рис. 6. Компрометация уведомлений

Решение проблемы (рис. 7): не экспортировать компоненту, либо защитить доступ к ней по Permission [5].

```
<receiver android:name=«…NotificationBarBroadcastReceiver»
          android:permission="com.yandex.mail.permission.write"
          android:exported="false">
```

Рис. 7. Решение проблемы

В зависимости от требований к приватности хранимых данных в Android можно использовать:

- ✓ SharedPreferences
- ✓ Internal Storage
- ✓ External Storage
- ✓ Default DB (SQLite)
- ✓ SQLCipher
- ✓ Custom Database
- ✓ Network

На Google I/O сообщили, что порядка 80 % устройств под управлением Android 7 и порядка 25 % под управлением Android 6 зашифрованы.

Что это означает на практике? Сравним распространенность версий Андроид с данными о шифровании:

– Android 5.1.1 и более старые: ~62 % рынка (данных о шифровании нет);

– Android 6: 0,31 (31 % рынка) * 0,25 = 0,078;

– Android 7: 0,07 (7 % рынка) * 0,80 = 0,056.

Итого получаем цифру в 13,4 %. Это – число устройств на Android, которые точно зашифрованы. Основная заслуга здесь принадлежит Google, которая заставила производителей устройств, выходящих с Android 6 или 7 на борту, обязательно активировать шифрование [6].

Список используемых источников

1. Официальный сайт, защита устройства на андроид. URL: https://source.android.com/security
2. Официальный сайт, улучшения безопасности в андроид 7.0. URL: https://source.android.com/security/enhancements/enhancements70
3. Официальный сайт, улучшения безопасности в андроид 6.0. URL: https://source.android.com/security/enhancements/enhancements60
4. Статья, уязвимости в операционной системе андроид. URL: https://xakep.ru/2019/02/07/forgotten-android/
5. Доклад Яндекс, безопасность андроид приложений. URL: https://www.youtube.com/watch?v=6Xj54AdvSls
6. Статья, сравнительная характеристика по версиям. URL: http://www.spy-soft.net/bezopasnost-android/

УДК 654.739
ГРНТИ 71.01.85

ОСОБЕННОСТИ ВНЕДРЕНИЯ СИСТЕМЫ ИНТЕГРАЦИОННОЙ ШИНЫ ДАННЫХ, ПОСТОЕННОЙ НА ПЛАТФОРМЕ 1С В СПбГУТ

Ю. С. Ахметова, В. О. Долгун, Д. Б. Казаков, М. Ю. Пацкан

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье продемонстрированы проблемы и особенности внедрения системы ИШД (Интеграционная шина данных) реализованной на платформе 1С. Внедрение системы ИШД состоит из нескольких этапов: проведение обследования внедряемой области, подготовка и настройка инфраструктуры, установка ИШД, проведение приёмо-сдаточных испытаний, обучение и консультирование работников, проведение опытной эксплуатации. Цель внедрения – повышение эффективности деятельности за счет автоматизации бизнес-процессов университета.

интеграционная шина данных, цифровизация, автоматизация, 1С, университет, бизнес-процесс, образование.

На текущий момент эффективная работа любого современного предприятия во многом зависит от скорости обработки информации, необходимостью распределения между подразделениями организации, а также от надежности информационной составляющей. В связи с этим, все чаще встает вопрос об модернизации и цифровизации бизнес – процессов учебного заведения.

На сегодняшний день ИШД является новым программным продуктом на рынке IT, предоставляющий организациям возможность автоматизировать ее бизнес – процессы, объединяя их в единое информационное пространство.

На сегодняшний день ни одна бюджетная или коммерческая организация не обходится без таких систем, как 1С:Бухгалтерия, 1С:Зарплата и управление персоналом, 1С:Университет или аналогичная система и многие другие системы, которые свойственны организации (рис. 1).

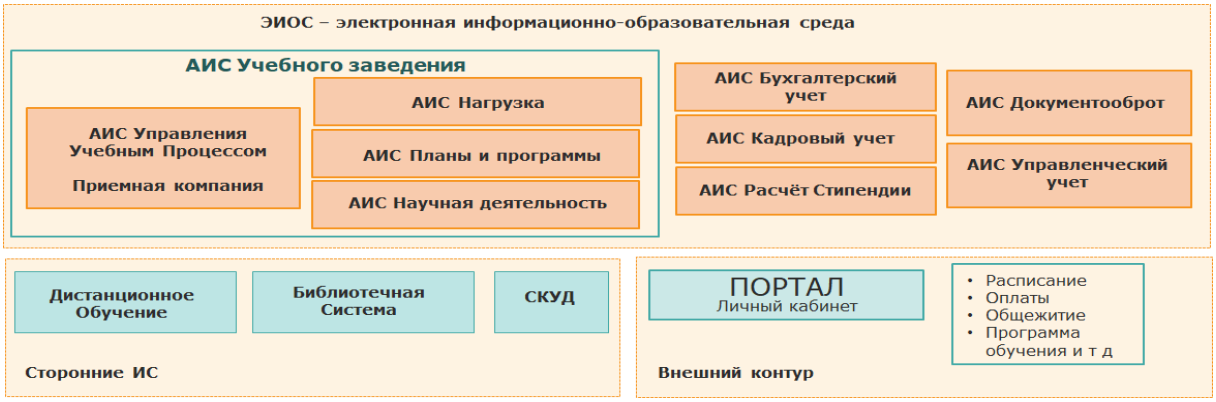


Рис. 1. Схема типовой инфраструктуры ВУЗа

Цифровизация деятельности предприятия заключается в оптимизации бизнес – процессов университета, а также повышении контроля принимаемых управленческих решений.

ИШД представляет собой программный продукт, позволяющий объединять большое число информационных систем, а также организовать взаимодействие между ними на основе сервисов [1]. Для обмена через ИШД можно использовать универсальный типовой адаптер, предназначенный для ИС, разработанных на базе платформы 1С 8.3. Адаптер – функционал, позволяющий производить интеграцию ИШД с информационными системами, может быть встроен в информационную систему или выступать в роли отдельного модуля (рис. 2, см. ниже). Его основной функцией является корректная отправка и принятие пакетов данных. Взаимодействие с информационными системами осуществляется с помощью адаптеров. Данный механизм встраивается в конфигурацию для связи с ИШД, но при этом не изменяет саму структуру ИС, в которую внедряется, сохраняя возможность поддержки разработчиков 1С.

Основными задачами и целями внедрения ИШД являются:

– создание единой точки входа;

– организация многопоточного обмена данными;

– анализ данных между однородными и гетерогенными системами;

– работа с нормативно – справочной информацией;

– сервис, позволяющий объединить внешние ИС, использующие MS SQL, MySQL, PostgreSQL.

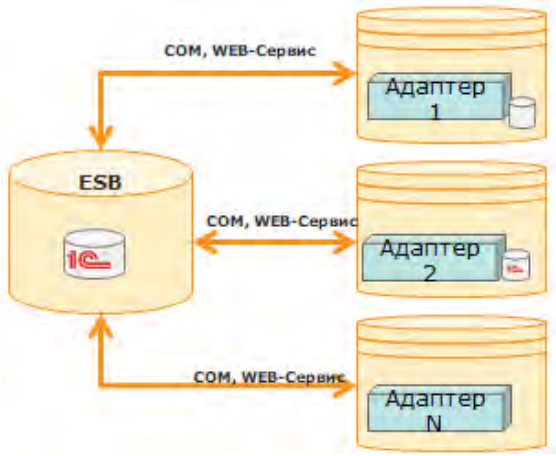


Рис. 2. Схема встраиваемого адаптера

Проблемы, которые требовалось решить с помощью ИШД:

– наличие не связанных друг с другом разнородных систем. Возникновение в связи с этим неактуальных данных;

– вероятность возникновения дублирования данных при объединении всех систем;

– отсутствие централизованного сервиса по контролю внесенной информации, возникновение дублей;

– необходимость отдельного занесения одних и тех же данных в несвязанных системах;

– отсутствие систематизированного подхода к администрированию;

– отсутствие контроля процессов обмена;

– отсутствие единого контролирующего звена, которое было бы ответственное за актуальность предоставленных данных из различных информационных систем;

– отсутствие статистических данных.

При выборе интеграционной шины данных был произведена оценка рынка. На ранке представлено огромное количество enterprise service bus, которые имели большое количество коннекторов к различным системам, как 1С, так и сторонним системам.

Причины выбора программного продукта ИШД от ГК Омега, созданной на платформе 1С:

– наличие рекомендованной схемы объединения основных 1С систем: БГУ, ЗКГУ, ДО, Омега.ПФУ и Университет;

– сервис, позволяющий объединить внешние информационные системы, посредством использования встраиваемых модулей в MS SQL, MySQL, PostgreSQL, Firebird;

– работа с нормативно – справочной информацией (хранение/обмен/управление правами на редактирование/создание/удаление);

– наличие единой точки входа, то есть централизованное управление пользователями и их правами в ИС;

– многопоточный обмен данными – анализ данных, обмен между однородными и гетерогенными системами, отчет по состоянию и статистике обмена;

– предоставление рекомендованной схемы потоков данных для учебных заведений, включающей в себя основные ИС используемых в организации.

Программный продукт ИШД позволяет осуществлять контроль за всеми процессами ИС, которые протекают через шину[2], настраивая внутреннюю матрицу отправителей и получателей, отслеживая их статус, и текст ошибки при ее наличии. При обследовании была составлена матрица потоков, часть из которой представлено на рис. 3 (см. ниже).

На данной матрице потоков (см. рис. 3) представлено в каких случаях ИС является источником или получателем.

В процессе внедрения составлена структура работы всех сущностей СПбГУТ на основе представленной матрицы потоков. Благодаря имеющимся документам – Схема потоков и Матрица потоков, быстро был разработан план настройки системы под СПбГУТ. Обследование было основано на сравнении текущих систем СПбГУТ и эталонных схем потоков, предоставленных в Матрице. В ИС требовалось скорректировать реквизитный состав (поля), а также присоединить список сущностей к ИШД.

На рис. 4. (см. ниже) представлено направление сущностей в одностороннем и в двухстороннем порядке. Пример односторонней сущности – «28 поток «Сотрудники» из ИС 1С:ЗКГУ в ИС 1С:ДО», а двухсторонней – «34 поток «Контрагенты» ИС 1С:БГУ и ИС 1С:ДО».

Итогами внедрения при совместной работе группы сопровождения разработок и внедрения университета телекоммуникаций и специалистов «ГК Омега» стали:

– уменьшение времени определения коллизий и причин возникновения до пяти минут;

– уменьшение времени присоединения в обмен нового объекта с указанием отправителей и получателей для ИС с одинаковой структурой до десяти минут;

– уменьшение времени централизованной блокировки изменений в справочниках до пяти минут;

– уменьшилось время на создание и назначение прав учетной записи; уменьшилось время на проведение анализа состояния обмена, анализа загрузки данных и очереди разбора до десяти минут.

№	Сущность/ИС	Ключевое поле	БГУ	ЗКГУ	ЗКГУ стип	УНТ	ДО	Комментарии
1	Организации	УИД, Наименование, ИНН, КПП	И	П	П	П	П	В УНТ интегрируется со справочниками "Контрагенты", "Структура университета", документ "Формирование структуры университета", регистр сведений "Данные об организации"
2	Виды контакной информации		И	П	П	П	П	
3	Контрагенты	УИД, ФИО, ИНН, СНИЛС, доп. Реквизит	И/П	И			И/П	ЗКГУ - источник для БГУ для отражения удержаний по исполнительным Листам и проф взносам
4	Статьи финансирования	УИД, Наименование	И	П	П			
54	Способ отражения зарплаты в бух учете		И	П	П			Необдима для корректного обмена по Отражению зарплаты в бух. Учете. Есть в стандартном обмене.
19	Кадровая история			И	И	И/П		УНТ - источник для ЗКГУ стип
20	Штатное расписание			И			П	только в части конретных признаков для определения руководителя подразделения
21	Отражение зарплаты в бухучете бюджетных организаций		П	И	И			Стандартный обмен ЗКГУ - БГУ
22	Начисление оценочных обязательств по отпускам		П	И				Стандартный обмент ЗКГУ - БГУ
23	Военкоматы			И	П	П/И		УНТ-источник для ЗКГУ стип
24	Отношение к воинской обязанности			И	И	П		
25	Годность к воинской службе			И	И	П		
26	ВУС			И	И	П		
27	Воинский учет			И	П	П/И		УНТ-источник для ЗКГУ стип
28	Ученые степени физических лиц			И	П	П/И		УНТ-источник для ЗКГУ стип
29	Ученые звания физических лиц			И	П	П/И		УНТ-источник для ЗКГУ стип
30	Кадровое движения			И	П	П/И		УНТ-источник для ЗКГУ стип
31	Табель учета рабочего времени			П		И		из УНТ передаются документы "Посещаемость", "Ведомость"

Рис. 3. Матрица потоков СПбГУТ

Рис. 4. Схема потоков ИС СПбГУТ

Список используемых источников

1. Шаппелл Д. А. ESB – Сервисная Шина Предприятия. СПб. : БХВ-Петербург, 2008. 345 с.

2. Лесневская С. В. Автоматизация управления вузом на базе технологий класса ERP // Информатизация образования и науки. 2010. № 5. С. 114–126.

УДК 004.891.2
ГРНТИ 20.23.17

ИНТЕЛЛЕКТУАЛИЗАЦИЯ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ОБЛАСТИ ФИНАНСОВОГО АНАЛИЗА КРЕДИТНЫХ ОРГАНИЗАЦИЙ

А. В. Бабаева, В. Л. Литвинов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Финансовая стабильность банковского сектора и страны в целом во многом зависит от эффективного банковского регулирования и надзора. При анализе финансового состояния кредитных организаций в расчет принимается огромный массив данных. При принятии решений о применении мер надзорного реагирования, классификации, выборе дальнейшей стратегии регулирования деятельности кредитных организаций кураторами анализируется множество различных показателей и нормативов. Внедрение новых интеллектуальных технологий анализа данных позволит повысить эффективность работы надзорного блока банковских организаций.

банковский надзор, анализ финансового состояний кредитных организаций, интеллектуальные системы поддержки принятия решений.

Информационные технологии и инновации становятся неотъемлемой частью банковского сектора, оптимизируя операционные процессы банков.

Системы поддержки принятия решений активно используются в коммерческих банках, выполняя следующие функции:

– анализ финансового состояния потенциальных заемщиков;
– определение маркетинговой политики банка;
– управление финансовыми показателями банка и другие.

В настоящее время перед участниками финансового рынка и Центральным банком стоят принципиально новые задачи, обусловленные появлением новых бизнес-моделей и стремительным развитием цифровых технологий, в том числе технологий машинного обучения, обработки больших данных, распределенных реестров, открытых интерфейсов, а также облачных технологий. Одновременно с использованием новых технологических решений при предоставлении востребованных финансовых продуктов и услуг, а также повышением эффективности взаимодействия с клиентами в новой цифровой среде целесообразно применять цифровые технологии для упрощения, удешевления и повышения качества функций, связанных с исполнением регуляторных требований [1].

В работе рассматриваются основные задачи, которые могут быть решены при внедрении интеллектуальных систем поддержки принятия решений в Центральном банке Российской Федерации в области финансового анализа кредитных организаций.

Интеллектуальный анализ данных обычно определяют, как метод поддержки принятия решений, основанный на анализе взаимозависимостей между данными [2].

Обычный анализ отчетов, построенный по базе данных, также может рассматриваться как разновидность интеллектуального анализа данных.

Существует два подхода к автоматизации поиска зависимостей между данными. В первом случае пользователь сам выдвигает гипотезы относительно зависимостей между данными. Традиционные технологии анализа развивали именно этот подход. Действительно, гипотеза приводила к построению отчета, анализ отчета к выдвижению новой гипотезы и т. д. Это справедливо и в том случае, когда пользователь применяет такие средства, как OLAP, поскольку процесс поиска по-прежнему полностью контролируется человеком. В этом процессе автоматизирована проверка достоверности гипотез, что позволяет оценить вероятность тех или иных зависимостей в базе данных.

Второй подход основывается на том, что зависимости между данными ищутся автоматически.

Существующие программные комплексы Центрального банка Российской Федерации [3], предназначенные для автоматизации деятельности структурных подразделений по надзору за деятельностью кредитных организаций и их филиалов, относятся к первому подходу автоматизации поиска зависимостей между данными.

На данный момент анализ финансового состояния кредитных организаций проводится с использованием программного комплекса «Анализ финансового состояния банка» и основан на:

– использовании системы показателей, характеризующих деятельность банка и виды принимаемых рисков с выявлением взаимосвязи между показателями;

– изучении факторов изменения этих показателей и величин принимаемых рисков;

– сравнении полученных показателей со средними показателями по группе однородных банков.

Система показателей, используемых в рамках данной методики, сгруппирована в аналитические пакеты по следующим направлениям анализа:

1. Структурный анализ балансового отчета.

2. Структурный анализ отчета о прибылях и убытках. Коммерческая эффективность (рентабельность) деятельности банка и его отдельных операций.

3. Анализ достаточности капитала.

4. Анализ кредитного риска.

5. Анализ рыночного риска.

6. Анализ риска ликвидности.

Каждый аналитический пакет содержит таблицы аналитических показателей, позволяющих выявить тенденции и сделать выводы по соответствующему направлению анализа, а также графики, характеризующие динамику показателей, и диаграммы, отражающие структурные характеристики. Данный программный комплекс относится к первому подходу автоматизации поиска зависимостей между данными.

Система использует огромный массив входных данных:

– более 40 форм отчетности кредитных организации;

– нормативно-справочная информация банковского сектора;

– информация о нарушениях кредитных организаций, о результатах инспекционных проверок, мерах надзорного реагирования, примененных к данной кредитной организации.

Кроме того, для полного анализа текущей ситуации и принятия решений специалистами данного подразделения о дальнейшем режиме надзора за кредитной организацией, используются и иные данные, которые хранятся и просматриваются посредствам дополнительных программных продуктов.

Согласно информации, представленной Банком России, основными направлениями Стратегии информационных технологий в области финансового анализа являются:

– предиктивная аналитика, в том числе в реальном времени;

– технологии, позволяющие собирать, хранить и обрабатывать большие объёмы данных (*Big Data, Smart Data*);

– поддержка принятия управленческих решений на базе информации из разных источников.

На данный момент уже активно осуществляется построение единого информационного пространства в Банке России. Следовательно, внедрение интеллектуальной системы поддержки принятия решений в надзорный блок не только поможет проанализировать массив всех данных, необходимых для надзора за кредитными организациями, но и сократить время обработки этих данных.

Особое внимание Банк России уделяет организации превентивного банковского надзора. Проводится идентификация системных рисков на основе постоянного анализа состояния банковского сектора и принимаемых рисков с учетом внешних факторов.

Использование исторических данных в совокупности с текущими показателями кредитных организаций в интеллектуальной системе поддержки принятия решений в области финансового анализа кредитных организаций дает возможность построения прогнозов и ассоциаций. Прогнозы в данном случае возможны не просто как отражение основных тенденций, а как метод нахождения и создания шаблонов, реально отражающих динамику поведения целевых показателей по временным рядам баз данных. С их помощью можно предсказывать поведение кредитных организаций в будущем. Выявление негативных тенденций в деятельности банка еще на ранних стадиях соответствует принципам превентивного банковского надзора. Ассоциации же используются в том случае, когда несколько событий связанны между собой, что дает возможность выявления мошеннических схем.

С учетом рассмотренных направлений развития политики Центрального банка Российской Федерации можно сделать вывод о необходимости внедрения интеллектуальной системы поддержки принятия решений в области банковского надзора за кредитными организациями. Таким образом, рассмотрены следующие задачи, которые могут быть решены при внедрении интеллектуальной системы:

1. Оптимизация рабочего процесса надзорного блока Банка России.

2. Сокращение времени обработки массива данных.

3. Выстраивание доступного для пользователя результата анализа финансового состояния кредитных организаций.

4. Построение прогнозов дальнейшего поведения кредитной организации и банковского сектора в целом.

5. Определение взаимосвязанных событий для выявления мошеннических схем.

Список используемых источников

1. Анализ финансового состояния банка : учебно-метод. пособие. УМЦ Банка России. Тверь : 2000. 341 с.
2. Попов А. Л. Системы поддержки принятия решений : учебно-метод. пособие. Екатеринбург : Урал. гос. ун-т, 2008. 80 с.
3. Центральный банк Российской Федерации. URL: https://cbr.ru/ (дата обращения: 30.01.2020).

УДК 004.056
ГРНТИ 81.93.29

СТРУКТУРА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ УЗЛОМ СВЯЗИ

М. И. Бажин, В. Г. Иванов, В. А. Карев, А. С. Лебедев

Военная академия связи

В данной статье представлена структура программно-аппаратного комплекса автоматизированной системы управления узлом связи, предназначенная для организации автоматизированного планирования, эксплуатации узлов связи и осуществления ствolового контроля за состоянием каналов и средств связи с использованием web-технологий.

программно-аппаратный комплекс, система управления, узел связи, распределенное приложение, организация управления.

Основным направлением совершенствования систем управления узлами связи ВС РФ являются автоматизация процессов их управления в ходе эксплуатации на базе автоматизированных систем управления. Следовательно, создание автоматизированной системы управления узлом связи (АСУУС) имеет цель сокращения времени и усилий, затрачиваемых на техническую и расчетно-информационную работу, а также сокращение времени на сбор и обработку информации о состоянии узлов связи и его элементов, доведение задач до подчиненных с одновременным их документированием, обеспечение циркулярной или выборочной передачи важных команд и распоряжений до всех инстанций.

Решение задачи комплексной автоматизации процессов управления узлами связи в ходе его эксплуатации, не только при планировании его применения, но и в ходе дежурства предполагается осуществлять путем использования автоматизированной системы управления узлом связи.

Кроме того, актуальность разработки программно-аппаратного комплекса характеризуется тем, что уже сегодня требуется комплекс, позволяющий организовать автоматизированную систему управления узлом связи, с точки зрения, выполнения его функциональных задач по обеспечению современными услугами связи должностных лиц органов управления.

Узлы связи являются важнейшими элементами всех звеньев управления войсками. На них возлагаются основные задачи по обмену сообщениями между различными пунктами и должностными лицами управления войсками. Управление узлом связи – есть постоянное и целенаправленное воздействие должностных лиц на элементы и боевые посты узла связи по всесторонней подготовке и эффективному применению сил и средств связи для выполнения поставленной задачи.

Целью управления узлом связи является обеспечение своевременного предоставления услуг связи командованию и передачи заданных потоков сообщений в установленные сроки.

Наиболее сложной, трудоемкой и важной задачей в организации управления узлом связи является сбор информации о состоянии различных видов связи, каналов и средств связи.

Решение задачи комплексной автоматизации процессов управления узлами связи в ходе его эксплуатации, не только при планировании его применения, но и в ходе дежурства предполагается осуществить путем создания автоматизированной системы управления узлом связи. На рис. 1 представлена структура системы управления узлом связи.

При разработке программного комплекса АСУУС необходимо поставить условия обеспечения совместимости с программно-аппаратной платформой «Эльбрус», а также Windows и Linux, интегрируемость с системами управления оборудованием связи, а также предоставлением удобного интерактивного интерфейса для эффективного управления с использованием возможностей отображения информации на экране «Терминала». Ниже представлены технологии и инструменты, на основе которых разработан программный комплекс.

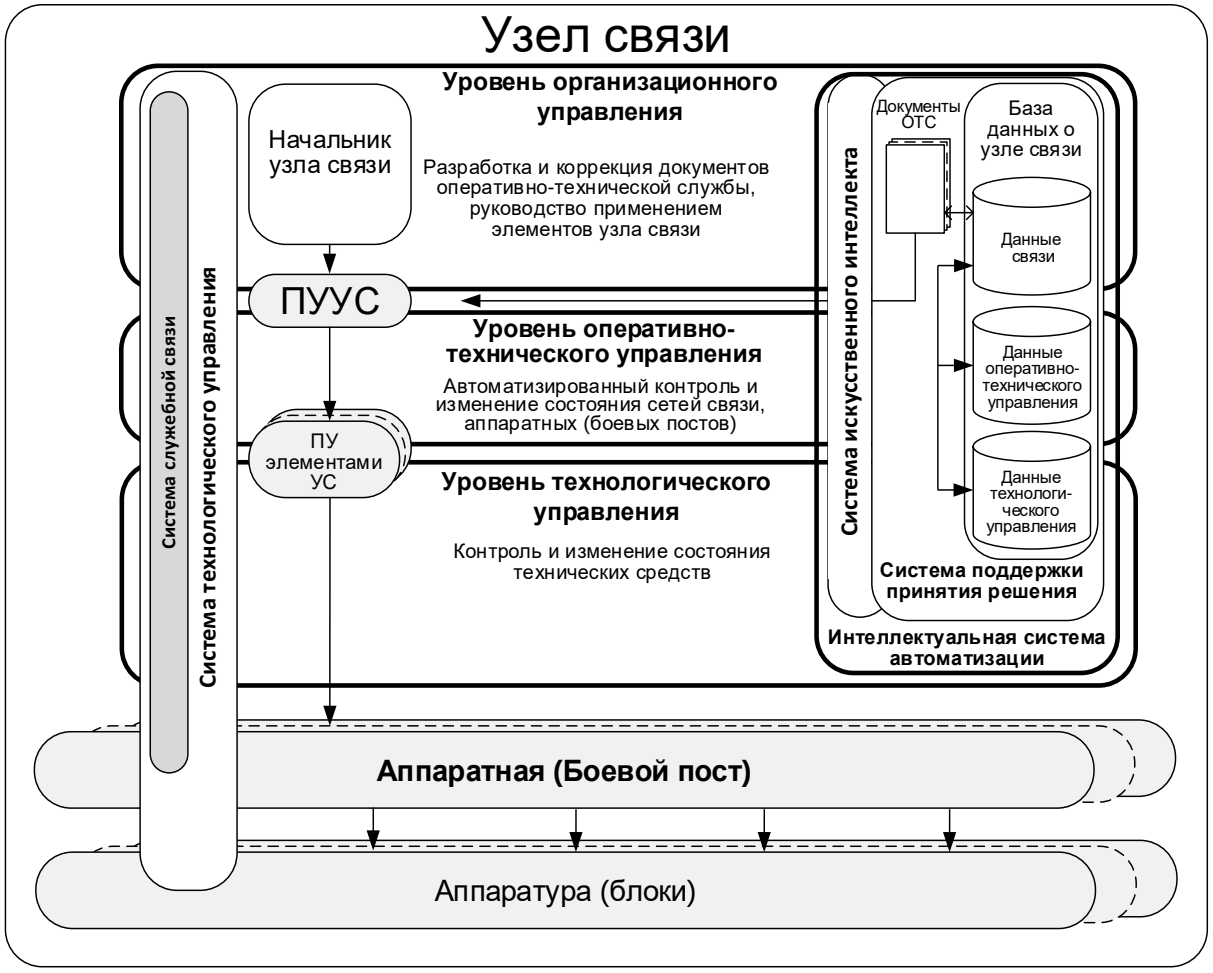


Рис. 1. Структура управления узлом связи

Для разработки программного комплекса также предлагается применять приложение Django REST.

Для создания и организация пользовательского интерфейса необходимо использовать фреймворк Vue.js.

Для обработки файлов, баз данных, почты и создания веб-сервера предлагается использовать кроссплатформенное программное обеспечение Apache Web Server.

На рис. 2 приведена структура web-сервера.

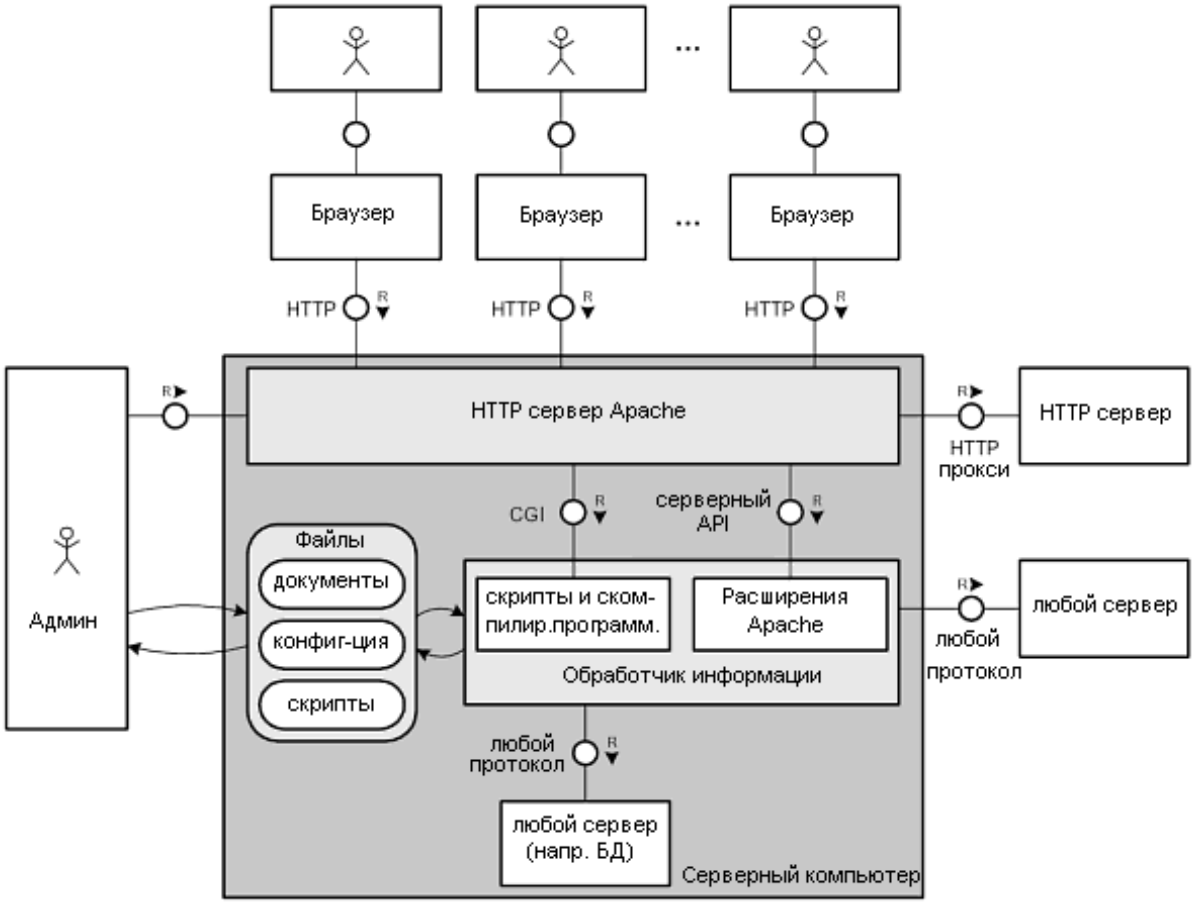


Рис. 2. Структура web-сервера

Работа веб-сервера заключается в обслуживании системы в сети. Для этого он выполняет роль посредника между компьютером сервера и компьютером клиента. Он берёт контент с сервера на каждый запрос пользователя и доставляет его клиенту.

Для организации управления средствами связи из состава аппаратных и станции УС нужно использовать протокол SNMP – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP.

Приведенные выше технологии позволят выполнить разработку программного комплекса АСУУС в виде Web-приложения. Архитектура такого приложения позволяет кратко описать алгоритм работы программно-аппаратного комплекса.

Опираясь на рассмотренный программный инструментарий программно-аппаратный комплекс АСУУС должен функционировать по принципу клиент-серверной технологии и обеспечивать автоматизированную разработку оперативно-технических данных в органах управления связи и документов оперативно-технической службы на узлах связи пунктах управления, а также организацию автоматизированного контроля за состоянием аппаратуры связи аппаратных.

ПАК должен формировать документы оперативно-технической службы в табличном виде, таких как:

1. Оперативно-технические данные.
2. Схема-приказ УС ПУ, элементу УС ПУ, аппаратной.
3. Схема калибрования УС.
4. Схема электроснабжения УС.
5. Схема организационно-технической структуры УС ПУ.

При организации «стволового» контроля ПАК осуществляет работу по клиент-серверной технологии, где сервером должен являться ПЭВМ начальника УС. Видом отображения информации служат разработанные в программной среде документы. Изменения состояния связи должны автоматически записываться в журнал несения дежурства по узлу связи.

ПАК должен включать серверную, клиентскую части и структурно иметь три модуля:

1. Модуль формирование оперативно-технических данных.
2. Модуль формирование документов ОТС.
3. Модуль обеспечения управления УС.

На рис. 3 изображена структура ПАК АСУУС.

Рис. 3. Структура ПАК АСУУС на уровнях управления

Практическая значимость

Автоматизация процессов управления и создание системы управления узлом связи позволит уменьшить долю времени и усилий, затрачиваемых на техническую и расчетно-информационную работу, сократить время на сбор и обработку информации о состоянии узлов связи и его элементов, доведение задач до подчиненных с одновременным их документированием, обеспечение циркулярной или выборочной передачи важных команд и распоряжений до всех инстанций [3].

Заключение

Предлагаемая структура ПАК АССУС разработана в соответствии с последовательностью работы должностных лиц органов управления связи и узлов связи по организации планирования и управления узлом связи.

Список используемых источников

1. Иванов В. Г., Панихидников С. А. Теория и практика построения технической основы системы управления специального назначения : монография. СПбГУТ. СПб., 2016. – 184 с.

2. Иванов В. Г. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи : монография. СПб. : ПОЛИТЕХ-ПРЕСС, 2018. – 214 с.

3. Иванов В. Г., Корякин Д. Д., Панихидников С. А. Автоматизированные системы управления связью // Труды учебных заведений связи. 2016. Т. 2. № 4. С. 56–62.

4. Иванов В. Г., Корякин Д. Д. Особенности функционирования современных автоматизированных систем мониторинга телекоммуникационных сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2017. С. 353–356.

Статья представлена научным руководителем, доцентом ВАС, кандидатом военных наук, доцентом, полковником В. Г. Ивановым.

УДК 004.925.83:004.928
ГРНТИ 27.21.21

АНАЛИЗ ГЕОМЕТРИЧЕСКИХ МОДЕЛЕЙ СИМУЛЯЦИИ ВОДНОЙ ПОВЕРХНОСТИ ДЛЯ ОТОБРАЖЕНИЯ В РЕАЛЬНОМ ВРЕМЕНИ

Д. Д. Балакирев, Е. В. Гунина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В трёхмерной графике использование водной глади – не редкость. Однако, методы построения её геометрической модели заметно отличаются от построения геометрии статических моделей, поскольку она не только видоизменяется в зависимости от времени, но и преобразуется по своим собственным законам. Их исследование и анализ, включающий поиск недочётов в зависимости от целей симуляции, а также построение выводов – это то, чему посвящена данная работа.

3D-графика, программирование, визуализация, симуляция, геометрическая модель.

В различных симуляторах и видеоиграх с трёхмерной графикой наличие водной глади – не редкость. Однако, методы построения её геометрической модели заметно отличаются от построения геометрии статических моделей, поскольку она не только видоизменяется в зависимости от времени, но и преобразуется по своим собственным законам, заложенных программой. В различных программных продуктах эти законы различаются. Их исследование, включающее нахождение закономерностей, анализ, включающий поиск недочётов, а также проектирование и формулировка своего способа моделирования геометрии водной поверхности – это то, чему посвящена данная работа.

В чём особенность отрисовки графики в реальном времени в отличие от предварительной отрисовки графики, которая может встречаться, к примеру, при создании спецэффектов к фильмам? В первую очередь, она должна быть относительно нетребовательна к вычислительным ресурсам компьютера, поскольку поддерживания достаточной частоты кадров для комфортного восприятия иллюзии анимации – одна из главных задач. В следствие этого рождаются ухищрения и упрощения для снижения затрат вычислительных ресурсов, которые, однако, негативно влияют на качество отображения. Нахождение баланса между качеством и низких затрат ресурсов является очень важной задачей. Конечно, прогресс не стоит на месте, и со временем идеальный баланс смещается в сторону качества, постепенно убавляя необходимость в ухищрениях и похода на уступки. Но тем не менее,

оптимизация ресурсозатрат до сих пор является одной из самых важных задач при организации процесса отрисовки изображения в реальном времени.

Первой задачей является исследование уже существующих геометрических моделей симуляции водной поверхности. Разумеется, посмотреть изнутри алгоритм является невозможным из-за того, что он является коммерческой тайной. Что доступно для исследования, так это визуальные результаты отработки этих алгоритмов. Были выбраны некоторые современные их представители.

Сперва для исследования была выбрана симуляция воды из «The Elder Scrolls V: Skyrim» (2011, 2016) (рис. 1).

Рис. 1. Водная поверхность в «The Elder Scrolls V: Skyrim»

Поверхность воды реализована достаточно хорошо. Она отображает отражения в экранном пространстве с учётом преломления света. На отражающую способность действует закон Френеля, который гласит о зависимости отражающей способности поверхности в зависимости от того, под каким углом находится точка обзора. При попадании динамических объектов на поверхность воды те создают иллюзорные колебания на них с помощью пиксельных шейдеров. Дождь, попадая на поверхность, создаёт рябь.

Однако у этой геометрической модели есть недостатки. Первым является плоскость поверхности (все волновые колебания сделаны иллюзорно). Вода хоть и выглядит на первый взгляд достаточно правдоподобно, но если смотреть на неё под углом, то можно заметить, что её поверхность является совершенно плоской. Кроме того, нет влияния статичных объектов на колебания. В реальной жизни волны способны ударяться об объекты. Например, о стену. Однако, в данной симуляции этот эффект не учитывается. Также, ветер не может возмущать водную поверхность.

Несмотря на недочёты, она вполне хорошо справляется со своей задачей. Поскольку игрок и объекты реального мира редко взаимодействуют

с водой, а та в свою очередь появляется в игровом пространстве в спокойном виде, излишняя её проработанность может не стоить затрат вычислительной мощности компьютера.

«Subnautica» (2018). Трёхмерная графика в этом программном продукте стилизована под 3D-мультипликацию. Воде было уделено особое внимание, что сказалось на качестве её симуляции (рис. 2).

Рис. 2. Водная поверхность в «Subnautica»

Геометрическая модель водной поверхности имеет те же свойства, что и модель, описанная ранее. Из преимуществ можно заметить реальную объёмность волновых колебаний на поверхности в отличие от мнимой, лишь создающей иллюзию их наличия. С целью оптимизации затрат ресурсов, с удалением водной поверхности от экрана уменьшается её детализация.

В целом, вода выглядит достаточно реалистично. Из недочётов можно отметить отсутствие воздействия объектов на колебания поверхности. Кроме того, анимация поверхности «статична» и не зависит ни от каких факторов. Была замечена повторяемость волновых колебаний – если посмотреть с высоты птичьего полёта на поверхность воды, то волны выстраиваются в одинаковые ровные полосы с одинаковыми промежутками, которые странным образом выделяются зеленоватым оттенком, что очень бросается в глаза.

Особо следует отметить существенный минус – отсутствие проработки физики воздействия волн на плавающие объекты, с которыми пользователь активно взаимодействует в виртуальной среде. Они словно прикованы к одной точке и являются статичными. Это негативно сказывается на реалистичном восприятии виртуального мира.

Следующий программный продукт, «The Legend of Zelda: Breath of the Wild» (2017), не претендует на реализм, а его графика стилизована под 2D-анимацию (рис. 3, см. ниже).

У воды этого представителя реализованы полноценные объёмные волны, однако мелкая рябь на поверхности сделана плоской и лишь создаёт иллюзию объёма. Динамические объекты могут создавать стилизованные

волны. Реализован закон Френеля и течение рек. На поверхности отображается отражения статических объектов с учётом волновых колебаний.

Рис. 3. Водная поверхность в «The Legend of Zelda: Breath of the Wild»

Однако у симуляции были найдены недостатки. Волновые колебания одинаковы по всей поверхности воды и не зависят от глубины водоёма и от того, является ли он стоячим или же в ней имеется течение. Кроме того, динамические объекты не влияют на волновые колебания. Единственный эффект – стилизованные 2D волны, распространяющиеся по поверхности на малую дистанцию. Также дождь не создаёт рябь на водной поверхности.

Многие недостатки могут быть оправданы малой вычислительной мощностью платформы, для которой предназначен этот продукт. Однако такая маленькая деталь, как рябь на водной поверхности, создаваемая дождём, является существенным минусом.

Симуляция водной поверхности под названием «Position Based Fluids» [5] создана программистами Nvidia и является воистину великолепной моделью, работающей в реальном времени (рис. 4).

Если предыдущие модели были представлены в виде динамической сетки, то эта модель основана на физике и взаимодействии отдельных частиц, которые визуально преобразуются в единую водную среду. Это очень правдоподобная симуляция, в которой группы частиц могут быть разделены и помещены в ёмкость, чего так просто не достичь сеточной моделью.

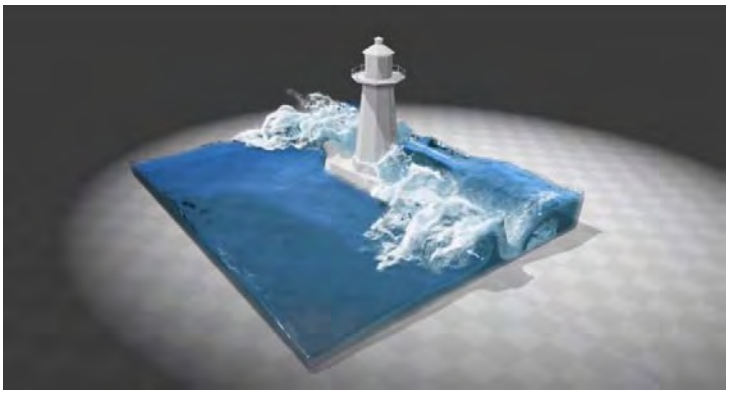


Рис. 4. Position Based Fluids в действии

Из её недостатков можно выделить высокое потребление вычислительных ресурсов. Не смотря на невероятное качество воды, эта модель вряд ли будет являться практичной для использования в реальном времени, поскольку в настоящих условиях помимо геометрии воды просчитывается поведение и геометрия множества других объектов, которые находятся в одной и той же сцене.

Однако, однажды наступит будущее, в котором подобные расчёты не будут занимать много времени, и уже тогда данная симуляция сможет приятно удивить человека, решившего погрузиться в виртуальный мир.

Подытожив, можно сказать о том, что разработчики при создании симуляции воды добиваются вполне хороших результатов. Моделирование воды пусть и является одной из самых сложных задач в графике, но тем не менее, существует множество достойных примеров. Однако при разработке недостаточно внимания уделяют различным мелким деталям, которые пусть по отдельности и являются незначительными, но вместе создают общую картину впечатлений от живости виртуального мира.

Из общих недостатков, которые часто встречаются в программных продуктах, можно отметить отсутствие интерактивности – редко где проработано взаимодействие окружающих объектов с водой. Например, волны не колеблют плавающие объекты. Или сами объекты не создают волны на поверхности. Кроме того, до сих пор выходят программные продукты, где волновые колебания являются исключительно иллюзорными, но по факту геометрия поверхности воды является совершенно плоской. Также довольно распространённой проблемой является отсутствие течения воды в текучих водных объектах.

Список используемых источников

1. OpenGL Tutorial [Электронный ресурс]. URL: http://www.opengl-tutorial.org/ru/ (дата обращения: 25.12.2019).

2. Знакомимся с OpenGL [Электронный ресурс]. URL: https://habr.com/ru/post/111175/ (дата обращения: 25.12.2019).

3. Суперсовременный OpenGL [Электронный ресурс]. URL: https://habr.com/ru/post/456932/ (дата обращения: 25.12.2019).

4. Modern OpenGL Tutorials [Электронный ресурс]. URL: http://ogldev.atspace.co.uk/ (дата обращения: 25.12.2019).

5. Новый 3D алгоритм симуляции воды [Электронный ресурс]. URL: https://habr.com/ru/post/177995/ (дата обращения: 25.12.2019).

УДК 004
ГРНТИ 81.93.29

АТАКИ ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ» (DDOS)

И. А. Баландин, В. О. Зиберов, Д. С. Кукунин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На сегодняшний день атаки типа «отказ в обслуживании» стали очень популярны в мире компьютерных технологий. Пострадало множество сервисов, компании потеряли прибыль и своих клиентов. В этой статье представлены теоретические сведения об атаках типа «отказ в обслуживании», их видах, способах действия, а также мотивации тех людей, которые организовывают эти атаки.

DDoS, отказ в обслуживании, атаки, безопасность.

Распределенная атака типа «отказ в обслуживании» (*DDoS*) – это вредоносная попытка сделать онлайн-сервис недоступным для пользователей, как правило, путем временного прерывания или приостановки работы служб его хост-сервера [1, 2].

DDoS-атака (рис.) запускается с многочисленных скомпрометированных устройств, часто распределенных по всему миру. Это называется «ботнет». Она отличается от других атак типа «отказ в обслуживании» (*DoS*), которые используют одно подключенное к Интернету устройство (одно сетевое подключение) для заполнения целевого объекта вредоносным трафиком. Этот нюанс является основной причиной существования этих двух, несколько отличных друг от друга, определений [3].

Рис. Схема DDoS-атаки

В целом, DoS и DDoS атаки можно разделить на три типа:

1. Объемные атаки. Включают в себя наводнения UDP, наводнения ICMP и другие поддельные пакеты наводнений [4, 5]. Цель атаки состоит в том, чтобы насытить пропускную способность атакуемого хоста. Величина атак измеряется в битах в секунду (*Bps*).

2. Атаки по протоколу. Включают в себя SYN наводнения, фрагментированные атаки пакетов, пинг смерти, SmurfDDoS [6] и многое другое. Этот тип атаки потребляет фактические ресурсы сервера или промежуточного

коммуникационного оборудования, такого как брандмауэры и балансировщики нагрузки. Величина атак измеряется в пакетах в секунду (*Pps*) [5].

3. Атаки на уровне приложений. Включают в себя медленные атаки, наводнения GET/POST, атаки, которые нацелены на Apache, уязвимости Windows, OpenBSD и многое другое [5, 7]. Они состоят из кажущихся законными и невинными запросов, цель которых – вывести из строя веб-сервер. Величина атак измеряется в запросах в секунду (*Rps*).

Распространенные типы DDoS-атак

Некоторые из наиболее часто используемых типов DDoS-атак включают:

– Наводнение UDP

Потоком UDP, по определению, является любая DDoS-атака, которая наводняет цель с помощью пакетов протокола UDP (USER *Datagram Protocol*). Целью атаки является наводнение случайных портов на удаленном хосте. Это заставляет цель многократно прослушивать приложения на этих портах и, когда никакие приложения не найдены, отвечать с пакетом ICMP «Destination Unreachable». Этот процесс подрывает ресурсы хоста, что в конечном итоге может привести к недоступности [8].

– Наводнение ICMP (*Ping*)

Подобно атаке потока UDP, поток ICMP переполняет целевой ресурс пакетами эхо-запроса ICMP (*Ping*), обычно отправляя пакеты как можно быстрее, не ожидая ответов. Этот тип атаки может потреблять как исходящую, так и входящую полосу пропускания, так как серверы жертвы часто пытаются ответить пакетами ICMP «Echo Reply», что приводит к значительному общему замедлению системы [9].

– SYN Flood

DDoS-атака SYN Flood использует известную слабость в последовательности TCP-соединений («трехстороннее рукопожатие»), при которой на запрос SYN для инициирования TCP-соединения с хостом должен быть получен ответ SYN-ACK от этого хоста, а затем подтвержден ответом ACK от инициатора запроса. В сценарии SYN Flood инициатор запроса отправляет несколько SYN-запросов, но либо не отвечает на ответ SYN-ACK узла, либо отправляет запросы SYN с поддельного IP-адреса. В любом случае, хост-система продолжает ждать подтверждения для каждого из запросов, выделяя ресурсы до тех пор, пока новые соединения не смогут устанавливаться, и, в конечном итоге, это приводит к отказу системы [10].

– Пинг смерти

Атака «Ping of death» (POD) включает в себя отправку злоумышленником на компьютер нескольких искаженных или вредоносных эхо-запросов. Максимальная длина пакета IP-пакета (включая заголовок) составляет 65 535 байт. Однако уровень канала передачи данных обычно ограничивает

максимальный размер кадра – например, 1500 байт по сети Ethernet. В этом случае большой IP-пакет разбивается на несколько IP–пакетов (известных как фрагменты), и узел получателя повторно собирает IP-фрагменты в полный пакет. В сценарии «Ping of Death» после злонамеренной манипуляции с содержимым фрагмента цель получает IP-пакет, размер которого при повторной сборке превышает 65 535 байт. Это может переполнить буферы памяти, выделенные для пакета, вызывая отказ в обслуживании законных пакетов [11].

– Slowloris

Высоконадежная атака, позволяющая одному веб-серверу вывести из строя другой сервер, не затрагивая другие службы или порты в целевой сети. Slowloris удерживает множество соединений с целевым веб-сервером открытыми как можно дольше. Это достигается путем отправки не полного запроса. Slowloris постоянно отправляет заголовки HTTP, но никогда не завершает запрос. Целевой сервер сохраняет открытыми все эти ложные подключения. Это в конечном итоге переполняет максимальный параллельный пул соединений и приводит к отказу в дополнительных соединениях от реальных клиентов [12].

– Усиление NTP

В атаках усиления NTP злоумышленник использует общедоступные серверы протокола сетевого времени (NTP) для переполнения целевого сервера UDP-трафиком. Атака определяется как нападение с усилением, поскольку отношение запроса к ответу в таких сценариях находится, где-то между 1:20 и 1:200 или более. Это означает, что любой злоумышленник, который получает список открытых NTP-серверов (например, с помощью такого инструмента, как Metasploit или данных из открытого проекта NTP), может легко создать разрушительную, высокоскоростную, крупномасштабную DDoS-атаку [13].

– Наводнение HTTP

При DDoS-атаке HTTP Flood злоумышленник использует кажущиеся законными HTTP-запросы GET или POST для атаки веб-сервера или приложения. HTTP-наводнения не используют искаженные пакеты, методы подмены или отражения и требуют меньшей пропускной способности, чем другие атаки. Атака наиболее эффективна, когда она заставляет сервер или приложение выделять максимально возможные ресурсы в ответ на каждый отдельный запрос [14].

– DDoS-атаки нулевого дня

Определение «нулевого дня» охватывает все неизвестные или новые атаки, использующие уязвимости, для которых еще не выпущен «патч». Этот термин хорошо известен среди членов хакерского сообщества, где практика торговли уязвимостями нулевого дня стала популярной деятельностью. [15]

Мотивация DDoS-атак

DDoS-атаки быстро становятся наиболее распространенным типом кибер-угроз, быстро растущих в прошлом году, как по количеству, так и по объему согласно последним исследованиям рынка. Тенденция заключается в уменьшении продолжительности атаки, но увеличении объема атак с пакетами в секунду.

Злоумышленники в первую очередь мотивированы [1, 4]:

Идеология – так называемые «хактивисты» используют DDoS-атаки как средство таргетинга на сайты, с которыми они идеологически не согласны.

Деловые распри – компании могут использовать DDoS-атаки для стратегического уничтожения веб – сайтов конкурентов, например, чтобы удержать их от участия в важном событии, таком как Киберпонедельник.

Скука – кибер-вандалы используют предварительно написанные сценарии для запуска DDoS-атак. Исполнители этих атак, как правило, скучают, потенциальные хакеры ищут прилив адреналина.

Вымогательство – злоумышленники используют DDoS-атаки или угрозу DDoS-атак как средство вымогательства денег у своих объектов.

Кибернетическая война – санкционированные правительством DDoS-атаки могут быть использованы как для нанесения ущерба оппозиционным сайтам, так и инфраструктуре вражеской страны.

В заключение хотелось бы отметить, что DDoS-атаки долгое время были серьезной проблемой лишь для ограниченного числа бизнес отраслей, таких как электронная коммерция, торговля и биржа, банкинг и платежные системы. Но с продолжающимся развитием интернета наблюдаются DDoS-атаки увеличенной интенсивности и частоты в абсолютно всех частях интернета. Это значит, что сервисы, которые мы используем, будут все чаще подвергаться атакам и быть недоступными, если компании не предпримут заранее никаких действий, направленных на отражение этих угроз.

Список используемых источников

1. Джесси Рассел. Система обнаружения вторжений. VSD, 2012. 174 с. ISBN 978-5-5129-1161-7.

2. DDoS Attacks [Электронный ресурс]. URL: https://www.imperva.com/learn/application-security/

3. Bots [Электронный ресурс]. URL: https://www.imperva.com/learn/application-security/what-are-bots/

4. Флёнов М. Linux глазами хакера. – СПб. : БХВ-Петербург, 2010. – 480 с

5. Dhruba Kumar Bhattacharyya, Jugal Kumar Kalita. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance.

6. Smurf DDoS attack [Электронный ресурс]. URL: https://www.imperva.com/learn/application-security/smurf-attack-ddos/

7. What is a DDoS Attack? [Электронный ресурс]. URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

8. User datagram protocol (UDP) [Электронный ресурс]. URL: https://www.imperva.com/learn/application-security/udp-user-datagram-protocol/

9. Ping flood (ICMP flood) [Электронный ресурс]. URL: https://www.imperva.com/learn/application-security/ping-icmp-flood/

10. TCP SYN Flood [Электронный ресурс]. URL: https://www.imperva.com/learn/application-security/syn-flood/

11. Ping of Death (POD) [Электронный ресурс]. URL: https://www.imperva.com/learn/application-security/ping-of-death/

12. Slowloris [Электронный ресурс]. URL: https://www.imperva.com/learn/application-security/slowloris/

13. NTP Amplification [Электронный ресурс]. URL: https://www.imperva.com/learn/application-security/ntp-amplification/

14. HTTP Flood [Электронный ресурс]. URL: https://www.imperva.com/learn/application-security/http-flood/

15. Zero-day (0day) exploit [Электронный ресурс]. URL: https://www.imperva.com/learn/application-security/zero-day-exploit/.

УДК 004.912
ГРНТИ 20.19.27

ПРЕОБРАЗОВАНИЕ НОРМАТИВНЫХ АКТОВ В ФОРМАТ МЕЖВЕДОМСТВЕННОГО ОБМЕНА В РАМКАХ НАЦИОНАЛЬНОГО ПРОЕКТА «ЦИФРОВАЯ ЭКОНОМИКА»

И. Ю. Баранов, А. А. Невров

Академия ФСО России

Требуется осуществлять межведомственный обмен нормативными актами. Часть нормативных актов требуют преобразования формата и не поддаются автоматическому переформатированию. Рассматриваются вопросы автоматизации преобразования форматов на основе настраиваемых шаблонов документов.

нормативный акт, формат моноширинного текстового документа, преобразование форматов.

В рамках национального проекта «Цифровая экономика» решается задача внедрения цифровых технологий и платформенных решений в сферах государственного управления и оказания государственных услуг, в том числе в интересах населения и субъектов малого и среднего предпринимательства, включая индивидуальных предпринимателей [1]. Для решения за-

дачи на базе системы межведомственного электронного взаимодействия создается платформа межведомственного взаимодействия обмена данными, в том числе нормативной справочной информацией [2]. Значительная часть от общего объема нормативной справочной информации в настоящее время хранится и обрабатывается в интегрированном полнотекстовом банке правовой информации (ИПБПИ) «Законодательство России» (www.pravo.gov.ru/ips). ИПБПИ содержит правовые акты (ПА), которые в силу сложившихся причин хранятся в устаревшем формате моноширинного текстового документа (ФМТД), форматирование в котором производилось не специальными управляющими тэгами документа, а пробелами. В настоящее время число подобных документов в ИПБПИ составляет около 400 тыс. (1969–2000 гг.).

ПА в ФМТД, размещенные в ИПБПИ имеют ряд существенных недостатков, особенно остро проявляющихся при поддержании актуальной редакции документа. Поэтому ФМТД не является предпочтительным форматом для осуществления межведомственного обмена данными и требуется переформатирование документов, например, в формат Open Document (.odt). Способ переформатирования документа из ФМТД во многом зависит от вида ПА. Под видом ПА в ИПБПИ будем понимать перечень видов актов, приведенных в документе по адресу: www.pravo.gov.ru/ips/?start_search&fattrib=1. Под формой ПА в ИПБПИ будет понимать вид ПА в формате, принятом федеральном органе исполнительной власти (ФОИВ) и региональном органе исполнительной власти (РОИВ).

Перечень видов ПА в ИПБПИ представляет собой ограниченное множество, его расширение проводится редко. Формы ПА не приведены к общему стандарту, несмотря на существование руководящих документов, предусматривающих применение определенных правил оформления ПА [3]. Вследствие этого изменение документов в ФМТД, требующееся при поступлении новых ПА, в формат, обеспечивающий возможность создания актуальной редакции изменяемого документа, не является детерминированным процессом и в настоящее время требует рутинной ручной обработки. При этом такая обработка входного потока ПА занимает большой ресурс рабочего времени и нуждается в автоматизации.

Для автоматизации процесса при использовании не жестко структурированного текста используется направление автоматического анализа вероятностного соотнесения ключевых слов и словосочетаний документа с заранее заданными словарными эталонами, привязанными к определенным стилям, предметным областям, подъязыкам или тематическим рубрикам. К таким ключевым словам относятся исходные атрибуты документов: реквизиты органа, издавшего ПА; вид ПА; место подписания ПА; дата подписания ПА; подписант ПА ФОИВ или РОИВ и др.

Обобщенный порядок конвертирования из ПА в ФМТД в ПА в пропорциональном шрифте с известной структурой представлен на рис. 1.

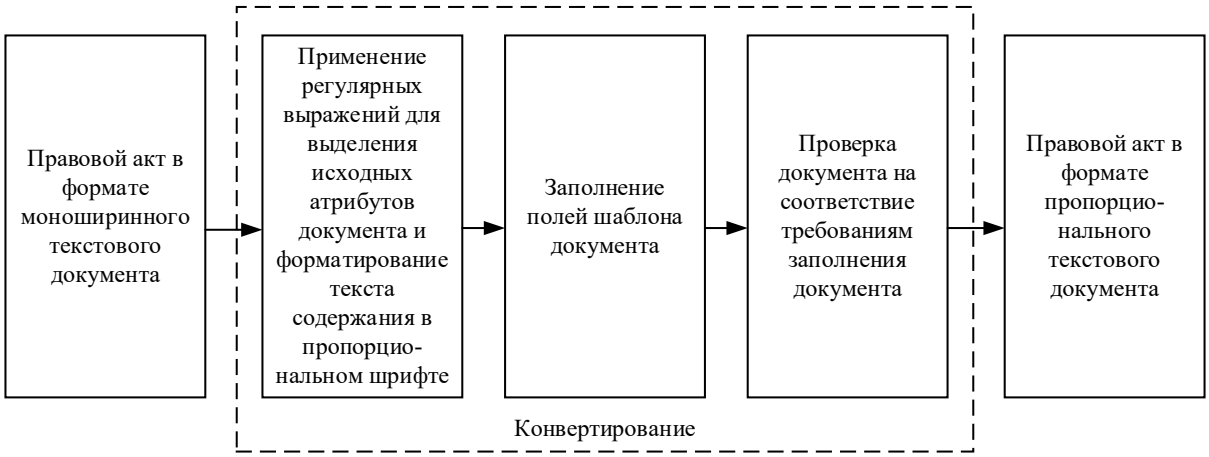


Рис. 1. Макроструктура обобщенного порядка конвертирования из ПА в ФМТД в ПА в пропорциональном шрифте

В качестве примера на рис. 2–3 приведено представление одного вида ПА «Закон» РОИВ в различных формах в ФМТД, где исходные атрибуты документов размещены в разных местах.

```
27 апреля 1998 года                                              68-ОЗ
-----------------------------------------------------------------------

                        ЗАКОН АМУРСКОЙ ОБЛАСТИ

             О БЮДЖЕТЕ ТЕРРИТОРИАЛЬНОГО ДОРОЖНОГО ФОНДА
                   АМУРСКОЙ ОБЛАСТИ НА 1998 ГОД

                                                              Принят
                                                            Амурским
                                                  областным Советом
                                                  народных депутатов
                                                 16 апреля 1998 года

    (В редакции Закона Амурской области от 02.10.98 г. N 93-ОЗ)
...
    Глава Администрации
    Амурской области          А.Н. БЕЛОНОГОВ

    г.Благовещенск
    27 апреля 1998 года
    N 68-ОЗ
```

Рис. 2. Форма представления закона Амурской области

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ЗАКОН ЧЕЛЯБИНСКОЙ ОБЛАСТИ

О бюджете областного дорожного фонда на 1998 год

Статья 1. Утвердить бюджет областного дорожного фонда на 1998 год по доходам в сумме 1556890 тыс. руб. и по расходам в сумме 1556890 тыс. руб.

...

Губернатор
Челябинской области П.И.Сумин
N 40-ЗО от 16 апреля 1998 года 30.04.98 г.

Рис. 3. Форма представления закона Челябинской области

Наибольшую трудность при конвертировании ПА в ФМТД представляет работа с таблицами и рисунками, выполненными символами псевдографики. При этом оформление таблиц ПА в ФМТД из ИПБПИ не стандартизовано и выполнялось в ФОИВ различными способами, что, в свою очередь, сильно затрудняет выявление общих табличных признаков (заголовок, тело таблицы, объединение ячеек и др.) для последующего создания шаблонов. Примеры таблиц ПА в ФМТД из ИПБПИ показаны на рис. 4–5.

Размер облагаемого совокупного дохода, полученного в календарном году	Сумма налога
до 20 000 руб.	12 процентов
от 20 001 до 40 000 руб.	2 400 руб. + 15 процентов с суммы, превышающей 20 000 руб.

Рис. 4. Таблица из Федерального закона № 159-ФЗ от 31 декабря 1997 г.

Выданы водительские удостоверения

Дата выдачи	Серия, N водительского удостоверения	Разрешенные категории	Наименование подразделения, выдавшего удостоверение	Подпись должностного лица, печать

Рис. 5. Приказ Министерства внутренних дел Российской Федерации № 860 от 30 декабря 1997 г.

В связи с разными формами ПА, принятыми в ФОИВ и РОИВ, целесообразна разработка создаваемых и редактируемых пользователем шаблонов документов.

В случаях конвертирования ПА в ФМТД в формат документов с пропорциональным шрифтом, но без изменения его структуры, требуется разработка инструмента, позволяющего пользователю определять структуру исходного документа, извлекать исходные атрибуты документа, создать шаблон и поместить исходные атрибуты в поля шаблона (рис. 6).

Для конвертирования таблиц, выполненных символами псевдографики требуется разработка инструмента, позволяющего автоматически находить позиции границ строк и столбцов, и далее предоставить пользователю возможность в автоматизированном режиме настраивать границы (объединять и разбивать ячейки таблицы) с визуализацией каждого шага конвертирования.

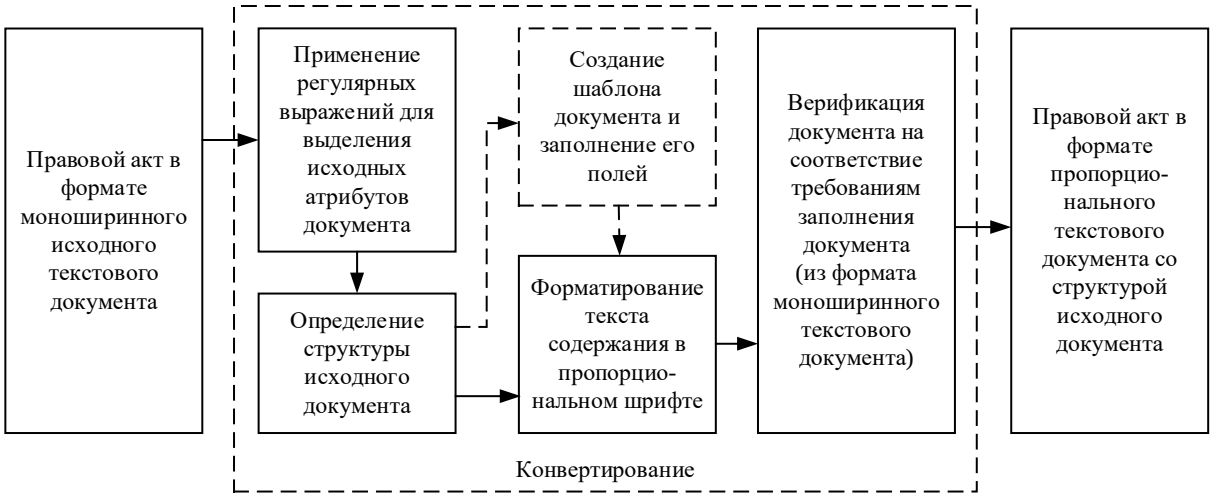


Рис. 6. Макроструктура порядка конвертирования из ПА в ФМТД в ПА в пропорциональном шрифте с сохранением структуры документа

Если принять каждое поле исходных атрибутов документа как блок, то задача разработки структуры для создания шаблона сводится к взаимному расположению этих блоков в соответствии с их размещением в документе в ФМТД. Таким образом, под структурой документа будем понимать взаимное размещение элементов исходных атрибутов документа на странице. Созданный и верифицированный шаблон вида документов сохраняется в базе шаблонов и в дальнейшем применяется, минуя этапы определения структуры и создания шаблона.

Выводы. Автоматизация процесса конвертирования (блок «Конвертирование» рис. 6) должна включать в себя в том числе процесс определения структуры исходного документа без участия пользователя или с минималь-

ными затратами ручного труда. Определение структуры исходного документа и создание его шаблона выполняется один раз для группы однотипных видов документов ФОИВ или РОИВ.

Список используемых источников

1. Паспорт федерального проекта «Цифровое государственное управление» национальной программы «Цифровая экономика Российской Федерации» от 04.06.2019 года [Электронный ресурс]. URL: https://digital.ac.gov.ru/upload/iblock/aa1/%D0%9F%D0%B0%D1%81%D0%BF%D0%BE%D1%80%D1%82%20%D0%A4%D0%9F%20%D0%A6%D0%93%D0%A3%20%D0%B8%D0%B7%20%D0%93%D0%98%D0%98%D0%A1%20%D0%AD%D0%91%20(%D0%BD%D0%B0%2027_06_2019).docx (дата обращения: 27.11.2019).

2. Федеральный проект «Цифровое государственное управление» [Электронный ресурс]. URL: https://storage.strategy24.ru/documents/project/d2813ede37c46a4ac2888ccc04cea5b5.pdf (дата обращения: 27.11.2019).

3. Чуковенков А. Ю. Юридическая техника и правила оформления документов // Секретарь-референт. 2009. № 5. С. 17–21.

УДК 004.75
ГРНТИ 50.53.17

РАЗРАБОТКА АЛГОРИТМА ИНТЕЛЛЕКТУАЛЬНОЙ ОБРАБОТКИ БОЛЬШИХ ОБЪЕМОВ ИНФОРМАЦИИ С ПРИМЕНЕНИЕМ МОДУЛЯ APACHE SPARK

И. В. Беликов, С. М. Макеев

Академия ФСО России

В данной работе рассматривается вариант алгоритма по интеллектуальной обработке больших объемов информации на базе программного обеспечения с открытым исходным кодом. Представлена структурная схема алгоритма, описание метода, использованного для интеллектуальной обработки информации, полученной из сети Интернет с целью классификации контента по эмоциональной окраске.

большие данные, модуль Apache Spark, задача классификации, обработка текстовой информации на естественном языке.

Основным источником информации различной по форме и своей структуре в настоящее время является всемирная глобальная сеть Интернет, а именно, социальные сети (СС). Анализ информации, которая, зачастую, является слабоструктурированной и огромной по своему объему является

важной задачей, так как выявление негативных и агрессивно настроенных пользователей СС по отношению к каким-либо событиям на региональном или федеральном уровне поможет предупредить и обезопасить общество от нежелательных происшествий [1].

Целью данной работы является разработка алгоритма для интеллектуальной обработки больших объемов информации, полученной из СС с применением модуля Apache Spark, который позволяет распараллелить вычисления, тем самым, повысить оперативность процесса обработки информации.

Так как контент, содержащийся в социальных сетях представляет собой как текстовые данные, аудио и видеофайлы, так и статические изображения, которые несут смысловую нагрузку. Для полноты и точности оценки отношения пользователей в СС к каким-либо событиям, которые представлены в виде различных публикаций, необходимо учитывать всю разнородность контента. В данной работе представлена частная задача по обработке текстовых комментариев, оставленных пользователями в СС в отношении определенных проблем и тематик.

В СС накапливаются огромные массивы комментариев и личных сообщений, которые необходимо обрабатывать в режиме реального времени, используя современные технологии обработки и анализа. Обработка большого объема слабоструктурированной и разнородной информации без применения новых технологий, методов и вычислительных модулей не имеет смысла.

Новейшие методы работы с большим объемом данных представляют собой распределенную обработку информации на множествах узлах – исполнителях, т. е. тех рабочих станциях, на которых производятся все вычисления. Такой подход обеспечивает сразу несколько важных преимуществ:

- Имеется возможность по увеличению количества узлов, на которых производится обработка данных до нескольких тысяч, что позволяет системе быть гибкой и масштабируемой.
- Центральный сервер (рабочая станция) освобождается от основных нагрузок по обработке и хранению промежуточных результатов, которая, в свою очередь, перекладывается на узлы-исполнители.
- Обеспечение обмена данными между удаленными пользователями [2].

Для распределенной потоковой обработки данных предлагается использование специализированной платформы Apache Spark, реализованной в облачной инфраструктуре. Основными преимуществами такого подхода является:

- Возможность хранения и работы с большими объемами входных данных за счет применения распределенной файловой системы (HDFS).

•Высокая горизонтальная масштабируемость, достигаемая за счет добавления дополнительных узлов в вычислительный кластер без необходимости внесения изменений в алгоритмы обработки.

•Возможность организации работы с данными, поступающими в потоковом режиме [3].

В качестве математической модели, реализующей семантическую обработку текстовой информации, был выбран метод Word2Vec, который основывается на сверточной нейронной сети. На рис. 1 представлена схема алгоритма интеллектуальной обработки больших объемов информации. Выборка, предназначенная для обучения модели, была получена из СС Twitter. Она включала себя комментарии к конкретным публикациям и новостям. Размер выборки составил 5 Гб.

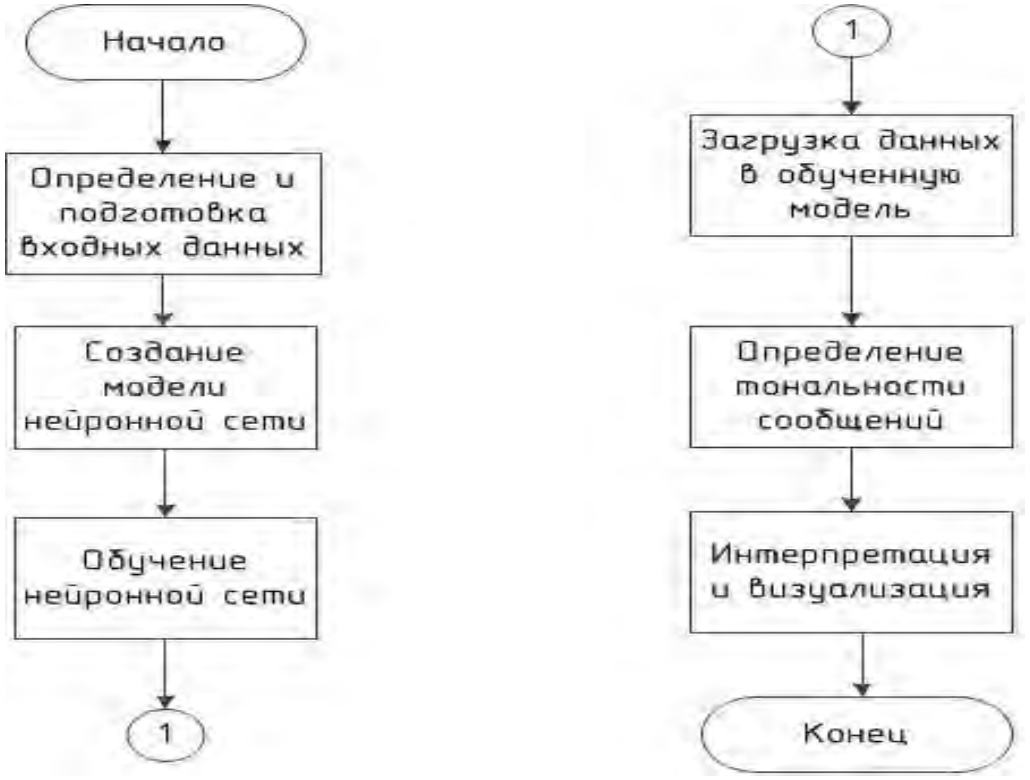
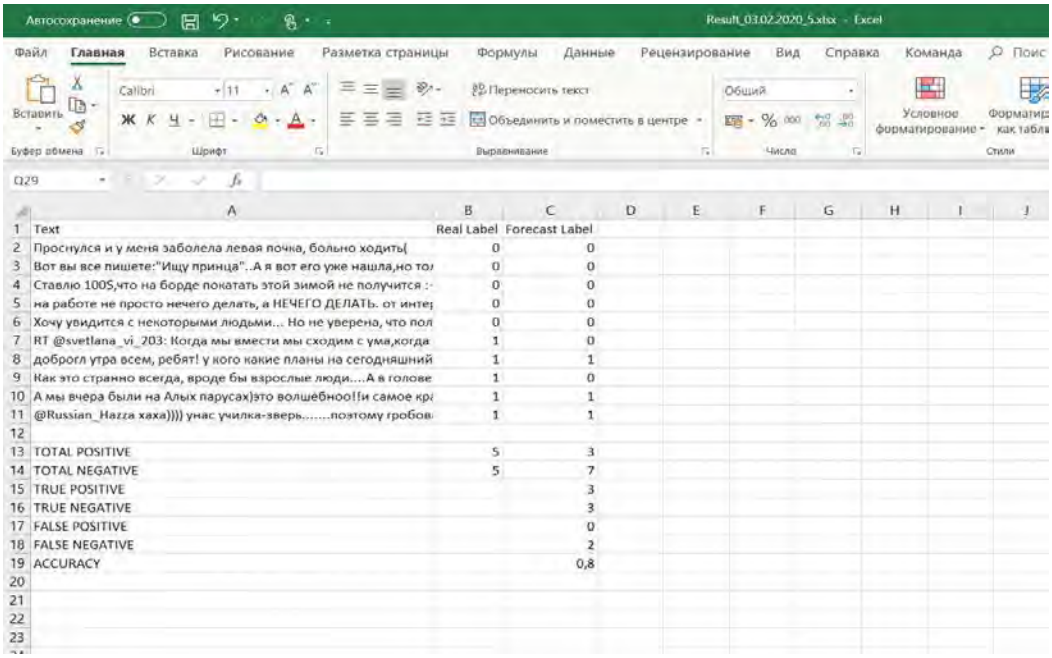


Рис. 1. Схема алгоритма интеллектуальной обработки больших объемов информации

На первом этапе осуществлялось разбиение исходной выборки на 3 составляющих, 50 % выборки предназначалось для обучения нейронной сети, 30 % выборки предназначалось для тестирования работы обученной модели и 20 % для оптимизирования показателей нейронной сети с целью увеличения качества классификации. Также, на данном этапе производилась фильтрация сообщений из социальной сети при помощи регулярных выражений, чтобы на вход модели поступали только текстовые данные, несущие смысловую нагрузку [4, 5].

На последующих этапах (создание и обучение нейронной сети) была получена модель, которая с точностью 81 % определяет класс сообщения из СС. Данная точность оценивалась с помощью параметра F1-меры [5].

На последующих этапах производится загрузка новых сообщений в уже обученную модель. Результатом работы алгоритма является отчетный файл с определенной эмоциональной окраской текстовых комментариев, полученных в качестве входных данных (рис. 2) и подробной визуализацией (рис. 3).



	A	B	C
1	Text	Real Label	Forecast Label
2	Проснулся и у меня заболела левая почка, больно ходить(	0	0
3	Вот вы все пишете:"Ищу принца"..А я вот его уже нашла,но то	0	0
4	Ставлю 100$,что на борде покатать этой зимой не получится :-	0	0
5	на работе не просто нечего делать, а НЕЧЕГО ДЕЛАТЬ. от интер	0	0
6	Хочу увидится с некоторыми людьми... Но не уверена, что пол	0	0
7	RT @svetlana_vi_203: Когда мы вместе мы сходим с ума,когда	1	0
8	доброго утра всем, ребят! у кого какие планы на сегодняшний	1	1
9	Как это странно всегда, вроде бы взрослые люди....А в голове	1	0
10	А мы вчера были на Алых парусах)это волшебное!!и самое кр	1	1
11	@Russian_Hazza хаха)))) унас училка-зверь.....поэтому гробов	1	1
12			
13	TOTAL POSITIVE	5	3
14	TOTAL NEGATIVE	5	7
15	TRUE POSITIVE		3
16	TRUE NEGATIVE		3
17	FALSE POSITIVE		0
18	FALSE NEGATIVE		2
19	ACCURACY		0,8

Рис. 2. Результат обработки новых комментариев

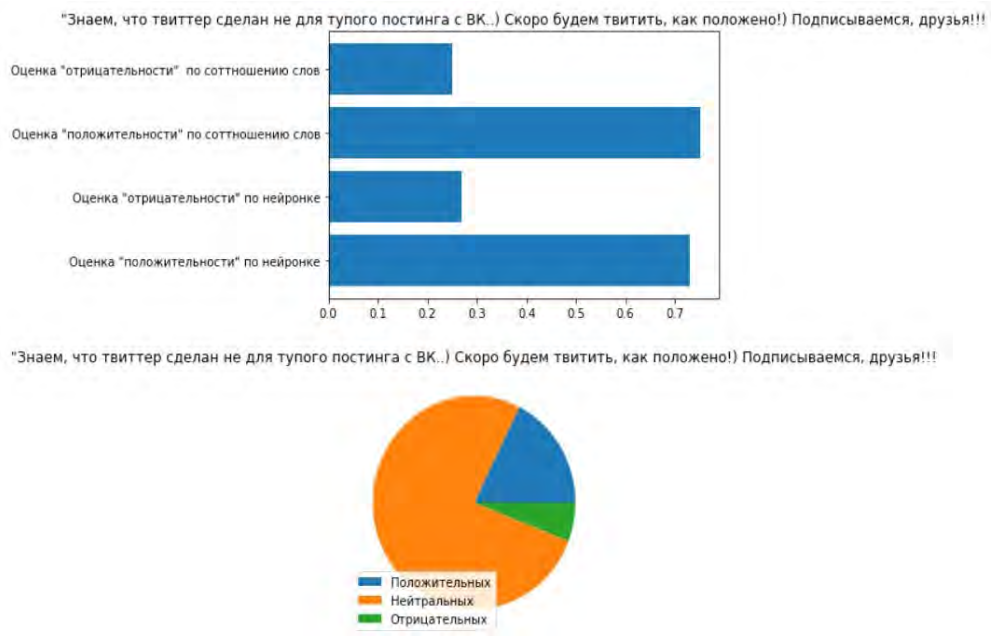


Рис. 3. Визуализация полученных результатов

Для демонстрации точности полученной модели на рис. 4 представлена оценка точности процесса классификации [6]. Из представленных диаграмм видно, что модельные значения приближены к значениям истинным. Следовательно, обученная модель пригодна для прогнозирования.

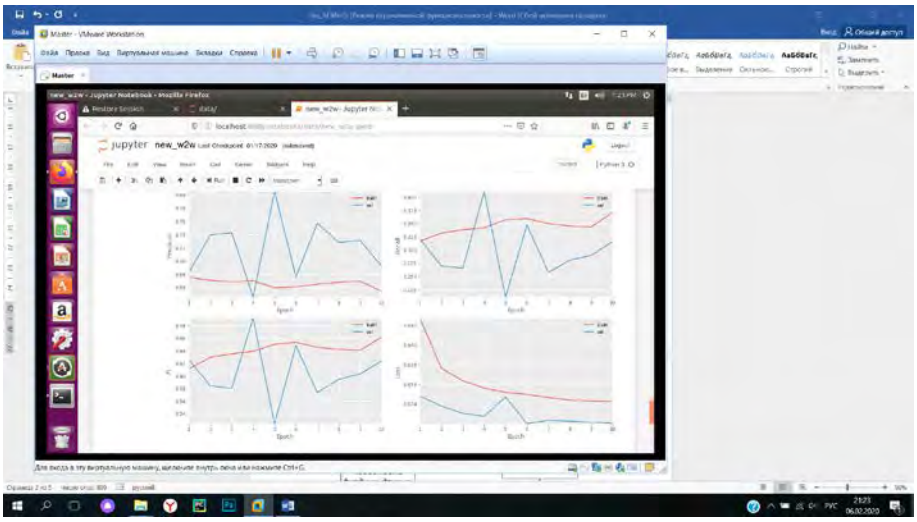


Рис. 4. ROC – кривая

Таким образом, в результате проделанной работы был разработан алгоритм для интеллектуальной обработки больших массивов информации. Применение данного алгоритма с использованием модуля Apache Spark позволит повысить оперативность анализа разнородной информации большого объема. Дальнейшим направлением исследования является классификация входных данных, представленных в графическом формате.

Список используемых источников

1. Федеральный список экстремистских материалов URL: http://minjust.ru/ru/extremist-materials (дата обращения: 01.02.2020).

2. Макеев С. М., Воробьев А. А., Грушевая Е. В. Исследование возможностей применения модуля Apache Spark для интеллектуальной обработки разнородных данных // Известия ТулГУ. 2019. Вып. 3. С. 254–262.

3. Официальный сайт разработчиков Spark: работа с библиотекой MLlib [Электронный ресурс]: [сайт]. – Режим доступа: https://spark.apache.org/docs/latest/ mllib-feature-extraction.html (дата обращения: 04.02.2020).

4. Makeev S. M., Belikov I. V., Lebedev I. V., Perov V. I. Application of intelligent decision support system for processing a big data of heterogeneous information // Modern informatization problems in the technological and telecommunication system analysis and synthesis (MIP-2020’AS) : Proceeding of the XXV-th International Open Science Conference (Yelm, WA, USA, January 2020) / Editor in Chief Dr. Sci., Prof. O. Ja. Kravets – Yelm, WA, USA: Science Book Publishing House, 2020. 108 p. PP. 247–251.

5. Макеев С. М., Воробьев А. А., Жусов Д. Л., Беликов И. В., Лебедев И. В., Перов В. И. Программный модуль для обработки больших объемов информации в интеллектуальной системе поддержки принятия решений // Свидетельство о регистрации программы для ЭВМ RU 2020610754, 20.01.2020. Заявка № 2019667352 от 24.12.2019.

6. Оценка точности классификатора: [сайт]. URL: http://bazhenov.me/blog/2012/07/21/classification-performance-evaluation.html (дата обращения: 08.02.2020).

УДК 004.056
ГРНТИ 81.93.29

СПОСОБ СЕТЕВОГО КОНТРОЛЯ НА ОСНОВЕ АНАЛИЗА СЕТЕВОГО ТРАФИКА В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПРИ НАЛИЧИИ АНОМАЛИЙ

А. С. Бирюков, В. А. Липатников

Военная академия связи

Рассматривается решение актуальной задачи сетевого контроля на основе анализа сетевого трафика в информационных системах при наличии аномалий автоматизированных систем управления и связи специального назначения. Исследованы методы контроля трафика в сети, указаны их достоинства и недостатки. Предложен способ сетевого контроля на основе анализа сетевого трафика в информационных системах при наличии аномалий. Реализован подход с использованием прогнозирующих моделей (Model Predictive Control), обеспечивающий поддержку принятия решений.

сетевой контроль, информационные системы, трафик, аномалии.

Введение

Неоднозначность, одноактность и неповторимость возникновения множества событий информационной системы (ИС), в которой требуется принятие решений, состоит в низкой структурированности таких событий, так как не все факторы, влияющие на трафик, можно предугадать заранее. Также заблаговременно неизвестна и взаимосвязь между факторами. Она может обнаруживаться только с течением времени. Некоторые из факторов и их взаимосвязь не могут определяться количественно, а только качественно.

Кибербезопасность (КБ) – одно из ключевых направлений деятельности любой успешной организации, защиты ресурсов для обеспечения непрерывности бизнеса и требованиями соответствия законодательству и отраслевым стандартам. Одним из наиболее важных аспектов, составляющих обеспечение безопасности киберпространства, является сетевой контроль (СК).

Показателем результативности СК является требуемая достоверность при допустимом уровне временных затрат выявления аномалий.

Выбор метода решения

Определено, что технологии анализа трафика в сети развиваются по двум основным путям: увеличение «глубины» исследования каждого пакета, то есть данные анализируются на более высоких уровнях модели OSI, и увеличение доскональности учета состояния всего трафика, содержащего пакет [1]. Эта технология по глубине анализа условно разделяется на три уровня: упрощённый, средний и интенсивный анализ пакетов [2].

Упрощённый анализ характеризуется достаточно невысокими запросами к вычислительным ресурсам, что даёт возможность анализировать значительные объемы трафика. Такой анализ применяется в преобладающем количестве сетевых экранов операционных систем, устройств маршрутизации и т. п. На его основе реализуются списки управления доступом пользователей к сети на уровне IP-адресов и портов (*AccessControlList,* ACL).

В предлагаемом способе выбрана для применения библиотека функций (MPI – *message passing interface*), предназначенная для поддержки работы параллельных процессов в терминах передачи сообщений.

Следовательно, упрощённый анализ имеет смысл использовать для ограничения доступа к службам (портам) и отдельным компьютерам (IP) внутренней сети из внешнего мира.

При средней глубине анализа пакетов анализирует трафик, путём мониторинга на сеансовом уровне модели OSI, используя настроенный промежуточный шлюз (устройство MPI). На этом уровне анализа данные из пакетов проверяются промежуточным шлюзом по установленным принципам и не полностью. Такой шлюз располагается между сетевым шлюзом провайдера и оконечными пользователями.

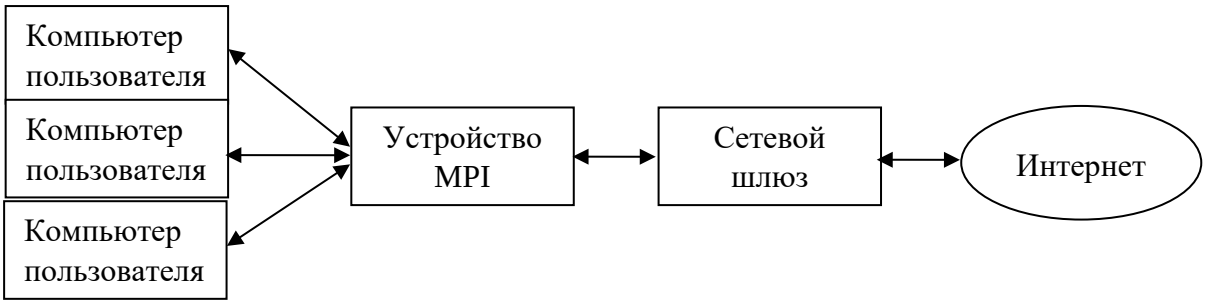


Рис. 1. Схема применения устройства анализа на основе технологии MPI

Устройство MPI проверяет заголовочную часть пакетов до транспортного уровня модели OSI и некоторое количество пакетных данных, с целью сравнить проверяемую часть с заранее составленным перечнем сопоставления линейной последовательности токенов естественного (формального)

языка с его формальной грамматикой, за которым следует ответ, если они обнаружены [2]. При интенсивном анализе трафика (DPI) пакеты из потока данных могут модифицироваться, фильтроваться и перемаршрутизироваться.

При такой глубине анализа устройство DPI проверяет все составные части всех пакетов. Определяющим отличием от вышеперечисленных способов есть то, что устройства DPI имеют возможность принимать решения, не ограничиваясь только содержимым пакетов, но и анализируя неявные отличия, свойственные конкретным программам и сетевым протоколам. С этой целью обычно применяется статистический анализ. В частности, проверка частоты появления некоторых значений, размера пакетов, времени, прошедшего между последовательными метками синхронизации и т. п. [2].

Логическими компонентами при анализе трафика являются сборщики, анализаторы и контроллеры. В таблице показаны компоненты, работающие на определенном этапе работы аппаратно-программного комплекса.

ТАБЛИЦА. Компоненты, работающие на определенном этапе системы

Этапы работы системы	Компоненты, работающие на этапе
Этап накапливания знаний	Сборщик, Анализатор
Этап поиска аномалий	Сборщик, Анализатор, Регулятор

Сборщик осуществляет мониторинг потока данных, выделяя данные из заголовков пакетов за установленный промежуток времени мониторинга, сортирует поток данных, абонентов и значения из заголовков для их последующей обработки анализатором. Определяется, является ли абонент новым или ранее был в поле зрения системы [2].

Если пользователь впервые попал в поле зрения системы, то анализатор начинает накапливать знания о нём, т. е. формирует новую незаполненную таблицу опорных значений и заполняет её. Если абонент не является новым для системы, анализатор выясняет, полностью ли заполнена таблица опорных значений для этого источника данных. Если нет, то система продолжит записывать опорные значения в существующую таблицу. Отметка времени в определенной ячейке таблицы поможет понять, как давно начался этап обучения. Если же этап накапливания знаний об абоненте уже завершен, т. е. таблица для него заполнена, то трафиком от этого пользователя начинает заниматься регулятор.

Сравнивая опорные значения, принятые от анализатора, с опорными значениями, записанными в таблице, регулятор принимает решение о наличии или отсутствии в трафике аномалий.

Аномалии предлагается выявлять во входящих и исходящих пакетах. Для этого они перехватываются, и из них извлекается такая информация,

как объем IP-пакета, IP-адрес источника, IP-адрес назначения, время и дата получения IP-пакета. Затем полученная информация сохраняется в базе данных сетевой статистики. Если же адекватной модели сетевого трафика не существует, то в таком случае проводится обработка динамического ряда учитывая особенности методики [3]:

$$x = \{V(t)\}(t = t_1, t_2, \dots, t_n),$$

где $V(t_k)$ $\left(k = \frac{1}{n}\right)$ определяет значение объема сетевого трафика на момент времени t_k. Если есть значение ряда однородных величин, характеризующих изменения во времени, то появляется возможность построить систему уравнений, которая воспроизводит поведение сетевого трафика, а затем предоставить прогнозы будущим значениям трафика:

$$\{V(t_{n+1}), V(t_{n+2}), \dots\}.$$

Определено, что методы статистического анализа динамических рядов чаще всего опираются на исследования авторегрессионных моделей вида:

$$V(t_k) = \{V(t_{k-1}), V(t_{k-2}), \dots, V(t_{k-m})\}, k \geq m + 1.$$

В этой ситуации прогнозирование динамического ряда переходит к решению задачи нейросетевого моделирования, то есть к задаче нейронной аппроксимации непрерывной функции многих переменных по заданному набору обучающих образцов. Если известно значение внешней входной последовательности $\{V(t_k)\}$ и нужно перевести её в другую наблюдаемую последовательность $\{Y(t_k)\}$, то, представляя саму систему нелинейной, есть возможность представить связь между входами и выходами в виде трехслойной нейронной сети, которая индуцирует сигналы в виде

$$V(t_{k+1}) = \sum_{i=1}^{n} c_i \varphi[w_{ik} V(t_k) - \theta_i], k = \overline{1, m}\ , k \geq m + 1,$$

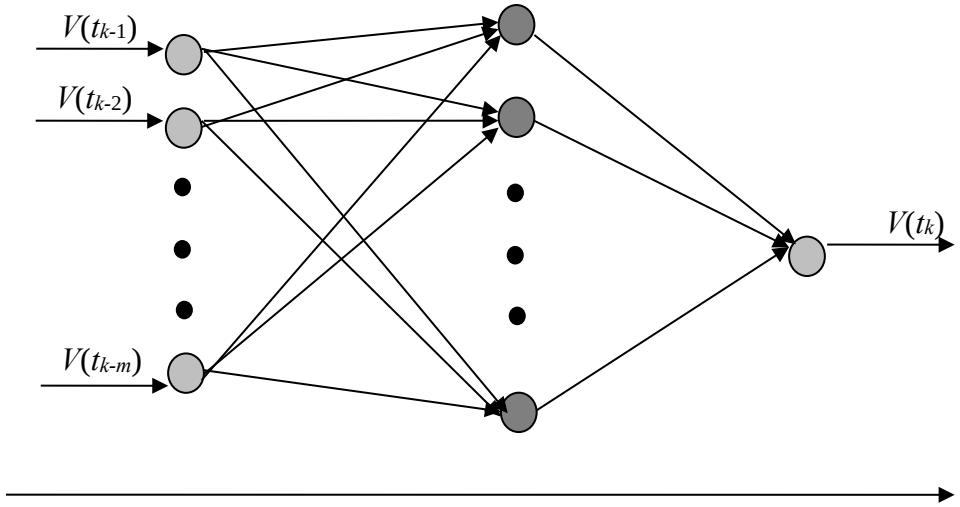
где n – количество нелинейных нейронов в скрытом слое, w_{ik} и c_i – веса входных и выходных синоптических связей, θ_i – пороговое значение i-го нелинейного нейрона из скрытого слоя, $\varphi[\dots]$ – нелинейная функция активации нейрона из скрытого слоя.

В общем виде задачу нейросетевого моделирования сетевого трафика как динамического ряда есть возможность представить так [4]:

$$V(t_k) = F[V(t_{k-1}), V(t_{k-2}), \dots, V(t_{k-m})].$$

где F[...] – нелинейная функция авторегрессии, реализующаяся с помощью трехслойной нейронной сети с топологической структурой, представленной на рис. 2.

При нейросетевом моделировании динамического ряда сетевого трафика формируются три совокупности данных: обучающая, валидационная и тестовая. Обучающая отвечает за построение самой нейронной сети, настраивает её параметры, а конкретно массу синоптических связей и пороги нейронов из скрытого слоя. С помощью валидационной совокупности выбирается оптимальная топологическая структура сети, а тестовая используется для контроля подлинности прогнозов [4].



$$V(t_k)=F[V(t_{k-1}),\ V(t_{k-2}),\ ....,\ V(t_{k-m})]$$

Рис. 2. Нейросетевая авторегрессионная модель прогнозирования аномалий

Новизна результата определяется тем, что предлагаемый способ прогнозирования аномалии в отличие от известных:

1) Учитывает динамику и стохастическую неопределенность основных процессов.

2) Использует параметры реальной структура ИС за счет применения прогнозирования аномалии.

3) Обеспечивает возможность обоснованного принятия решения на проведение организационно-технических мероприятий по предотвращению реализаций угроз безопасности.

4) Предложен общий алгоритм, включающий в себя этап прогнозирования состояния аномалии. Предложен алгоритм прогнозирования аномалии на основе методологии МРС.

Заключение

На основе анализа методов контроля трафика в сети, указаны их достоинства и недостатки, а также схема применения устройства анализа трафика.

Предложенный способ СК позволит обеспечить необходимый уровень защищенности ИС, путем внедрения различных модулей, объединенных в единую систему, для повышения эффективности сбора трафика, за счет использования фильтров для пакетов.

Список используемых источников

1. Липатников В. А., Торточаков С. В., Тихонов В. А. Модель процесса проактивного управления кибернетической безопасностью систем критических инфраструктур специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. С. 413–420.

2. Гетьман А. И., Маркин Ю. В., Евстропов Е. Ф., Обыденков Д. О. Обзор задач и методов их решения в области классификации сетевого трафика // Труды ИСП РАН. 2017. Т. 29, Вып. 3. С. 117–150. DOI: 10.15514/ISPRAS-2017-29(3)-8.

3. Бычков Б. И., Кудряшов Н. И., Гуренко В. В., Качественная оценка некоторых методов спектрального анализа. // Радиооптика. МГТУ им. Н. Э. Баумана. Электрон. журн. 2017. № 01. С. 34–46.

4. Гасанов В. И. Выявление аномалий в сетевом трафике на основе нейросетевого моделирования динамики изменения объемов IP-пакетов // 2018 ISSN 1028-9763. Математичні машини і системи. 2018. № 2. С. 40–45.

УДК 004.514
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ МЕТОДОВ И АЛГОРИТМОВ ОПТИМИЗАЦИИ АВТОМАТИЧЕСКОГО ПОСТРОЕНИЯ МАРШРУТОВ ДВИЖЕНИЯ РОБОТИЗИРОВАННЫХ СИСТЕМ С ЦЕЛЬЮ МИНИМИЗАЦИИ ЭЛЕКТРОПОТРЕБЛЕНИЯ

Е. А. Бовыкин, Г. В. Верхова, С. П. Присяжнюк

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлены результаты исследования методов и алгоритмов оптимизации построения маршрутов движения роботизированных систем с целью миними-

зации электропотребления. Задача оптимизации может быть сведена к поиску кратчайшего пути на направленном графе, у которого весовые коэффициенты ребер пропорциональны энергопотреблению автономного подводного аппарата с учетом совершаемого маневра, длине пути и параметров среды. Предлагаемый метод позволяет выполнить декомпозицию решения задачи на три этапа: 1) построение трехмерной сетки, состоящей из всех возможных графов направления движения; 2) определение весовых коэффициентов ребер графа на основе информации о среде, в которой происходит движение подводного аппарата; 3) нахождение оптимального пути на графе.

построение маршрутов, автоматические системы, численная оптимизация.

Для решения задачи построения маршрутов движения роботизированных систем с целью минимизации электропотребления предлагается алгоритм, состоящий из 4 этапов:

1. Дискретизация пространства путем построения трехмерной сетки.
2. Построение графа возможных направлений на основе построенной сетки.
3. Определение весов ребер графа с учетом параметров среды и перемещения объекта.
4. Поиск оптимального пути на построенном графе.

Для решения задачи построения сеток в настоящее время используют прямые и итерационные методы. Прямые методы обеспечивают создание сетки за один проход. В случае применения данных методов структура сетки и координаты всех ее узлов заранее известны. В случае применения итерационных методов, сетка строится последовательно, в течение нескольких итераций. На каждой итерации к создаваемой сетке добавляется одна или несколько секций. В данном классе методов координаты узлов и структура сетки заранее не известны и могут динамически изменяться в процессе построения [1].

Главными преимуществами прямых методов являются высокая скорость сеток и надежность. Основным недостатком прямых методов является их применимость только для областей, имеющих определенную геометрическую конфигурацию, что ограничивает их применение на практике.

В отличие от прямых методов, итерационные методы являются универсальным и могут быть использованы для дискретизации областей, имеющих произвольную форму. Благодаря своей универсальности итерационные методы получили широкое применение для формирования траектории движений автономных беспилотных транспортных средств. Недостатками итерационных методов являются высокая ресурсоемкость, более низкая скорость работы по сравнению с прямыми методами, а также их меньшая надежность.

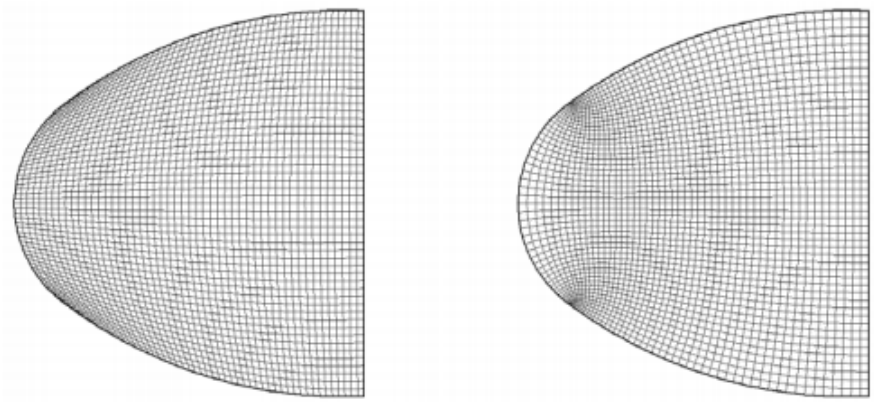


Рис. 1. Пример сетки трехмерного пространства при различных параметрах

В качестве алгоритма построения сетки предлагается модификация итерационного алгоритма, предложенного Коротковым А. А. в работе «Метод построения ортогональных сеток на плоскости, на гладкой трехмерной поверхности» [2], с расширением его на случай построения трёхмерной сетки. В основе метода лежит численное решение дифференциальных уравнений. Пример построенной сетки при различных параметрах пространства приведен на рис. 1 (см. выше).

Для построения графа на основе трёхмерной сетки достаточно соединить соседние узлы сетки ребрами. Для увеличения числа возможных путей и возможности лучшей оптимизации целевой функции кроме непосредственных соседних вершин ребрами предлагается соединить вершины, находящиеся на диагонали. Для учета параметра движущегося объекта предлагается в каждом узле сетки построить множество вершин графа, каждая из которых будет описывать множество конкретных состояний параметров. Примерами параметра могут являться вершина, из которой объект перешел в текущую вершину, его скорость, ускорение, угол поворота. Суммарное количество возможных состояний равно:

$$N = \prod_{f \in F} C(f),$$

где F – множество всех параметров, $C(f)$ – количество различных состояний параметра f.

Пример построения графа для сетки приведен на рис. 2 и 3. Для каждого узла сетки определен один параметр с двумя возможными состояниями, поэтому каждому узлу соответствует две вершины в графе. Ребра на графе проведены в вертикальном и горизонтальном направлениях.

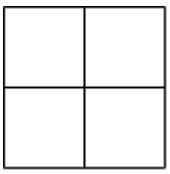


Рис. 2. Пример сетки для построения графа

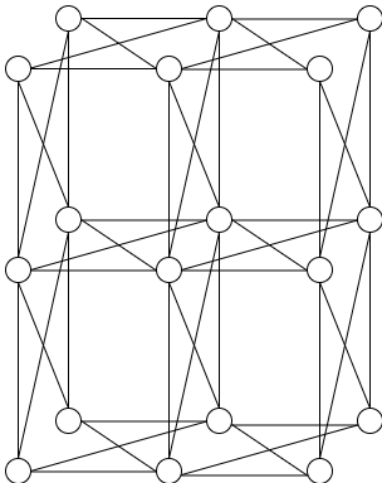


Рис. 3. Пример построенного графа на основе сетки

В качестве алгоритма поиска пути на взвешенном графе предлагается использовать алгоритм A*. Основной задачей при использовании этого алгоритма является подбор эвристической функции, оценивающей целевую функцию. Эвристическая функция h должна обладать свойством монотонности, то есть для любой вершины v_1 и ее потомка v_2 разность $h(v_1)$ и $h(v_2)$ не превышает фактического веса ребра $c(v_1, v_2)$ от v_1 до v_2, а эвристическая оценка целевого состояния равна нулю. В качестве эвристической функции предлагается использовать эвклидово расстояние, поскольку оно удовлетворяет требованию монотонности. Однако эта эвристическая функция может быть расширена для учета различных состояний в одной и той же пространственной точке, которой соответствует множество вершин графа. Например, может быть вычислена сложность поворота относительно текущего положения, скорости и ускорения движущегося объекта. Дальнейшее исследование может быть проведено с целью установления оптимальности эвклидова расстояния в качестве эвристической функции и возможного ее улучшения.

Список используемых источников

1. Галанин М. П., Щеглов И. А. Разработка и реализация алгоритмов трехмерной триангуляции сложных пространственных областей: прямые методы: отчет о НИР. Москва: ИПМ им. М. В. Келдыша РАН, 2006. 15 с.

2. Коротков А. А., Первичко В. А., Плотникова И. Г., Чуданов В. В. Метод построения ортогональных сеток на плоскости, на гладкой трехмерной поверхности // Институт проблем безопасности развития атомной энергетики РАН, № IBRAE-2006-06. М. : ИБРАЭ РАН, 2006. 98 экз. 47 с.

3. Nosrati M., Karimi R., Hasanvand H.A. Investigation of the * (Star) Search Algorithms: Characteristics, Methods and Approaches // World Applied Programming, Vol (2), No (4), 2012. PP. 251–256.

УДК 004.056.53
ГРНТИ 81.93.29

ВЫБОР И ОБОСНОВАНИЕ СРЕДСТВ РАЗРАБОТКИ СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ЯЗЫКАХ ВЫСОКОГО УРОВНЯ ДЛЯ ОТЕЧЕСТВЕННЫХ АППАРАТНО-ПРОГРАММНЫХ ПЛАТФОРМ

Г. С. Боголепов, А. А. Пронин, И. Ю. Скибинский

Военная академия связи

Рассматривается актуальная проблема перехода Российских Вооруженных Сил на отечественную аппаратно-программную платформу. Проблема переноса специального программного обеспечения решается путем переписывания программ на кроссплатформенные языки программирования. Целью работы является обеспечение эффективности мероприятий по модернизации существующего специального программного обеспечения при переходе на ОАПП. В статье представлена классификация средств разработки для отечественной аппаратно-программной платформы.

государственная тайна, автоматизированные системы управления, отечественная аппаратно-программная платформа, Astra Linux.

Задачи обеспечения безопасности и работоспособности информационных систем Вооруженных Сил России является приоритетным направлением деятельности. В связи с этим предпринимается переход с импортных аппаратно-программных платформ на отечественные аналоги [1].

Отечественные аппаратно-программные платформы состоят (рис., см. ниже) из аппаратной части, функционирующей на базе центрального процессора «Эльбрус» под управлением операционной системы семейства Linux. Для разработки специального программного обеспечения необходимо выбрать средства разработки на языках высокого уровня.

Выбор средств разработки для отечественной аппаратно-программной платформы ограничивается необходимостью защиты сведений, составляющих государственную тайну, а также операционной системой семейства Linux [2].

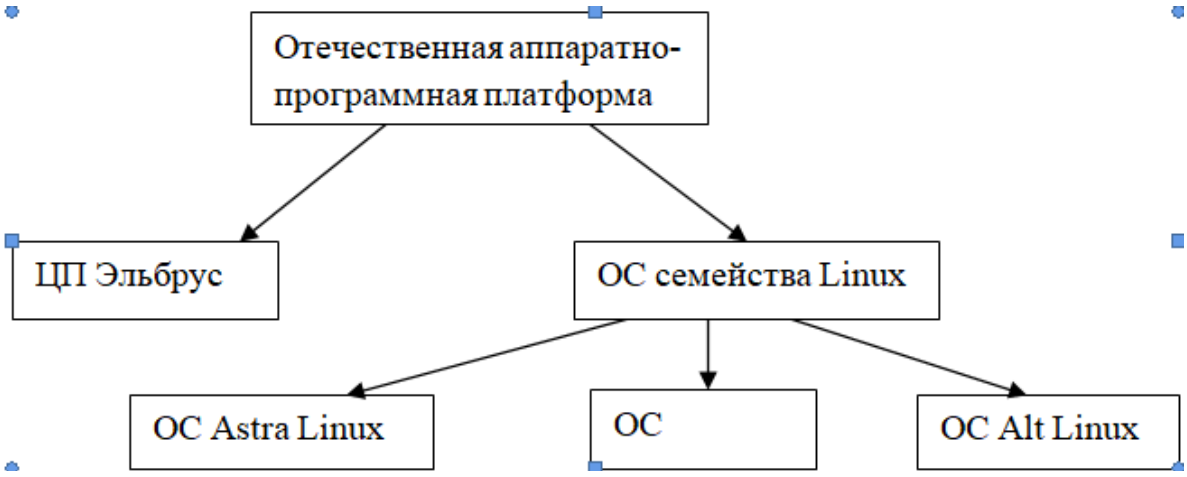


Рис. Состав отечественной аппаратно-программной платформы

Так в операционных системах Astra Linux, Эльбрус имеются инструменты компиляции кода C/C++: библиотеки, компиляторы, средства сборки, специальные пакеты для разработки программ и отладчики. Также есть возможность запустить программы на языке C# с помощью Mono, которое дает возможность работы с платформой Framework на любой системе. Для работы с языком Java загружается Java Development Kit, включающий в себя компилятор Java. Имеется возможность установить на данные системы компиляторы php, python, JavaScript.

Защита сведений, составляющих государственную тайну, является актуальной для Вооруженных Сил задачей. Она реализуется использованием программных средств, обладающих защитой от несанкционированного доступа к информации.

Степень защиты информации от несанкционированного доступа определяется сертификацией автоматизированных систем управления. Всего выделяют 9 классов защищенности автоматизированных систем (3Б, 3А, 2Б, 2А, 1Д, 1Г, 1В, 1Б, 1А), в зависимости от совокупности минимальных требований по защите. Критерии, по которым производится сертификация автоматизированных систем являются: подсистема управления доступом – идентификация, проверка и контроль доступа пользователей в систему, ЭВМ, программам, файлам; подсистема регистрации и учета – регистрация и учет входа пользователей в систему, запуска ими процессов и программ, модифицирование прав субъектов доступа, учет носителей информации, оповещение о попытках нарушения защиты; криптографическая подсистема – шифрование конфиденциальной информации [3].

Требования сертификации предусматривают полный доступ к исходному коду продукта для проверки на предмет наличия не декларированных возможностей.

Открытый исходный код распространяется на основе открытой лицензии. Открытая лицензия позволяет свободно и совместно использовать и изменять программное обеспечение. Это значит, что исходный код таких программ полностью доступен [4, 5].

В соответствии с требованиями безопасности выбор языков программирования определяется по их соответствию данным классам.

Языки программирования, имеющие открытый исходный код, являются: C, C++, Python, JavaScript, php, c#.

Программы на языке Java выполняются на виртуальной машине Java, что усложняет контроль над выполняемыми программами.

В языке JavaScript программы выполняются на встроенном движке и преобразуются в машинный код. Тем самым обусловлен полный контроль над исходным кодом программы. Однако данный язык имеет слабости в виде криптографической проблемы.

Язык C, являющийся прародителем всех языков программирования, имеет большое количество уязвимостей (переполнение буфера, доступ к произвольным областям памяти и т. д.) с открытым исходным кодом.

C++ – распространенный язык программирования с открытым исходным кодом, фрейморками и библиотеками. В отличие от языка C, имеет меньшее число уязвимостей и является достаточно безопасным в использовании.

Python имеет большую библиотеку с открытым исходным кодом. Имеет низкий показатель уязвимости высокой степени серьезности.

Язык php и его интерпретатор разрабатывается в рамках проекта с открытым кодом. Php имеет наибольшее число уязвимости среди вышеперечисленных языков.

Таким образом с учетом требований по защите государственной тайны на отечественной аппаратно-программной платформе распределение доступных языков программирования высокого уровня по требованиям к различным классам защищенности выглядит следующим образом:

Для класса 3А: C, C++, C#, Python, JavaScript.

Для класса 3Б: C, C++, C#, Python, Java, JavaScript, php.

Для класса 2А: C++, C# Python.

Для класса 2Б: C, C++, C#, Python, JavaScript, php.

Для класса 1Д: C++, C#, Python, JavaScript.

Для класса 1Г: C++, C#, Python, JavaScript.

Для класса 1В: C++, Python, JavaScript.

Для класса 1Б: C++, Python.

Для класса 1А: C++, Python.

Для работы с данными языками программирования на операционной системе Linux могут использоваться следующие среды разработки:

1) Qt Creator – кроссплатформенная IDE для разработки на языках C, C++. Разработана компанией Trolltech для осуществления работы с фреймворком Qt. Включает в себя графический интерфейс отладчика и средств разработки интерфейса через QtWidgets и QML.

2) Eric – свободно распространяемая интегрированная среда разработки для языков программирования Python и Ruby.

3) NetBeans IDE – свободная интегрированная среда для разработки приложений с использованием языков программирования Java, Python, PHP, JavaScript, C, C++ и других.

4) Code::Blocks – доступная кроссплатформенная среда разработки. Среда разработана на языке C++ и использует библиотеку wxWidgets. Дает возможность написания программ на языках программирования C, C++, Fortran.

5) Eclipse – интегрированная среда разработки модульных кроссплатформенных приложений. Данная среда является, прежде всего, платформой для разработки расширений. Так для нее создано Java Development Tools, C/C++ Development Tools.

Список используемых источников

1. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации – РД 50-680-296, утв. решением председателя Государственной технической комиссии при Президенте Рос. Федерации от 30.03.92 : ввод. в действие с 01.01.93. 29 с.

2. Бегаев А. Н., Кашин С. В., Зимненко С. А. Сертификация программного обеспечения и автоматизированных систем в различных системах сертификации. СПб. : Университет ИТМО, 2018. 45 с.

3. Васильков А. В., Васильков А. А., Васильков И. А. Информационные системы и их безопасность : учебное пособие. М. : Форум, 2011. 528 с.

4. Закалкин П. В., Мельников П. В. Система анализа программного обеспечения на предмет отсутствия недекларированных возможностей // Программная инженерия. 2018. Т. 9. № 2. С. 69–75.

5. Закалкин П. В., Мельников П. В., Горюнов М. Н., Борзов Р. В. Подход к разработке анализатора исходных текстов программ на основе использования LLVM // Программная инженерия. 2019. Т. 10. № 1. С. 14–19.

УДК 004.051
ГРНТИ 81.93.29

МЕТОДИКИ ОЦЕНКИ ЭФФЕКТИВНОСТИ ЗАТРАТ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИЙ

И. Б. Бондаренко, Г. В. Комков, С. Н. Шиманчук

Национальный исследовательский университет ИТМО

В статье исследованы методики оценки эффективности затрат на информационную безопасность предприятия. Рассмотрен пример из известной компании Microsoft, сделаны выводы о преимуществах и недостатках Total Cost of Ownership. Предложена методика оценки эффективности информационной безопасности на основе теории Total Cost of Ownership с внесением изменений для улучшения данной методики. Предложена методика, в которой методика ТСО вместе с методом расчета возврата от инвестиций дополняют друг друга, создавая оптимальную методику оценки эффективности затрат на информационную безопасность для российских организаций. Применение разработанной методики оценивания эффективности способствует увеличению прибыли предприятия, за счет сведения к минимуму прямых и косвенных затрат, которые не включаются в бюджет организации.

информационные технологии, информационная безопасность, методики оценки эффективности, подходы к обоснованию затрат на ИБ, ТСО, информационные риски.

В настоящее время информационные технологии (ИТ) имеют стремительное развитие, и как следствие их защита становится все сложнее. Применение современных методов информационной безопасности (ИБ) невозможно представить через 10 лет, также как сложно представить использование методов десятилетней давности сейчас.

Специалистам в области ИБ необходимо оспаривать необходимость инвестиций в программы и ресурсы ИБ. Это часто приводит к использованию точечных технологий, не учитывая сложность интеграции в существующие системы или полагаясь на традиционные устаревшие элементы управления ИБ и процессы, которые не адаптировались к изменяющимся угрозам. В результате, зачастую руководители организаций решаются вложить средства в комплексные программы обеспечения ИБ после того, как они уже столкнулись с инцидентом ИБ и понесли убытки.

Этого бы не случилось, если бы в организации была реализована грамотная и простая для восприятия оценка целесообразности затрат на систему ИБ. На сегодняшний день используются десятки таких моделей оценок, так как невозможно создать модель, подходящую всем. Самое главное,

что дали эти методики специалистам по ИБ – обоснование для руководства о необходимости затрат на повышение или поддержание на том же уровне системы ИБ.

Какие же цели преследует любая из систем оценок? Доктор технических наук Ажмухамедов И. М. в своих исследованиях на эту тему утверждал, что метод оценивания экономической эффективности должен:

– быть простым для восприятия, как с технической, так и с экономической точек зрения;

– быть применимым ко всем оценкам затрат (на приобретение техники, услуг, обучение персонала и т. д.);

– позволять моделировать ситуации, при которой существует несколько контрмер, направленных на предотвращение определенной угрозы, в разной степени влияющих на сокращение вероятности происшествия [1].

Набрав популярность в заграничных организациях, в последние годы в России самым распространенным методом оценки и обоснования экономических затрат на ИБ стал метод Total Cost of Ownership (оценка совокупной стоимости владения ИТ) – ТСО.

ТСО отражает разницу между ценой покупки и долгосрочной стоимостью. Этот анализ оказался в центре внимания, начиная с середины восьмидесятых из-за расходов на поддержку приобретения оборудования и программного обеспечения (ПО) [2]. Менеджеры обнаружили, что поддержка оборудования и ПО может в 5–8 раз превосходить стоимость самого оборудования или ПО.

Дополнительные затраты, которые должны быть добавлены к первоначальной стоимости для расчета общей стоимости владения:

– оборудование для ИТ (затраты на ремонт, стоимость технической поддержки, стоимость дополнительного оборудования и ПО, необходимых для использования данного оборудования);

– традиционное лицензирование ПО (исправление ошибок и обновление функций).

Создание КИС всегда затратное дело, а поддержание ее функционирования предполагает наличие постоянных и переменных затрат. Все эти затраты можно представить с помощью различных моделей ТСО [3].

На рис. (см. ниже) приведен пример модели ТСО, разработанной компанией Microsoft совместно с Interpose. Затраты на ИТ в ней разбиваются на две категории: прямые (бюджетные) и косвенные.

Прямые затраты планируются в рамках бюджета, где производятся заказы на покупку и оплачиваются счета-фактуры [4]. Это упрощает идентификацию и отслеживание прямых затрат. К таким затратам относятся: капитальные затраты, расходные материалы за период, плановое техническое обслуживание, контракты на обслуживание, корректирующее обслуживание, затраты на установку.

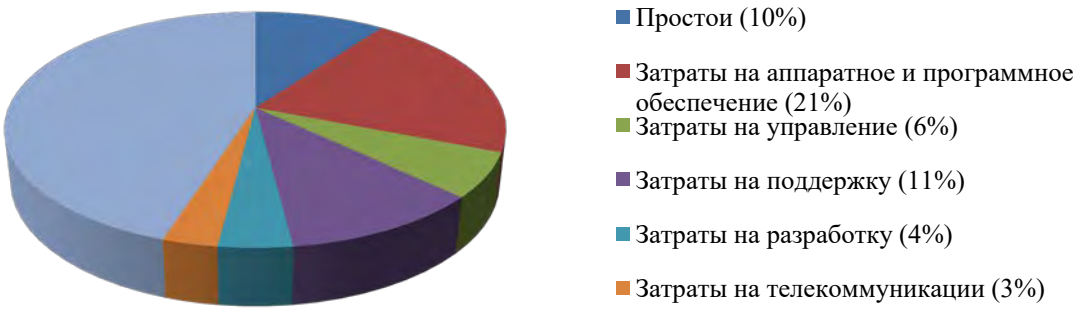


Рис. Структура затрат на ИТ организации

Косвенные затраты обычно скрыты и не включены в бюджет. Такие затраты составляют свыше 50 % средних расходов организаций на ИТ (см. рис.). Часто они не учитываются в ТСО. И даже если эти затраты учитываются в начале проекта, очень редко их контролируют [5]. К ним можно отнести: время простоя, если оборудование выходит из строя или в связи с текущими задачами обслуживания, обучение операторов, расходы на финансирование, стоимость утилизации.

Метод ТСО удобен во многом из-за возможности оценки совокупных затрат на ИТ [6]. В ТСО отображены экономические аспекты и, как правило, каждый показатель в нем соответствует различным статьям расходов.

Выбор оптимального метода зависит от ряда факторов, поэтому специалисты редко используют одну методику, чаще предпочитая комбинировать несколько методик вместе, чтобы добиться такой методики, которая идеально подойдет к масштабам инвестиций и срокам работ.

Для управления затратами на ИБ необходимы учет, анализ и контроль затрат на ИТ организации. Минимизация расходов и издержек при этом главный показатель для руководителей в целесообразности существующих методик оценки эффективности ИБ.

В таблице приведена методика оценки эффективности затрат на ИБ на основе метода ТСО.

ТАБЛИЦА. Методика оценки эффективности ИБ на основе планирования и контроля ТСО

№ п/п	Этапы планирования ТСО	Пояснение этапов
1	Определение «видимых» и «невидимых» затрат	При комплексном подходе прямые затраты на аппаратное и ПО, как правило, не превышают 30 % ТСО, но нельзя забывать о расходах на персонал и управление системой
2	Определение возможных косвенных затрат	Например, затраты, вызванные неработоспособностью КИС. Если у организации большой

№ п/п	Этапы планирования ТСО	Пояснение этапов
		дневной оборот, то стоимость отказа КИС будет очень высока
3	Распределение затрат по статьям	Распределение затрат по статьям, отталкиваясь от специфики, присущей данной отрасли, в которой работает организация
4	Расчет показателей ТСО	Для решения данной задачи можно воспользоваться дорогостоящим ПО (TCO Analyst, TCO Snapshot Tool) или самостоятельно подсчитать большинство затрат с помощью электронных таблиц
5	Выделение наиболее существенных статей расходов и оценка возможности снижения затрат на ИС	Действия по снижению затрат должны быть направлены, в первую очередь, именно на крупные расходы и издержки. Но не стоит забывать, что даже самые большие затраты могут быть объективными и целесообразными
6	Рассмотрение инструментов по снижению затрат	Инструменты для снижения затрат условно разделяются на технологические и процедурные. Технологические применяются на этапе эксплуатации системы, но их использование следует планировать заранее. Процедурные инструменты могут применяться как на этапах построения, так и на этапах функционирования ИС
7	Выбор эффективных инструментов по снижению затрат	Неверный выбор инструментов может повлечь за собой еще большие затраты, чем те, которые планировалось снизить
8	Применение инструментов по снижению затрат	Если все предыдущие шаги будут выполнены качественно и полноценно, то само применение станет заключительным этапом на пути оптимизации затрат на ИБ организации

Точное измерение эффективности выбранных мер ИБ требует от экспертов по ИБ всесторонней оценки профиля рисков всей инфраструктуры ИТ организации. Это означает выявление непосредственных рисков и их влияние на ключевые бизнес-операции, внедрение соответствующих мер контроля и процессов для устранения выявленных рисков, и создание надежной системы управления для снижения уровня рисков организации до приемлемого уровня [7].

Стремясь минимизировать затраты на всевозможные методики, специалисты ИТ-отделов, могут взять величину возврата от инвестиций (*Return on investment*, ROI), как простую методику оценки. Однако далеко не все ИТ-проекты организации могут быть достаточно просто связаны с конкретным доходом, поэтому этот метод не так популярен. В ROI не учитываются неопределенности и риски, поэтому корректнее учитывать влияния результатов отдельных ИТ-проектов на дальнейшее развитие бизнеса организации

в целом. Соответствующим показателем является рентабельность активов (*Return on assets*, ROA) [8]. Так как многие инвестиции в ИТ являются долгосрочными, то использование такого показателя, позволяет более корректно учитывать увеличение капитализации организации.

Использование методики TCO вместе с методом расчета возврата от инвестиций (TCO, как расходную часть, и ROI – расчетную) способствует достижению оптимального результата с минимальными затратами. Также данный подход помогает оценить степень отдачи от инвестиций в систему ИБ и может гарантировать, что каждый уровень бизнеса понимает, какие приоритеты лежат в плане риска, и какие гибкие инициативы в области ИБ должны быть созданы, чтобы позволить бизнесу соответствовать его целям цифровой трансформации.

Список используемых источников

1. Ажмухамедов И. М. Оценка экономической эффективности мер по обеспечению информационной безопасности // Вестник Астраханского государственного технического университета. 2011. № 1. С. 185–190.

2. Rob Wright. What does a CISO do now? It's a changing, increasingly vital role // Information Security magazine. 2015.

3. Peter Loshin. Cybersecurity roadmap: What's driving CISOs' agendas for 2018 // Information Security magazine. 2017.

4. Войтик А. И., Прожерин В. Г. Экономика информационной безопасности : учеб. пособие. СПб. : НИУ ИТМО, 2012. 115 с.

5. Jason Sparapani. A cloud provider ruminates on the role of a CISO // George Mason University. 2016.

6. Баутов А. Эффективность защиты информации [Электронный ресурс]. URL: http://www.osp.ru/os/2003/07-08/183282/ (дата обращения: 27.12.2014).

7. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. М. : Компания АйТи; ДМК Пресс, 2004. 384 с.

8. Тронников И. Б. Методы оценки информационной безопасности предприятия : автореф. дис. ... канд. техн. наук : 05.13.19 / Троников Игорь Борисович. СПб., 2012. 20 с.

УДК 519.652:004.622
ГРНТИ 27.41.15:20.23.19

ИСПОЛЬЗОВАНИЕ СПЛАЙНОВ НА ОСНОВЕ ДЕЛЬТА-ПРЕОБРАЗОВАНИЙ ВТОРОГО ПОРЯДКА НА РАЗНЫХ ЭТАПАХ И СТАДИЯХ ДАТА МАЙНИНГА

Ю. М. Бородянский, А. В. Дагаев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье описываются возможности использования сплайнов на основе дельта-преобразований второго порядка на этапах подготовки данных для анализа закономерностей при возможной неполноте имеющихся данных во времени с целью их восстановления, а также на этапе визуализации результатов. Сплайны на основе дельта-преобразований второго порядка, в отличии от классических, параметрических функций отличаются высоким быстродействием, что критично при обработке больших и сверх больших объемов данных.

интеллектуальный анализ данных, интерполяция, дата майнинг, сплайн, дельта-преобразования второго порядка.

В настоящее время активно развивается такая область человеческих знаний, как интеллектуальный анализ данных (англ. *Data Mining*). Современное общество производит и, главное, сохраняет огромное количество информации об окружающих нас объектах и, протекающих в реальном времени, экономических, социальных, научных и прочих процессах. Более того, разные заинтересованные лица или организации зачастую учитывают информацию об одних и тех же объектах только под разными углами интереса. Это несомненно приводит к многократному дублированию тех или иных свойств объектов, только эта информация по-разному структурирована и напрямую сравнить или проанализировать имеющиеся архивы невозможно.

Однако, эта особенность, теоретически, позволяет взглянуть на окружающие нас объекты, события, процессы более общим и широким взглядом. И именно для этого существует интеллектуальный анализ данных. Если говорить вкратце, то его суть состоит в поиске скрытых закономерностей, могущих принести практическую выгоду, между данными описывающими некоторую прикладную область. Существенной спецификой дата майнинга является необходимость работы с, в принципе, неограниченным объемом данных. В общих чертах сама процедура дата майнинга приведена

на рис. 1. Как видно из приведенных этапов – это итерационный процесс, в котором очень важную роль, кроме несомненно самих методов анализа, играет качество и релевантность данных, на базе которых и осуществляется анализ.

Какие же сложности можно выделить на этапе подготовки данных для анализа? Во-первых, это необходимость объединить в единую структуру данные из разных архивов, имеющих совершенно свои структурные особенности, начиная от отсутствия некоторых необходимых элементов данных и, заканчивая отличающейся размерностью. Во-вторых, необходимые данные могут не совпадать по временной шкале или располагаться через различные временные интервалы. Наконец, в разных архивах просто могут быть ошибки и повреждения отдельных областей.

Рис. 1. Этапы дата майнинга

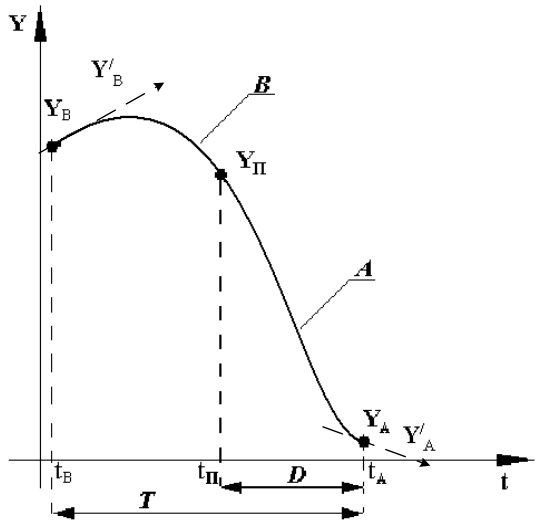


Рис. 2. Интерполяционная кривая, состоящая из траекторий A и B

Не претендуя на решение всех выше перечисленных и многих не указанных проблем 3-го этапа дата майнинга, в этой статье предлагается метод интерполяции сплайнов на основе дельта преобразований второго порядка, оптимизированных по быстродействию и точности. Использовать его предлагается с целью производительного заполнения разрывов в подготавливаемых данных. Эти разрывы могут образоваться как в случае сомнений в достоверности некоторых объемов данных, так и для восстановления единой системы временных интервалов в данных из разных информационных источников. Естественно речь идет о численных данных.

Суть алгоритма интерполяции на основе дельта-преобразований заключается в следующем [1]. Пусть нам даны 2-е точки Y_b и Y_a, а также нам известны производные в этих точках Y'_b и Y'_a. Тогда любую интерполяционную кривую, в общем случае, можно разбить на две траектории: B – торможение и A – ускорение. Общий вид такой кривой представлен на рис. 2.

Значение i+1-й точки кривой Y_{i+1} и её производной Y'_{i+1} рассчитывается по следующим формулам:

$$Y'_{i+1} * \nabla t = Y'_i * \nabla t + c^* \Delta,$$

$$Y_{i+1} = Y_{i+1} + Y'_i * \nabla t + 0,5 * c^* \Delta,$$

$$c^* = |P|,$$

$$\Delta = -sign(P), \qquad i \le T - D,$$

$$\Delta = sign(P), \qquad i > T - D,$$

$$D = \frac{Y'_A - Y'_B + TP}{2P}, \qquad 0 \le D \le T,$$

$$P = \frac{-(Y_B - Y_A - 0,5T(Y'_B + Y'_A)) \pm \sqrt{(Y_B - Y_A - 0,5T(Y'_B + Y'_A))^2 + 0,25T^2(Y'_B - Y'_A)^2}}{0,5T^2},$$

где c^* – постоянный коэффициент, определяющий вес кванта модуляции; ∇t – шаг дискретизации независимой переменной, Δ – знак кванта модуляции, T – интервал между узлами интерполяции; D – расположение точки переключения знака кванта модуляции; P – квант приращения производной.

Применяя данный алгоритм построения кривой, можно также интерполировать поверхность. На рис. 2 и 3 представлены 2 этапа этого процесса. На первом этапе вдоль одной из осей строятся опорные кривые на базе имеющейся информации. А затем, на втором этапе, с любой требуемой дискретизацией интерполируются кривые вдоль другой оси, что и создает требуемую поверхность.

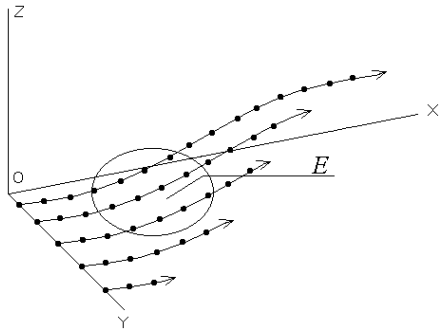


Рис. 2. 1-й этап построения поверхности на основе описанного выше алгоритма с применением дельта-преобразований 2-го порядка

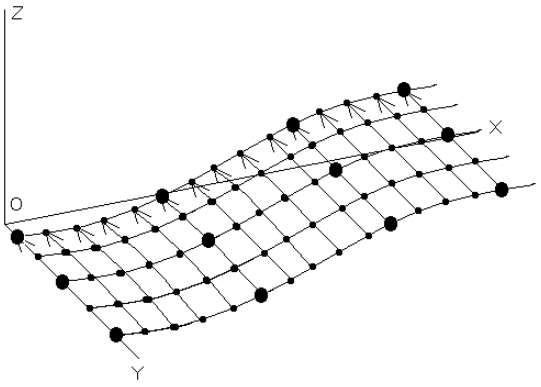


Рис. 3. 2-й этап построения поверхности на основе описанного выше алгоритма с применением дельта-преобразований 2-го порядка

Было произведено сравнение вычислительных затрат предлагаемого алгоритма и целого ряда популярных аналогов для построения кривых и поверхностей [2, 3 ,4]. При этом учитывались затраты на подготовку параметров алгоритмов и вычисление самих точек интерполяции. С учетом современного развития вычислительной техники затраты на все арифметические операции приравниваются. Из таблицы 1 видно, что предлагаемый метод в разы превосходит аналоги по быстродействию при построении отдельной точки интерполяции и занимает не самое лучшее место при подготовке параметров. Однако, предполагая, что количество точек интерполяции на порядки превышает количество интервалов интерполяции, общие вычислительные затраты у предлагаемого метода будут существенно меньше аналогов.

ТАБЛИЦА 1. Вычислительные издержки для интерполяции кривой

Алгоритмы интерполяции	Дельта-преобразования	Кубический сплайн	Кубический B-сплайн	Многочлен Эрмита
Издержки на сбор параметров	$38(r-1)-8$	$31r-23$	$98+36(r-1)+$ $+2(r+2)3/3$	$9(r-2)$
Издержки на подсчет одной интерполируемой точки	5–6	19	43	24

r – количество интервалов интерполяции.

Анализ таблицы 2 показывает, что и на первом этапе реализации алгоритма затраты самые маленькие по сравнению с аналогами (64 операции). На втором же этапе, самом массовом, выигрыш ещё больше (5 операций).

ТАБЛИЦА 2. Вычислительные издержки для интерполяции поверхности

Алгоритмы интерполяции	Издержки на сбор параметров	Издержки на подсчет одной интерполируемой точки
Дельта-преобразования	$9(s-2)r+31(r-1)s$	64(5)
Кубический сплайн	$(31s-23)(r+2)+(31r-23)2s$	77
Кубический B-сплайн	$36r+52rs+2(rs)^3/3$	119
Многочлен Эрмита	$9(r-2)(s+2)+18r(s-2)$	69

r, s – количество интервалов интерполяции по соответствующим осям.

Список используемых источников

1. Бородянский Ю. М., Кравченко П. П. Сплайн функции на основе дельта-преобразований второго порядка и возможности их применения в технических системах // Отдел депонирования ВИНИТИ, ТРТУ. – Таганрог, 2002, Деп. в ВИНИТИ 06.11.2002, № 1924-В2002.

2. Де Бор К. Практическое руководство по сплайнам. М. : Радио и связь, 1985. 304 с.

3. Шикин Е. В., Плис А. И. Кривые и поверхности на экране компьютера. М. : Диалог-МИФИ, 1996. 240 с.

4. Алберг Дж., Нильсон Э., Уолш Дж. Теория сплайнов и их приложения. М. : Мир, 1972. 319 с.

УДК 004.032.26, 519.685
ГРНТИ 28.23.37, 50.51.15

ИСКУССТВЕННЫЕ НЕЙРОННЫЕ СЕТИ В ВОПРОСАХ ПАРАМЕТРИЧЕСКОЙ ОПТИМИЗАЦИИ СЛОЖНЫХ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ ОПТИЧЕСКОГО ПРОИЗВОДСТВА

В. В. Ботяков, А. Д. Резницкий, Д. В. Соловьёв, Н. Ю. Топорков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются вопросы математического моделирования сложного технологического процесса вытягивания оптического волокна из заготовки в виртуальном пространстве компьютера. Прорабатывается вопрос параметрической оптимизации данного техпроцесса с помощью технологий ИНС.

системы автоматизированного проектирования, искусственные нейронные сети, математическое обеспечение, оптическое волокно, многослойный персептрон.

В настоящее время одним из приоритетных национальных проектов является программа «Цифровая экономика». Данная программа нацелена на развитие целого ряда сфер деятельности, сопряжённых с экономикой, информационными технологиями, производством высокотехнологического оборудования и информационной инфраструктурой. Для реализации данного национального проекта необходимо развитие сопутствующих технологий, входящих в рамки данной программы [1]. Данной технологией, неразрывно связанной с направлениями развития в программе, являются нейротехнологии, а также технологии, имеющие в основе своей применение искусственного интеллекта в различных процессах.

Ускоренный рост и динамичное развитие технологий приводит к необходимости ускорения и оптимизации процессов передачи увеличивающегося объема данных на большие расстояния. Одной из перспективных и стремительно развивающихся технологий является передача данных

при помощи волоконно-оптического кабеля (ВОК) [2]. Оптическое волокно (ОВ) представляет собой нить из оптически прозрачного материала – кварцевого стекла – использующего принцип полного внутреннего отражения для передачи оптических сигналов на большие расстояния со скоростью в разы выше, по сравнению с предшествующими технологиями. В связи с широким распространением технологии и достаточно трудоёмким процессом производства основного элемента – оптического волокна, предпринимаются попытки оптимизации и снижения финансовых затрат при производстве оптического волокна.

Как показывает практика, одновременное применение трехслойного персептрона и алгоритма обратного распространения ошибки представляет собой инструмент, позволяющий решить комплекс задач, не поддающихся адекватной формализации, имеющих элементы неопределенности и не формализуемых традиционными математическими методами. В качестве такой задачи нами выбран сложный технологический процесс (ТП) производства оптического волокна методом вытяжки из заготовки (рис. 1).

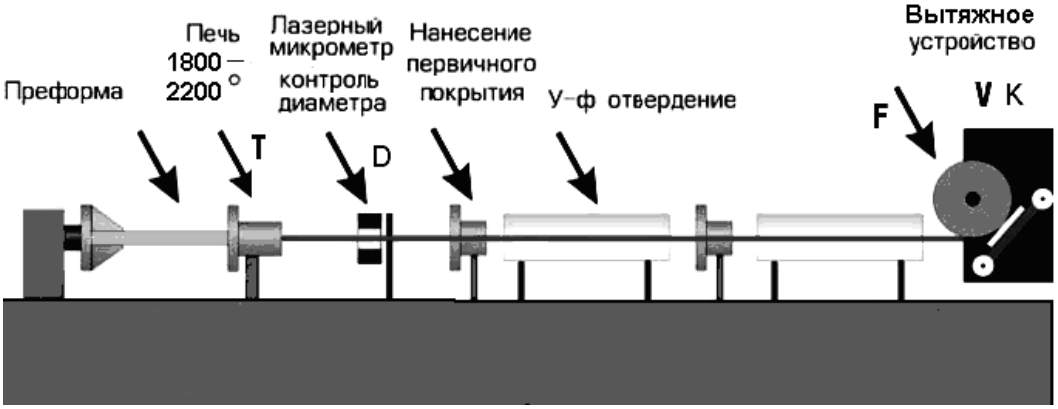


Рис. 1. Схема установки для вытяжки из заготовки оптического волокна, включающая в себя устройство вытягивания и намотки волокна (параметр *V*), печь нагрева (параметр *T*), датчик для получения данных диаметра волокна (параметр *D*), датчика параметра натяжения волокна (параметр F)

Как и многие технологические процессы производства материалов оптики, выбранный ТП обладает следующими характеристиками:

- малая информативность ТП из-за трудности или невозможности контроля определённых параметров на выходе;
- сложности явлений физико-химического рода, происходящих в ходе ТП, что в большой степени затрудняет построение аналитических и математических моделей, описывающих ТП;
- нестационарность ТП, есть не что иное, как итог протекания физических процессов в ходе ТП и изменения параметров, показывающих изменчивость свойств оборудования ТП, применяемого для производства во времени;

- параметрическая распределённость, возникающая из-за наличия в техпроцессе потоков оптических материалов, находящихся в движении, а в свою очередь контроль величин происходит в локальных зонах или косвенными методами;

- высокая протяженность и большое количество стадий техпроцесса производства оптических материалов.

На рис. 1 (см. выше) показана схема установки вытяжки – типовой набор компонентов для производства (вытягивания), в некоторых случаях производители оборудования включают в систему производства другие компоненты, представляющие собой: системы определения прочности волокна, системы датчиков, измеряющие величину затухания светового потока и прочие. В показанном нами случае прочность волокна на разрыв и затухание света описываются комплексным значением, являющимся показателем качества К. Каждый из перечисленных выше компонентов также входит в единую промышленную систему для изготовления оптического волокна.

Процесс изготовления оптических волокон промышленным путём состоит из следующих этапов: вначале заготовка закрепляется в специализированном устройстве, входящем в производственный комплекс для получения (вытягивания), для исключения сдвига или непроизвольного движения заготовки. Позиция фиксатора регулируется в вертикальном положении посредством использования подающего механизма. Конец заготовки подвергается нагреву до температуры 2 000°C, с целью вытягивания волокна из находящейся в расплавленном состоянии заготовки. Для достижения неизменности диаметра световода оптического волокна и его соответствия необходимой контролируемой величине требуется обеспечить возможность высокоточной и постоянной регулировки скорости вытяжки и механизма подачи, путем применения системы автоматического управления [3].

Величина усилия для вытягивания волокон имеет непосредственную зависимость от температурного коридора (диапазона температур). В ситуации, где пластичное деформирование материала становится невозможным из-за низкой температуры обжига заготовки или же, если скорость вытяжки превышает допустимую, и расплавленная заготовка приобретает упругопластичные свойства, то происходит разрыв заготовки, вследствие чего процедура вытяжки не может быть выполнена. Также следует отметить, что скорость вытяжки оптических волокон напрямую зависима от усилия вытяжки в процессе производства.

По результатам нашей работы была выведена математическая модель ТП вытяжки готового оптического волокна из заготовки, которая приведена ниже:

$$V_в = \frac{AF}{\eta_0} e^{\frac{E_a}{RT}}.$$

где η_0 – вязкость в центре волокна; E_a – энергия активации вязкого течения; T – температура в абсолютной величине; R – газовая постоянная; F – сила натяжения; A – постоянная для данного типа волокна, в которую входят геометрические размеры; $V_в$ – скорость вытяжки волокна.

Указанная математическая зависимость параметров ТП вытягивания оптических волокон была применена далее, по ней были сформированы обучающие наборы для искусственной нейронной сети на первоначальном этапе работы. Далее в качестве обучающих наборов были использованы данные, полученные с производственной установки и оборудования, входящего в состав системы производства оптического волокна. После этого была подготовлена к применению нейросетевая структура, направленная на решение задачи параметрической оптимизации ТП вытяжки оптического волокна.

Из научных источников известно [4], что для сети количество нейронов, а также слоёв, входящих в неё, имеет прямую зависимость от вычислительных возможностей нейронной сети. В частности, чем меньше количество слоёв и нейронов, тем быстрее нейросеть проходит процесс обучения, однако качество получаемых решений крайне низко. С учетом известных нам факторов, кардинально влияющих на скорость вытягивания и качественные характеристики получаемого оптического волокна, в дальнейшем решено было взять за основу топологию нейронной сети, а именно схему трёхслойного персептрона с единичным скрытым слоем.

В используемой модели нейросети количество входных данных (температура печи нагрева – T, сила натяжения вытягивающего устройства – F, диаметр волокна на выходе – D) равно трём, что отвечает количеству нейронов входного слоя. В выходном слое находится два нейрона, что совпадает с количеством выходных данных (скорость вытягивания – V, комплексный параметр качества – K). Величина нейронов в скрытом слое была выбрана опытным путем и равна восьми, являясь оптимумом с точки зрения качества и временных затрат, необходимых получения готового решения. Выработанная топология искусственной нейронной сети изображена на рис. 2.

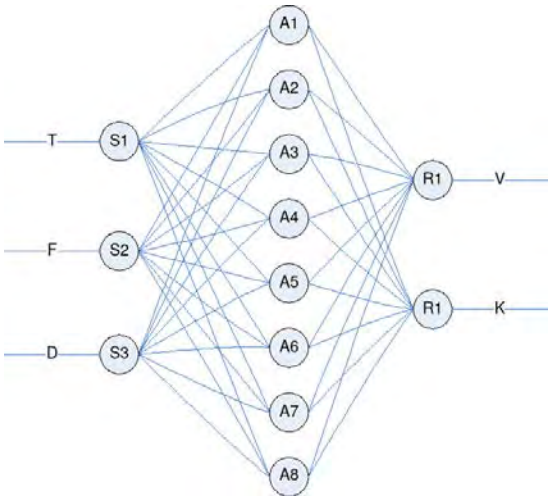


Рис. 2. Топология нейронной сети

Исходными данными первой выборки направленной на обучение нейросети являлись наборы параметров силы натяжения (параметр *F*), скорости вытяжки волокна (параметр *V*) и температура нагрева печи (параметр *T*), полученные на основе математической модели сложного технологического процесса вытяжки оптических волокон из заготовки. Критерий качества был косвенно учтён путем наложения ограничений на интервалы изменения параметров технологического процесса вытяжки, при которых известно, что оптическое волокно не разрывается и содержит минимум оптических и структурных дефектов. Вторая обучающая выборка формировалась путем экспорта информации с технологического оборудования для производства волокна, размещенного в лаборатории волоконной оптики.

На рис. 3 показаны результаты работы нейросетевого метода параметрической оптимизации сложного ТП по вытягиванию из подготовленной заготовки ОВ. В левой части графиком показана доля выборки для обучения, представленная наборами в количестве 20 штук, для волокон с диаметром 125 мкм. В ней содержатся данные о скорости подачи заготовки, скорости вытяжки волокна, температуре нагрева печи и численному количеству дефектов оптического волокна, полученного при производстве. В правой части рис. 3 приведены результаты работы выработанного нами нейросетевого алгоритма. При этом, как видно из графиков, величина ошибки оказалась не более одного процента. Одновременно над выборками был проведён анализ на выполнение критерия согласия Стьюдента. Вышеназванный критерий указал на адекватность выработанного нейросетевого метода параметрической оптимизации сложных техпроцессов производства оптических материалов, одним из которых и является показанный в настоящей статье ТП вытяжки ОВ.

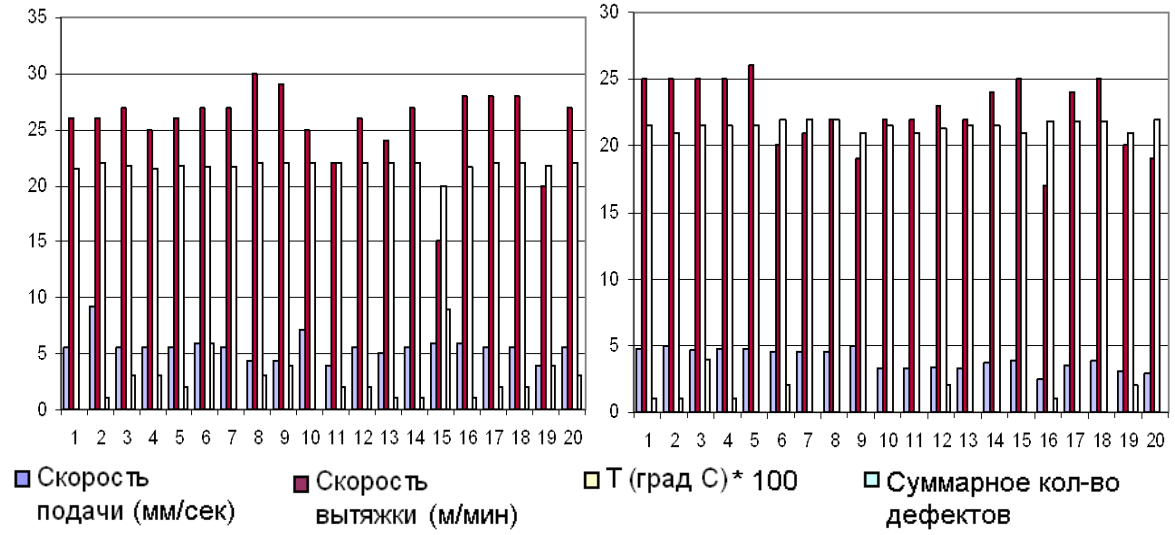


Рис. 3. Графики обучающей выборки (слева)
и результатов работы нейросетевого алгоритма (справа).

Список используемых источников

1. Распоряжение Правительства РФ от 28.07.2017 N 1632-р «Об утверждении программы "Цифровая экономика Российской Федерации».
2. Родина О. В. Волоконно-оптические линии связи: практическое руководство. М.: Горячая Линия – Телеком, 2009. 401 с.
3. Методы изготовления оптоволокна. Общее описание [Электронный ресурс]. URL: http://laser-portal.ru/content_368 (дата обращения: 25.03.2020).
4. Уоссермен Ф. Нейрокомпьютерная техника: Теория и практика. М.: Мир, 1992. 236 с.

УДК 004.056.57
ГРНТИ 81.93.29

МЕТОД ОБНАРУЖЕНИЯ НИЗКОИНТЕНСИВНЫХ DOS-АТАК НА ИНФОРМАЦИОННУЮ СИСТЕМУ С ПОМОЩЬЮ АЛГОРИТМОВ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

В. В. Ботяков, А. Д. Резницкий, Д. В. Соловьев, Н. Ю. Топорков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Проблема защиты информационных систем от атак на отказ в обслуживании становится наиболее актуальной среди большинства других задач по обеспечению безопасности информационных систем. Защита таких систем становиться трудоёмкой и ресурсоёмкой задачей, остро поставлен вопрос разработки принципиально новых систем обнаружения атак, построенных на алгоритмах искусственного интеллекта.

нейронные сети, отказ в обслуживании, персептрон, карты Кохонена.

На данный момент представляется невозможным функционирование любого предприятия без информационной системы. И тем важнее представляется задача по защите информационных систем. Однако многие системы по обнаружению атак опираются на методы имеющие существенные недостатки так сигнатурный анализ или анализ с помощью правил и непригодны для защиты от новых или неучтенных при задании правил атак. Поэтому в последние годы активно развивается эвристический анализ.

Использование такого анализа позволяет обнаружить атаки ранее неизвестные и не попадающие ни под одну сигнатуру. Для увеличения эффективности эвристического анализа предлагается использовать нейронные сети.

Обнаружение атак типа «отказ в обслуживании» особенно актуально из-за характеристик подобных атак: простоты проведения, относительно маленьких затрат и большой сложности распознания атаки до её завершения. Такие атаки проводятся злоумышленниками с целью устранения возможности получить доступ к сервису со стороны легитимных, настоящих клиентов, путем занятия всех портов и очередей на атакуемом устройстве с помощью вредоносного использования легальных пакетов, что видно на рис. 1. Для обнаружения такой атаки невозможно использовать сигнатурные методы и гораздо более разумно обратиться к математическому аппарату искусственных нейронных сетей [1].

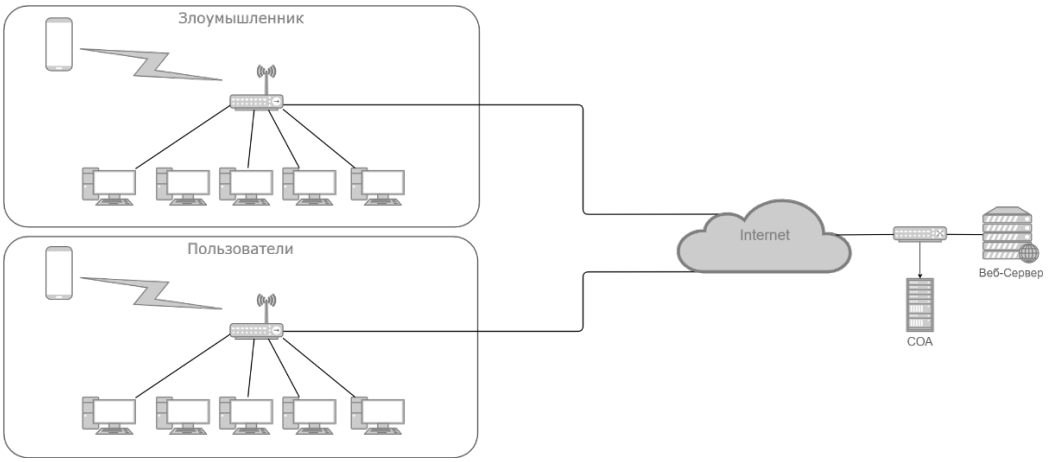


Рис. 1. Типовая схема работы предполагаемой системы

Нейронные сети – это компьютерное воспроизведение математической модели основных свойств биологической структуры мозга. Искусственные нейронные сети обладают тем же преимуществом что и сам мозг: нейронные сети обучаемы и могут меняться в зависимости от информации, поступающей из вне вовремя процесса обучения. Нейронные сети способны обрабатывать даже информацию ранее им не встречавшуюся и успешно строить предположения основываясь на совокупности признаков поступившей информации.

В работе предлагается использовать гибридную систему обнаружения атак, основанную на самоорганизующихся картах Кохонена и многослойном персептроне. Выбор такой архитектуры объясняется эффективным распределением ресурсов и времени для обнаружения атаки на информационную систему.

Карты Кохонена состоят из узлов или нейронов, каждый узел описывается двумя векторами: вектором весов и вектором координат. Визуально это отображается с помощью шестиугольных или квадратных ячеек.

Как видно на рис. 2 персептрон состоит из нескольких уровней нейронов, называемых слоями. Первый слой называется входным и принимает

начальные данные, которые следует обработать. Далее информация поступает на скрытые слои, где происходит её обработка. На конечном этапе выходной слой выдает результат работы нейронной сети [2].

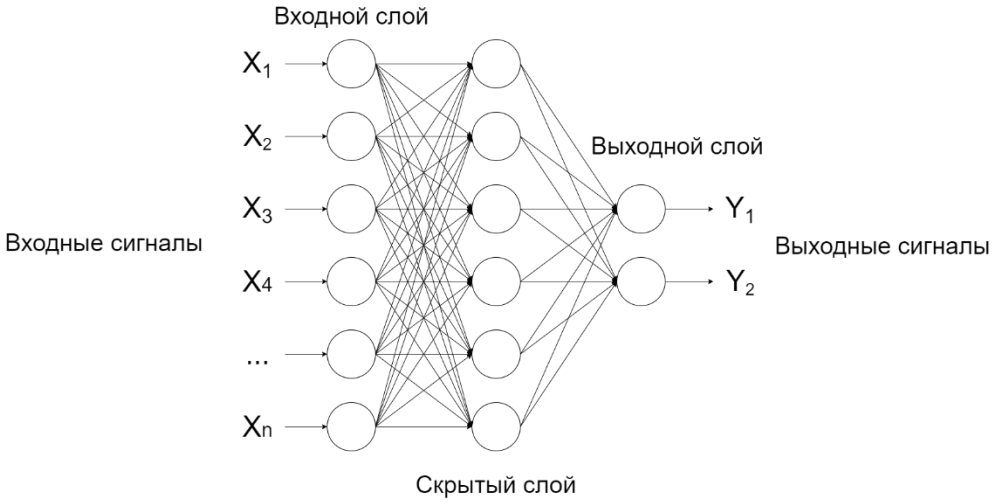


Рис. 2. Общая схема трёхслойного персептрона

Трафик, проходящий через нейронную сеть, имеет определенные атрибуты и характеристики. На основе таких характеристик принимается решение о легитимности трафика. После получения трафика на вход система с помощью карт Кохонена обобщает информацию и передает на вход персептрону.

Использование нейронной сети решает задачу классификации и определения вредоносного трафика. Работа системы происходит в двух режимах: режим обучения и режим обнаружения атак.

Обучение нейронной сети опирается на обучающую информацию, представленную трафиком, записанным заранее и заранее определенным в одну из двух категорий: легитимный или зараженный. Трафик записывается в два этапа: запись чистого трафика и запись трафика с атакой. Первый производиться под нагрузкой с интенсивным потоком обращений к серверу. Второй имеет более слабый поток легитимного трафика, но содержит атаку и нагружает систему сильнее. Обучающий трафик проходит через сеть Кохонена, где он кластеризуется и представляется в виде выходной информации, приведенной в бинарный вид. Далее данные поступают на входной слой персептрона и по этим данным производиться расчет первоначальных весов нейронов.

Выходные данные персептрона могут иметь погрешность пока он не «натренирован». Для настройки весов в процессе обучения использовался метод обратного распространения ошибки. В процессе обучения весовые коэффициенты нейронов изменяются. Постепенно количество ошибок, допущенных системой, падает.

При работе в режиме обнаружения угроз, система получает зеркалируемый трафик, определяет зараженный это трафик или легитимный и передает данные администратору.

Результаты работы. Для экспериментов был построен стенд со следящими характеристиками. В качестве аппаратной площадки использовался персональный компьютер на базе процессора Intel Core i5-3450 с тактовой частотой 3,1 ГГц, объемом оперативной памяти в размере 8 Гб и высокоскоростной твердотельный жесткий диск объемом 500 Гб. На компьютер был установлен Virtualbox, бесплатно распространяемый продукт компании Oracle. Атакуемый сервер – Ubuntu server и программное обеспечение web-сервер Nginx. Атакующий сервер – Kali Linux и программное обеспечение Slowhttptest. Сервер сбора данных поведения трафика в сети – Windows 10 Pro x64 с программным обеспечением WireShark.

Оценка эффективности производилась с использованием методологии тестирования OWASP Testing Guide.

На тестовой выборке системой были получены следующие результаты: как показано на рис. 3 и 4 величина ошибки первого рода составила 4,05 %, а величина ошибки второго рода составила 2,12 %. Таким образом, количество пропущенных атак составило 2,12 %, а количество ложных срабатываний составило 4,05 %. Метод обнаружения атак на информационную систему с помощью алгоритмов искусственных нейронных сетей позволяет эффективно и своевременно выявлять принадлежность трафика к атаке.

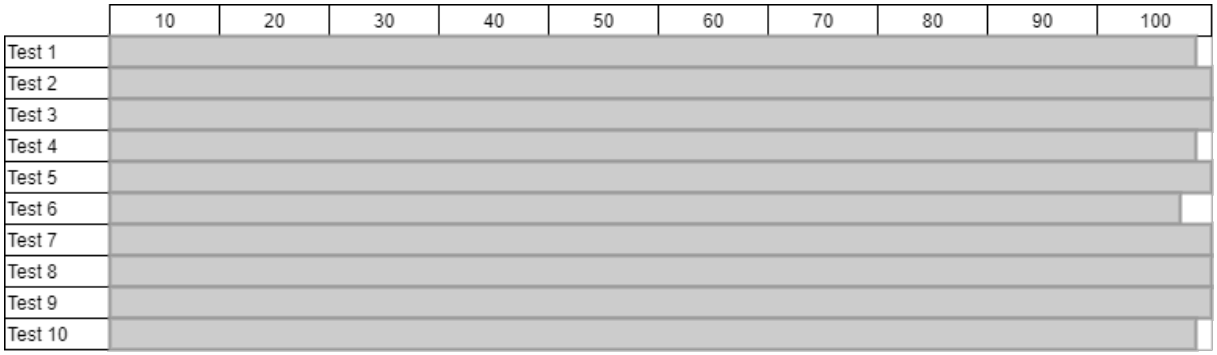


Рис. 3. Успешность прохождения тестов ложного срабатывания

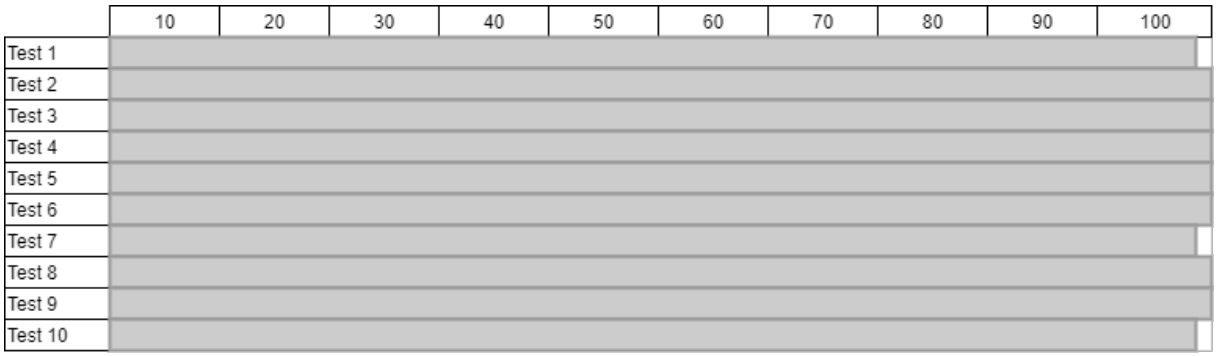


Рис. 4. Успешность прохождения тестов пропускания ошибки

Список используемых источников

1. Тарасов Я. В. Исследование применения нейронных сетей для обнаружения низкоинтенсивных DDoS-атак прикладного уровня // Вопросы кибербезопасности. 2017. № 5 (24). С. 23–28.
2. Мустафаев А. Г. Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика // Вопросы безопасности. 2016. № 2. С. 1–7.
3. Зинкевич А. В., Еремин К. Ю. Система обнаружения вторжений с использованием нейронной сети для анализа данных // Электронное научное издание «Ученые заметки ТОГУ». 2017. Том 8. № 4. С. 514–519.

УДК 004.056.57
ГРНТИ 81.93.29

МЕТОДЫ ПРОВЕДЕНИЯ РАСПРЕДЕЛЕННЫХ DOS-АТАК НА ИНФОРМАЦИОННУЮ СИСТЕМУ

В. В. Ботяков, А. Д. Резницкий, Д. В. Соловьев, Н. Ю. Топорков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются вопросы обеспечения информационной безопасности информационных систем от атак на отказ в обслуживании, приводится классификация таких атак.

низкоинтенсивные DDoS-атаки, ботнет, RUDY, SlowLoris, HTTP-flood.

В последние время можно наблюдать постоянное увеличение количества DDoS-атак и убытков от них. Жертвами хакеров могут стать как большие организации, так и маленькие компании, а финансовые потери могут быть существенными. 20 % компаний с по крайней мере 50 сотрудниками хотя бы раз подвергались DoS или DDoS-атаке. А средние финансовые потери от DDoS-атаки для крупной компании (1500 сотрудников и более) составляют около 417 тысяч долларов [1]. Целью распределенных атак типа «отказ в обслуживании» всё больше становятся web-ресурсы малого размера. Это обуславливается отказом жертв атаки от использования средств провайдеров для обнаружения и отражения таких атак ввиду экономической нецелесообразности.

Новым инструментом хакеров в последнее время являются низкоинтенсивные DDoS-атаки или атаки типа «отказ в обслуживании» малой мощности. Особенностью таких атак является сложность их обнаружения. Трафик, возникающий при такой атаке, может не отличаться от нормального

сеанса работы реальных пользователей. Поэтому такие атаки наиболее опасны и требуют особых мер для их предотвращения [2].

DoS-атака это атака на информационную систему, целью которой является доведение ее до отказа, то есть создание для системы таких условий, в результате которых клиенты этой системы не смогут получить доступ к предоставляемым системой ресурсам или доступ будет затруднен [3]. DDoS-атака это распределенная DoS-атака, то есть выполняемая с большого числа устройств.

Как показывает практика, многие устройства, подключенные интернету, являются участниками DDoS-атак, являясь узлами ботнета – сети компьютеров, управляемых хакерами удаленно (рис. 1). Хакер использует троянские вирусы, чтобы нарушить безопасность нескольких компьютеров и подключить их к сети в злонамеренных целях, таких как проведение DDoS-атак с их помощью.

Рис. 1. Структура ботнета

Как уже было сказано, наиболее эффективными и опасными являются низкоинтенсивные DDoS-атаки. Низкоинтенсивная DDoS-атака характеризуется длительными интервалами между передачей пакетов в одной сессии и значительной фрагментацией пакетов в данной сессии для передачи контентной информации. Возможность проведения низкоинтенсивной атаки объясняется уязвимостью протокола HTTP и необходимостью обязательного ожидания сервером конца передачи POST-запроса. При реализации низкоинтенсивной DDoS-атаки злоумышленник фрагментирует POST-запрос на пакеты малой длины и отправляет их серверу с интервалом меньшим, чем время ожидания окончания соединения. В итоге сервер должен ждать завершение приема POST-запросов хакера, в товремя как запросы легитимных клиентов игнорируются ввиду отсутствия свободного ресурса.

Характерными представителями низкоинтенсивных DoS-атак являются атаки RUDY, SlowLoris и HTTP-flood.

Принцип атаки R.U.D.Y. (*AreYouDeadYet*) основан на обычной работе HTTP-протокола при обработке POST-запросов.

Допустим, есть web-сайт, а на нём форма для ввода данных. Клиенту нужно заполнить эту форму. Такая ситуация типична для банков, интернет-магазинов, различных сайтов бронирования билетов, любого web-ресурса, где нужна аутентификация. Когда легитимный клиент заполняет web-форму, на сервер отправляется несколько пакетов, сессия с web-сервером

завершается, а ресурсы после этого высвобождаются. Сервер становится доступен для запросов других клиентов.

А вот как действует хакер, проводящий атаку RUDY. Данные, которые должны быть отправлены на web-сервер, разделяются на большое количество пакетов, каждый из которых содержит только один байт данных. Хакер отправляет запросы к серверу со случайным интервалом между ними, что не дает серверу возможность закрыть сессию, так как передача данных еще не окончена (рис. 2).

Сервер становится недоступен для правомочных клиентов в результате выполнения нескольких тысяч таких запросов за несколько минут. Для выведения ресурса из строя не требуется огромного объема трафика или большого количества пакетов. Все запросы здесь полностью легитимны. При такой атаке хакер создает видимость того, что он – клиент с медленным каналом связи. Цель хакера достигнута – web-ресурс недоступен. Такой уязвимости подвержен практически любой web-сайт [4].

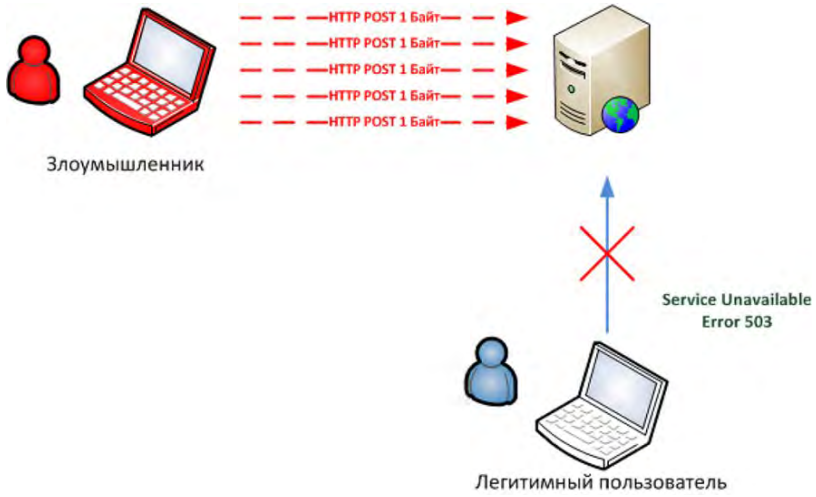


Рис. 2. Схема атаки типа RUDY

Инструмент SlowLoris, так же, как и предыдущий, базируется на обычном поведении HTTP-протокола при обработке запросов. Чтобы завершить HTTP-сессию, нужно отправить соответствующую последовательность. Легитимный клиент так и поступает. Нормальный GET-запрос на получение данных с web-сервера должен состоять из одного пакета, а завершается он специальной последовательностью в конце для закрытия сессии.

Суть атаки состоит в следующем: хакер создает множество подключений к серверу-цели, а соединения не закрываются при этом, так как в его запросе нет соответствующей последовательности символов, которая должна привести к разрыву сессии (рис. 3).

В итоге ресурсы сервера будут исчерпаны, и у легитимных пользователей не будет возможности подключиться. Таким образом хакер достиг своей

цели – сайт недоступен. Мы снова видим, что для успешной атаки не требуется огромного по объему трафика или большое количество пакетов. Все запросы здесь полностью легитимны, поэтому обычным средствам борьбы с DDoS-атаками очень сложно установить факт наличия такой атаки, а значит и противостоять ей [4].

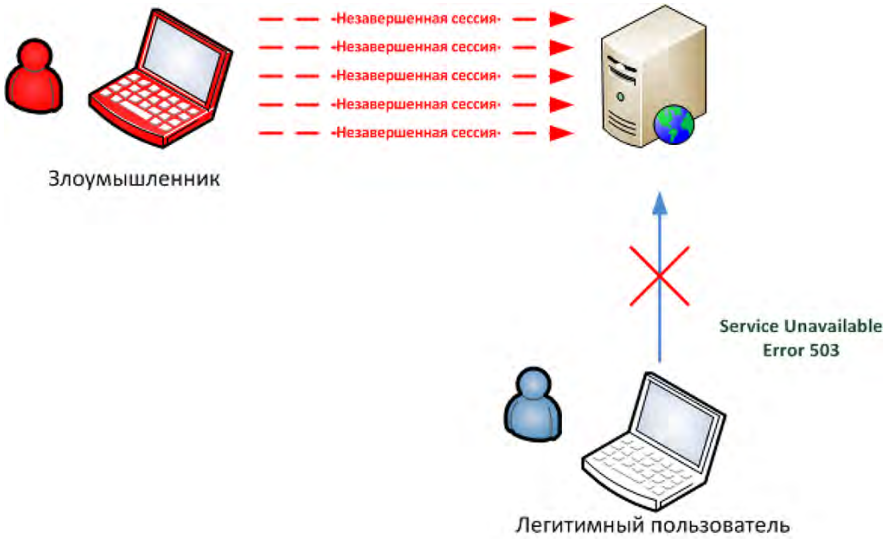


Рис. 3. Схема атаки типа SlowLoris

Есть два типа HTTP-flood – GET и POST. GETHTTP-flood состоит в отправке значительного числа GET-запросов, начинающих скачивание заметных объемов данных с атакуемого сервера (рис. 4), что приводит к ослаблению ресурсов сервера.

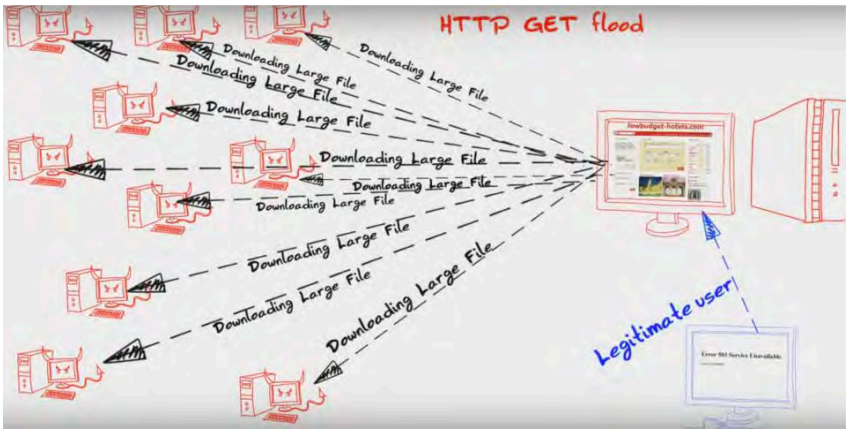


Рис. 4. Схема GETHTTP-floodатаки

При проведении POSTHTTP-flood атаки хакер отправляет значительное число данных в формах web-сайта, маскируясь при этом под легитимную отправку данных клиентов (рис. 5). Использование различных параметров запросов может позволить хакеру избежать обнаружения

и блокирования атаки при помощи средств защиты, основанных на статических сигнатурах трафика.

Рис. 5. Схема POSTHTTP-flood атаки

В результате рассмотрения представленных типов DDoS-атак, видно, что, во-первых, все они основаны на стандартных принципах работы сетевых протоколов прикладного уровня, а во-вторых, не требуют большого числа ресурсов от хакера, и инструменты для проведения таких атак широко доступны. Таким образом, осуществить подобные атаки очень просто даже при практически нулевых вложениях. Поэтому они так опасны и находят все большее распространение.

Список используемых источников

1. Kaspersky Lab. Denial of service: how businesses evaluate the threat of DDoS attacks it security risks special report series [Электронный ресурс]. URL: https://media.kaspersky-contenthub.com/wp-content/uploads/sites/45/2018/03/08234158/IT_Risks_Survey_Report_Threat_of_DDoS_Attacks.pdf (дата обращения: 15.03.2020).

2. Тарасов Я. В. Исследование применения нейронных сетей для обнаружения низкоинтенсивных DDoS-атак прикладного уровня // Вопросы кибербезопасности. 2017. № 5 (24). С. 23–28.

3. DoS-атака – Wikipedia [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/DoS-атака (дата обращения 17.03.2020).

4. Атаки DDoS. Часть 4 [Электронный ресурс] // Военные хитрости: БИТ 08.2015. URL: http://bit.samag.ru/archive/article/1559 (дата обращения: 18.03.2020).

УДК 004.654
ГРНТИ 20.53.17

ПОСТРОЕНИЕ ПЕРСПЕКТИВНОЙ СИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ

С. Н. Бушуев[1], В. И. Комашинский[2], О. И. Пантюхин[3], И. Б. Паращук[4], И. Б. Саенко[4]

[1]Акционерное общество «Научно-производственное предприятие ТЕЛДА»
[2]Институт проблем транспорта им. Н.С. Соломенко Российской академии наук
[3]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[4]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Представлена архитектура перспективной системы разграничения доступа к информации в облачных инфраструктурах критически важных информационных объектов, основанная на применении моделей разграничения доступа ABAC и RBAC. Приводится характеристика основных компонентов системы. Обсуждаются результаты ее реализации.

разграничение доступа, облачная инфраструктура, критически важный объект.

Облачные инфраструктуры представляют собой сравнительно новый вид компьютерных инфраструктур, которые притягивают к себе повышенное внимание в области информационных технологий и обладают повышенным интересом для потребителей информационных услуг и ресурсов. При этом отмечается значительное повышение роли и стремительное распространение облачных инфраструктур в критически важных информационных системах. Повышение совокупной стоимости активов устройств, программного обеспечения и критически важных данных таких систем, а также увеличение числа атак на них определяют актуальность задач разграничения доступа к информации в облачных инфраструктурах таких систем, а также обнаружения и разрешения конфликтов в используемых ими политиках разграничения доступа.

В то же время многие исследователи отмечают, что более широкому распространению облачных технологий препятствуют проблемы безопасности. Недостатком большинства существующих облачных инфраструктур является отсутствие возможности гибкого управления со стороны пользователей доступом к своим данным, что вызвано универсальностью решений по контролю доступа, принимаемых поставщиками облачных услуг [1]. Не-

однородность и большое разнообразие ресурсной среды облачного хранилища требуют всестороннего и детально проработанного механизма управления доступом, чтобы обеспечить динамические, постоянно расширяемые и хорошо настраиваемые требования по защите информации пользователей [2]. Однако существующие механизмы безопасности, обеспечиваемые поставщиками облачной инфраструктуры, не удовлетворяют этим требованиям [3]. Кроме того, проблемы безопасности информации в облачных инфраструктурах обостряются, если используются открытые веб-сервисы [4]. Все это требует проработки вопросов совершенствования политик разграничения доступа и моделей, лежащих в их основе.

В настоящей работе рассматриваются ключевые вопросы построения перспективной системы разграничения доступа к информации в облачных инфраструктурах критически важных информационных объектов. Эта система ориентирована на использование перспективной модели разграничения доступа, которой является модель разграничения доступа на основе атрибутов (*Attribute-Based Access Control,* ABAC) [5].

В отличие от других, традиционных моделей разграничения доступа, таких как, например, ролевая модель (*Role-Based Access Control,* RBAC), модель ABAC ориентирована на выполнение тех или иных действий над ресурсами (объектами), основываясь на проверку корректности выполнения множества логических условий (правил), которые определяют используемую политику контроля доступа. Правила формируются в виде логических выражений, в которых используются значения атрибутов. Множество атрибутов состоит из атрибутов пользователей (субъектов), атрибутов ресурсов (объектов) и атрибутов компьютерного окружения. К последней группе относится время. По этой причине модель ABAC является более гибкой, чем другие модели контроля доступа, и способной быстро реагировать на изменения.

Основными задачами, которые призвана решать перспективная система разграничения доступа к информации, являются:

– оценка качества политик разграничения доступа;

– структурная оптимизация политик разграничения доступа;

– верификация и обеспечение непротиворечивости политик разграничения доступа;

– структурная реконфигурация политик разграничения доступа.

Кроме того, должно обеспечиваться надежное распределенное хранение политик разграничения доступа.

Предлагаемая обобщенная архитектура перспективной системы разграничения доступа к информации отражает функциональные взаимосвязи и циркулирующие информационные потоки между отдельными компонентами, реализующими модели и методы анализа, структурной оптимизации и верификации систем разграничения доступа к информации (рис.).

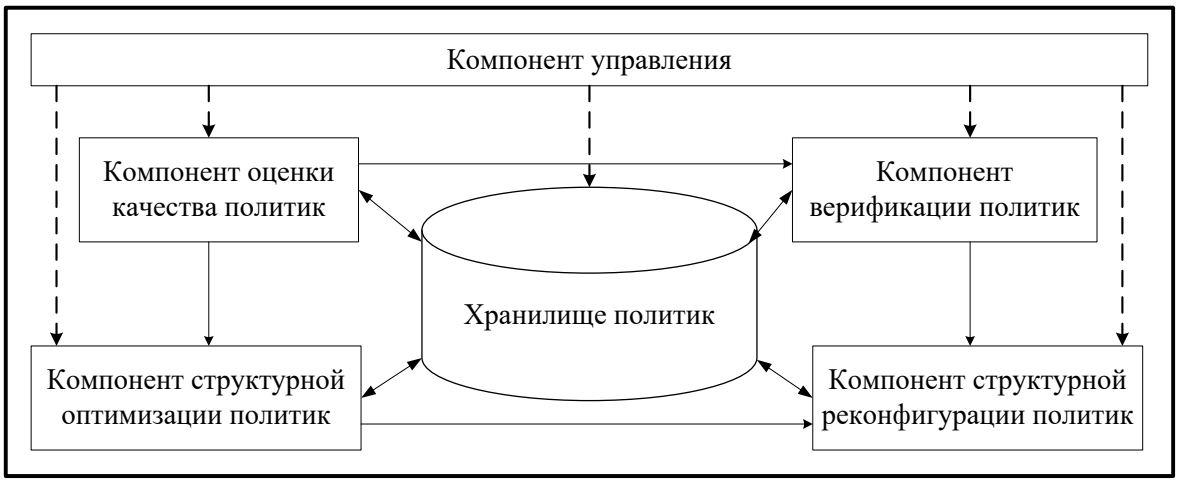


Рис. Обобщенная архитектура перспективной системы разграничения доступа к информации

Обязательными компонентами являются компонент управления и компонент хранения данных. Опциональными компонентами являются: компонент оценки качества политик разграничения доступа, компонент структурной оптимизации политик разграничения доступа, компонент верификации и обеспечения непротиворечивости политик разграничения доступа и компонент структурной реконфигурации политик разграничения доступа. Дадим краткую характеристику компонентов этой системы.

Компонент оценки качества политик разграничения доступа играет вспомогательную роль при решении проблемы нахождения качественной политики разграничения доступа. Результат решения этой проблемы во многом зависит от того, какие выбраны модели для оценки качества этой политики. Как правило, для оценки качества политик разграничения доступа учитываются следующие их основные свойства: точность, целостность и доступность. Так как доступность во многом определяется качеством хранилища данных, компонент ограничивается рассмотрением первых двух свойств. Для оценки точности используется универсальная матричную модель, основанную на учете атрибутов. Эта модель определяет матрицу доступа, в которой каждая строка представляется парой, состоящей из субъекта и множества его атрибутов $<S_i, ATTS(S_i)>$. Каждый столбец представляется парой, состоящей из объекта и множества его атрибутов $<O_j, ATTS(O_j)>$. Тогда каждая ячейка ($[S_i : O_j]$) соответствует множеству прав доступа, которые субъект S_i может выполнять над объектом O_j, полагая, что выполняются условия политики доступа. Для оценки целостности используется модель, в которой определяется взвешенная структурная сложность. В результате сложность правила $<e; o>$ вычисляется как $WSC(e) + WSC(o)$, где WSC – вес логического условия e или операции o, определяемый как количество содержащихся в них атомарных элементов.

Компонент структурной оптимизации политик разграничения доступа предназначен для решения проблемы оптимизации этих политик, которая обусловлена необходимостью создания в облачных инфраструктурах систем защиты информации, поддерживающих необходимый уровень информационной безопасности и требующих минимальных вычислительных и административных затрат на свое ведение. Этот компонент ориентирован на использование как модели ABAC, так и модели RBAC. При использовании модели ABAC задача оптимизации решается в тесной связи с задачей верификации политик. Для проведения процедуры верификации используется метод «проверки на моделях», основанный на математическом аппарате темпоральной логики. В постановке задачи оптимизации политик требуется: (1) определить степень расхождения результирующей политики разграничения доступа с требуемой; (2) выявить возможные противоречия и дублирования, присутствующие в этой политике. При использовании модели RBAC задача оптимизации сводится к формированию матриц «пользователи – роли» и «роли – полномочия», при которых выполняются два условия. Первое означает совпадение произведения этих матриц с заданной матрицей «пользователи – полномочия». Второе определяет необходимость достижения минимального количества ролей в результирующих матрицах. Данная задача относится к классу NP-полных оптимизационных задач. Для ее решения представляется целесообразным применение биоинспирированных методов оптимизации, в частности, генетических алгоритмов [6].

Компонент верификации и обеспечения непротиворечивости политик разграничения доступа, с одной стороны, позволяет провести верификацию политик разграничения доступа. При этом используется специальное программно-инструментальное средство. С другой стороны, этот компонент обеспечивает непротиворечивость политик разграничения доступа. В основе обеспечения непротиворечивости политик лежит модель, состоящая из множества состояний, множества переходов между состояниями и функции. Каждое состояние помечается набором свойств, истинных в этом состоянии. Модель строится на основании формул первого порядка с учетом следующих правил: (1) множество состояний есть множество всех оценок над множеством переменных; (2) для любой пары состояний отношение перехода соблюдается в том и только в том случае, когда соответствующая ему логическая формула становится истинной; (3) каждое атомарное высказывание представляет собой присваивание переменным значений из некоторого домена.

Компонент структурной реконфигурации политик разграничения доступа выявляет необходимость такой реконфигурации и обеспечивает ее проведение. Для выявления необходимости реконфигурации политик производится оценка, с одной стороны, уровня снижения качества этих политик, а с другой стороны – затраты администрирования, необходимые

для реализации этой реконфигурации. По этой причине в данном компоненте решается оптимизационная задача, аналогичная той, которая решается в компоненте оптимизации политик, но отличающаяся видом целевой функции. В целевую функцию добавляется слагаемое, которая определяет объем затрат на проведение реконфигурации.

Компонент хранения данных играет роль хранилища политик. Политик могут храниться в различных форматах: SQL, XML или RDF.

Компонент управления обеспечивает, с одной стороны, интерфейс с администратором системы разграничения доступа. С другой стороны, он играет системообразующую роль и обеспечивает взаимосвязь компонентов друг с другом.

Реализация и экспериментальная оценка системы разграничения доступа, имеющей предложенную архитектуру, была выполнена для предметной области, в которой пользователи увязаны в иерархическую структуру управления, а доступ к информационным ресурсам со стороны пользователей является разнородным и изменяемым во времени. Для этой цели для каждого компонента системы были разработаны программные прототипы. В качестве моделей разграничения доступа использовались модели RBAC и ABAC. В качестве инструмента верификации использовались SPIN и UPPAAL. Результаты оценки, полученной таким образом системы разграничения доступа продемонстрировали ее высокую эффективность и достаточную полноту возлагаемых на нее функциональных возможностей.

Работа выполнена при частичной финансовой поддержке проекта РФФИ № 18-07-01369 и бюджетной темы 0073-2019-0002.

Список используемых источников

1. Саенко И. Б., Бирюков М. А., Ясинский С. А., Грязев А. Н. Реализация критериев безопасности при построении единой системы разграничения доступа к информационным ресурсам в облачных инфраструктурах // Информация и космос. 2018. № 1. С. 81–85.

2. Komashinskiy D., Kotenko I. Malware Detection by Data Mining Techniques Based on Positionally Dependent Features // Proceedings of the 18th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2010). Pisa, Italy, 17–19 February, 2010. Los Alamitos, California. IEEE Computer Society. 2010. PP. 617–623.

3. Саенко И. Б., Бирюков М. А., Ефимов В. В., Ясинский С. А. Модель администрирования схем разграничения доступа в облачных инфраструктурах // Информация и космос. 2017. № 1. С. 121–126.

4. Patel S. Ch., Umrao L. S., Singh R. Sh. Policy-based Access Control in Cloud Computing // Proceedings of the International conference on Artificial Intelligent and Soft Computing, December 2012. 6 pages.

5. Karatas G., Akbulut A. Survey on Access Control Mechanisms in Cloud Computing // Journal of Cyber Security and Mobility. 2018. Vol. 7, № 3. PP. 1–36.

6. Kotenko Igor, Saenko Igor. Improved genetic algorithms for solving the optimization tasks in access scheme design for computer networks // Int. J. Bio-Inspired Computation. 2015. Vol. 7, No. 2. PP. 98–110.

УДК 004.891.2
ГРНТИ 20.23.17

ИНТЕЛЛЕКТУАЛИЗАЦИЯ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ РАБОТЕ С ОПЦИОННЫМИ СТРАТЕГИЯМИ НА ФИНАНСОВЫХ РЫНКАХ

И. В. Быстров, В. Л. Литвинов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном обществе торговля на финансовом рынке приобретает все большую популярность в связи с возможностью получения дополнительной прибыли, благодаря использованию множества инструментов, таких как акции, фьючерсы и производные от них опционы. Тем не менее, рынок опционов часто отпугивает новых и даже опытных инвесторов из-за его специфической терминологии и разнообразия стратегий. Это приводит к тому, что инвесторы теряют огромный набор возможностей, которые предоставляют опционы для управления капиталом. В этих условиях возникает необходимость в создании интеллектуальной системы поддержки принятия решений, которая анализирует выбранные инструменты в совокупности с их стандартными параметрами, что позволяет спрогнозировать и визуализировать поведение разработанной инвестором стратегии.

финансовый рынок, опцион, модель ценообразования, интеллектуальные системы поддержки принятия решений.

Инвестиционный портфель современного финансового аналитика или биржевого спекулянта состоит не только из акций различных компаний, как это было раньше. В него также входит множество других разнообразных финансовых инструментов и активов, которые сильно отличаются по своим показателям доходности и риска, но в совокупности, при правильном использовании могут принести максимальную прибыль при приемлемых рисках. Это именно то, к чему стремятся абсолютно все участники финансового рынка.

В работе рассмотрено общее описание опциона, как инструмента для формирования комбинированных стратегий. Рассмотрены принципы работы систем поддержки принятия решений для торговли на финансовом рынке, а также предложен вариант интеллектуализации подобных систем.

С развитием экономики и биржевой торговли на бирже стали появляться новые инструменты, способные удовлетворить различные финансовые потребности. Одним из таких инструментов является опцион [1].

Опцион – это гибкий производный инструмент, который дает дополнительные возможности для инвесторов, преследующих самые разные цели. Существует два вида опционов: опцион «колл», дающий право, но не обязательство произвести покупку определенного актива по фиксированной цене и опцион «пут», дающий право продажи определенного актива по фиксированной цене. Опцион является производным инструментом, то есть не может существовать без базового актива. Самым важным его отличием от остальных инструментов финансового рынка является то, что он имеет ограниченное время жизни, после окончания которого либо обесценивается, либо превращается в базовый актив, в зависимости от текущей цены базового актива.

Таким образом, все опционные стратегии основываются на комбинациях покупок и продаж опционов «колл» и «пут». Мелким спекулянтам опционы позволяют получить максимально возможный финансовый рычаг, в то время как крупные инвесторы могут осуществлять хеджирование своего портфеля и контролировать риск вложений. Тем не менее, лишь малая часть инвесторов используют эти преимущества, считая опционы в высшей мере сложным инструментом. Такое впечатление складывается по двум причинам. Во-первых, относительно недолгое существование не позволило этому инструменту стать предметом внимания широкой публики. Во-вторых, огромное разнообразие стратегий и связанная с опционами специфичная терминология.

Все осложняется тем, что современная рыночная среда характеризуется высокой скоростью процессов, происходящих в ней. Чтобы преуспеть в торговле на финансовом рынке современный инвестор должен действовать в соответствии с изменениями во внешней среде. В идеале спекулянт должен реагировать на эти изменения не только для того, чтобы показатели результативности не уменьшились, но и для того, чтобы извлечь прибыль из этих изменений. В отличии от консервативных стратегий покупки или продажи классических инструментов, с которыми знаком любой инвестор, опционы требуют аналитического анализа, на который без должного опыта может уйти достаточно большое количество времени, что не позволительно в данной ситуации.

Ситуация кардинально изменилась с развитием информационных технологий. До недавнего времени инвесторам приходилось вручную планировать и оценивать поведение разработанных ими стратегий по котировальным листам, что само по себе требует огромного внимания, не говоря уже об усложнении стратегий и добавления к ним опционов. С появлением специализированного программного обеспечения в значительной степени повысилась производительность труда финансовых аналитиков и инвесторов, а также стали проявляться преимущества использования опционов. Таким образом, этот инструмент начал завоевывать популярность не только среди профессионалов, но и среди начинающих инвесторов.

Программы для торговли, называемые терминалами, представляют из себя системы поддержки принятия решений и могут представлять собой набор специальных индикаторов, с помощью которых можно спрогнозировать будущее поведение инструментов. Кроме того, они содержат большое количество электронных котировок для наглядного представления информации и удобного заключения сделок. Для того, чтобы выстроить опционную стратегию и получить график её поведения в некоторых терминалах предусмотрена функция анализа. Входными данными являются несколько параметров, характерных для опциона – это дата истечения опциона, цена базового актива, цена исполнения опциона и волатильность доходности базового актива. Когда данные внесены, программа автоматически выстроит график на основе математической модели определения справедливой стоимости, показывающий, как меняется результат по опциону в зависимости от изменений цены актива и количества дней до истечения опциона. Основное удобство заключается в том, что панель анализа позволяет менять параметры выбранного инструмента, после чего мгновенно перестраивает график возможных результатов. В сложных стратегиях используется множество инструментов, работающих в связке, например, фьючерсы или акции и производные от них опционы. В этом случае, график визуализирует поведение всей стратегии в целом, на протяжении всего времени существования выбранных опционов. Таким образом, можно выстроить любую опционную комбинацию, их вариаций бесконечное количество.

Как было сказано выше, для построения стратегии программное обеспечение использует математическую модель расчета ценообразования опциона. Основной и классической является модель Блэка-Шоулза [2]. Данная модель определяет теоретическую цену на опционы, подразумевая, что базовый актив уже торгуется на финансовом рынке, и цена на опцион устанавливаться самим рынком. За счет своей простоты, модель содержит целый ряд допущений, некоторые из которых являются критическими. Например, если основным активом является акция, модель не учитывает дивиденды, которые выплачивает акционерная компания. Кроме того, в системе не учитывается уровень комиссионных и других платежей, которые осуществляет

трейдер в процессе открытия и закрытия сделок. Самым спорным допущением является определение эффективности целевого рынка и случайный характер динамики рыночных цен.

Существует также биноминальный метод расчета ценообразования, который известен как модель Кокса-Росса-Рубинштейна. Данная модель учитывает факторы, которые не рассматриваются в модели Блэка-Шоулза, тем не менее они дают очень близкие результаты. Биномиальная модель опционного ценообразования предполагает, что фактические события, связанные с изменением курсов базовых инструментов, происходят не случайном образом, а регулярно, с определенным шагом во времени. Большинство компьютерных программ, реализующих биномиальную модель опционного ценообразования, позволяют пользователю самостоятельно задавать число шагов, необходимых для оценивания опционов с требуемой точностью. Как правило, если срок «жизни» опциона невелик, ограничиваются не более чем 50 шагами. Так как при традиционном экономическом анализе обычно используется «дерево принятия решений», то биномиальная модель представляется нагляднее и проще для применения. Основной ее недостаток – громоздкость расчетов и вычислений, но вместе с тем она позволяет учесть все дополнительные факторы и сценарии развития рыночной ситуации.

Описанные модели используются системами поддержки принятия решений для оценки поведения стратегии на определенном временном промежутке, не беря в расчет исторические показатели. Как показывает практика, поведение рынка часто имеет тенденцию повторяться, то есть оно циклично. Благодаря этому появляется возможность использовать интеллектуальную систему поддержки принятия решений на основе методов машинного обучения. Использование исторических данных в совокупности с текущими показателями рынка в интеллектуальной системе поддержки принятия решений обеспечит возможность построения прогнозов и ассоциаций, которые в свою очередь позволят спрогнозировать поведение стратегии не только исходя из текущего состояния рынка, но и на основе исторического опыта. Прогнозы в данном случае возможны не просто как отражение основных тенденций, а как метод нахождения и создания шаблонов, реально отражающих динамику поведения стандартных параметров опционов по временным рядам баз данных. С помощью внедрения подобного механизма можно более точно предсказывать поведение опционных стратегий в будущем. Ассоциации же используются в том случае, когда несколько событий связанны между собой, что дает возможность выявления похожих паттернов в поведении рынка.

С учетом описанного преимущества, которое может обеспечить интеллектуализация системы поддержки принятия решений для работы с опционными стратегиями, можно сделать вывод о том, что дальнейшие исследования в этой области имеют определенный потенциал. В такой среде,

как финансовый рынок исторические данные играют большую роль, поэтому их использование даст большое преимущество и обязательно скажется на точности прогнозирования. Чем точнее система может предсказать результат, тем быстрее и качественнее инвестор сможет принимать решения.

Список используемых источников

1. Томсетт Майкл С. Торговля опционами: спекулятивные стратегии, хеджирование, управление рисками; пер. с англ. М. : Издательский дом «АЛЬПИНА», 2001. 360 с.

2. Как сделать приблизительный расчет стоимости опциона [Электронный ресурс]. URL: https://smart-lab.ru/blog/574961.php (дата обращения: 30.01.2020).

УДК 535.32
ГРНТИ 29.31.29

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МЕТОДОВ КОНТРОЛЯ КОНЦЕНТРАЦИИ ПРИМЕСЕЙ В ЖИДКИХ ДИСПЕРСНЫХ СРЕДАХ

А. В. Ваганов, В. А. Вачугова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются вопросы, связанные с разработкой метода и системы, предназначенных для непрерывного контроля концентрации примесей в жидких средах, перемещаемых по трубопроводу. Поясняется актуальность данного контроля и производится обзор существующих аналогичных методов. Предоставляется модель бесконтактного оптического турбидиметрического измерительного преобразователя, на основе которой разработана структурная схема и обоснован выбор современной элементной базы для разработки измерительной системы в целом.

Приводятся рекомендации по применению математического аппарата и исследованию моделей датчика и системы, а также формулируются рекомендации практического характера для разработки устройств подобного класса.

дисперсность, бесконтактный преобразователь, турбидиметрия, датчик.

Актуальность данной темы связана с распространённой проблемой проведения точного дисперсного анализа и необходимости использования современных технологий для контроля концентрации примесей в дисперсных средах. Для этого в первую очередь необходимо рассмотреть существующие способы оценки дисперсности, а затем рассмотреть элементную базу, на основе которой будет разработан датчик.

Дисперсный анализ или контроль дисперсности жидких сред широко используется в промышленном производстве и в различных областях науки и представляет собой совокупность методов для определения характеристик свободных частиц в жидких и газовых средах.

Существующие способы оценки дисперсности жидких сред можно условно разделить на две группы: контактные и бесконтактные. К первой группе будут относится методы, позволяющие определить размеры отдельных частиц через непосредственные измерения: оптическая и электронная микроскопия, а также через косвенные данные, такие как: скорость оседания частиц в вязкой среде или величина импульсов электрического поля – кондуктометрический метод.

Принцип действия кондуктометрического способа (счётчик Коултера) заключается в том, что измеряют электропроводность путем пропуска дисперсии через небольшое отверстие. Каждая частица, проходящая сквозь данное отверстие, даёт электрический импульс, величина которого пропорциональная объёму частицы (рис. 1).

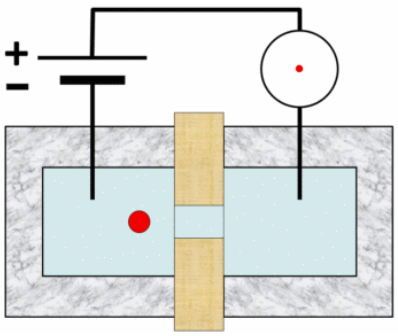


Рис. 1. Счётчик Коултера

Ко второй группе относятся методы, позволяющие оценить свободные частицы средних размеров: оптические и дифракционные методы. Данные методы основаны на изучении характеристик провзаимодействовавших с объектом излучений. Излучения, используемые в анализе, могут быть представлены в виде электромагнитных волн различных частот (оптические методы) или же как пучки заряженных частиц – электронов (дифракционные методы).

К оптическим методам относится нефелометрия и турбидиметрия [1]. Нефелометрия позволяет определить размер частиц по интенсивности света, рассеянного под углом 90°, в то время как турбидиметрия позволяет оценить количество и размер частиц с помощью измерения количества света, поглощаемого средой (рис. 2).

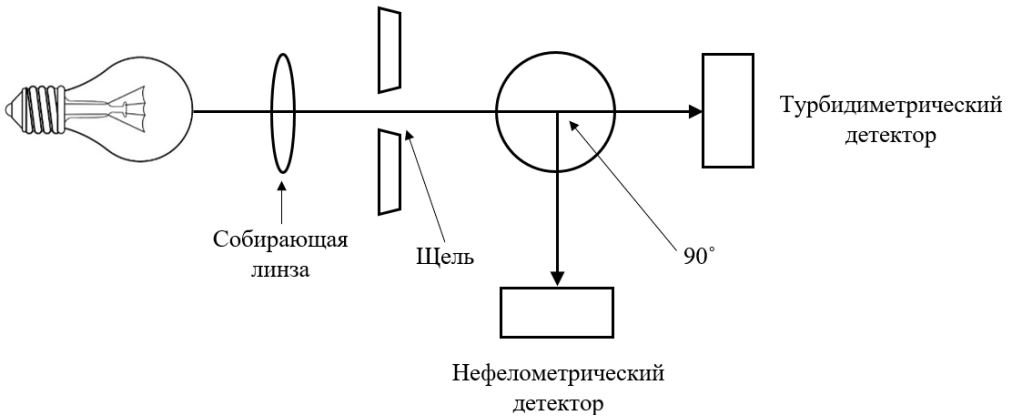


Рис. 2. Нефелометрия и турбидиметрия

Для решения проблемы проведения точного дисперсного анализа с использованием современных технологий необходимо иметь возможность определять количество примесей в широком диапазоне размера и состава частиц. Собственно, данная возможность зависит прежде всего от конструкции прибора.

В ходе литературного анализа способов контроля содержания различных примесей в жидких средах сделан вывод о необходимости построения метода и средства контроля концентрации примесей в жидкой дисперсной среде на основе оптической турбидиметрии.

Преимуществами данного способа является: создание бесконтактного автоматизированного метода; минимизация затрат на покупку комплектующих из-за отсутствия необходимости в высокочувствительных фотодиодах, небольшие габариты устройства.

Реализация средства контроля предполагает наличие первичной и вторичной обработки сигнала. Структурная схема блока первичной обработки системы контроля дисперсности представлена на рис. 3, где: *1* – источник оптического излучения (ИОИ), *2* – оптически прозрачный участок трубопровода (ОпТ), *3* – фотоприемное устройство (ФУ), *4* – формирователь (Ф), *5* – фильтр нижних частот (ФНЧ); *6* – фильтр верхних частот (ФВЧ); *7* – выпрямитель (В); *8* – выделитель информативной составляющей сигнала (ВИС); *9* – интегратор (И); *10* – аналого-цифровой преобразователь; *11* – стабилизатор мощности светового потока (Ст), *12* –микроконтроллер.

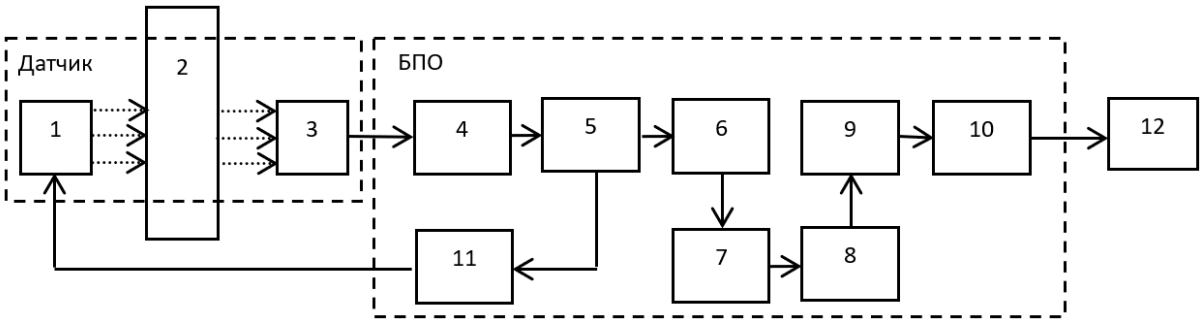


Рис. 3. Структурная схема системы контроля дисперсности

Датчик содержит в себе ИОИ, просвечивающий прозрачный участок трубопровода с контролируемой жидкостью, которая течет с постоянной скоростью. При этом режим излучения может быть, как непрерывный, так и импульсный. Стабилизация светового потока от ИОИ осуществляется стабилизатором Ст. Прямое и рассеянное оптическое излучение попадает в ФУ. Электрический сигнал от ФУ сначала поступает на Ф, где происходит выделение его огибающей, а затем на полосовой фильтр (ФНЧ и ФВЧ) для формирования рабочей полосы [2].

С выхода ФВЧ сигнал после получения его абсолютного значения с помощью В поступает на ВИС, который можно реализован на основе чересперiодного вычитателя (рис. 4), широко применяемого в радиолокации для исключения неподвижных целей.

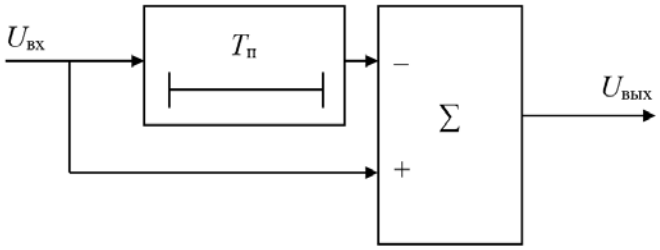


Рис. 4. Структурная схема чересперiодного вычитателя

При этом операция чересперiодного вычитания реализуется в соответствии с выражением:

$$U\text{вых}(t) = U\text{вх}(t) - U\text{вх}(t - T\text{п}),$$

где Tп – период следования импульсов от частиц при пересечении ими оптического потока датчика.

Для повышения чувствительности метода обнаружения частиц в целом может быть применено накопление информативной составляющей сигнала, поступающего с выхода ВИС устройством И [3].

Итоговое выражение, описывающее преобразование сигнала от датчика с целью выделения его информативной составляющей, может быть записано в виде:

$$U\text{сиг} = (Cv\text{ч} \cdot K(l\text{ч}) \cdot U\text{ч} + U\text{п}) \cdot K\text{ф} \cdot K\text{фнч} \cdot K\text{фвч} \cdot K\text{в} \cdot K\text{вис} \cdot K\text{и},$$

где $Cv_ч$ – объемная концентрация частиц в контролируемом датчиком объеме жидкой среды; $K(l_ч)$ – коэффициент преобразования датчика, учитывающий перемещение частицы в указанном объеме; $U_ч$ – амплитуда сигнала на выходе ИП от пересечения контролируемого объема одной частицей; U_n – амплитуда сигнала помехи; K_i – соответствующий коэффициент передачи i-го элемента БПО.

Математическая модель БПО на функционально-логическом уровне может быть описана в виде передаточной функции:

$$G\text{бпо}(s) = \frac{G\text{датчик} \cdot G\text{ф}(s) \cdot G\text{фнч}(s)}{1 + G\text{датчик} \cdot G\text{ф}(s) \cdot G\text{фнч}(s) \cdot G\text{ст}} \cdot G\text{фвч}(s) \cdot G\text{в} \cdot G\text{вис}(s) \cdot G\text{и}(s),$$

где G_i – передаточные функции i-го элемента БПО.

Проверку устойчивости контура Ст для светового потока ИОИ удобно проводить с помощью годографа Найквиста. На рис. 5 представлен результат моделирования данного контура при следующих параметрах: частота

среза ФНЧ – 10 Гц, порядок ФНЧ – 2, частота среза интегрирующего фильтра Ст – 0,1 Гц (n = 2), общее усиление в петле обратной связи – 100.

Как следует из рис. 5, годограф, обходя против часовой стрелки начало координат, не охватывает точку со значением (–1;0), что подтверждает устойчивость контура Ст и БПО в целом.

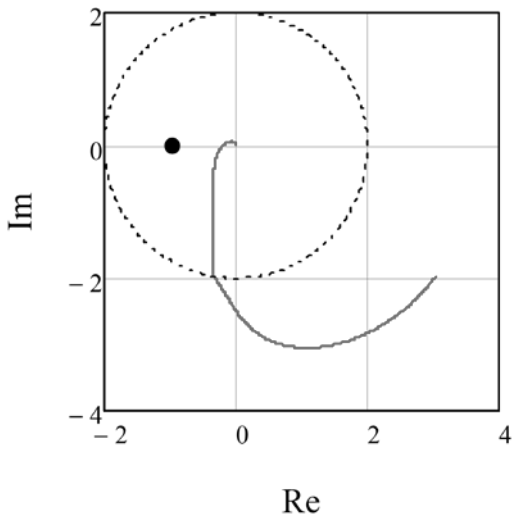


Рис. 5. Результат моделирования контура Ст

Таким образом был проведен анализ существующих способов, предназначенных для контроля концентрации примесей в жидких дисперсных средах, разработана модель бесконтактного оптического турбидиметрического измерительного преобразователя, на основе которой разработана структурная схема и обоснован выбор элементной базы. Кроме того, были приведены рекомендации по применению математического аппарата, исследованию и разработке устройств подобного класса.

Список используемых источников

1. Шишловский А. А. Прикладная физическая оптика. М. : Физматгиз, 1961. 822 с.

2. Титце У., Шенк К. Полупроводниковая схемотехника. 12-е изд. Том II: пер. с нем. М. : ДМК Пресс, 2008. 942 с.

3. Ваганов А. В., Захаров И. С. Математическая модель взаимодействия оптического излучения с инфузориями в жидких дисперсных биологических средах // Известия СПбГЭТУ «ЛЭТИ» № 10, 2009. С. 60–66.

Статья представлена заведующей кафедрой АПС СПбГУТ, доктором технических наук, доцентом Г. В. Верховой.

УДК 621.317
ГРНТИ 45.01.85

ТРАКТ ПЕРВИЧНОЙ ОБРАБОТКИ СИГНАЛА, КАК ЭЛЕМЕНТ СИСТЕМЫ СБОРА ДАННЫХ В АСУ

А. В. Ваганов, А.С. Иванов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются вопросы, связанные с разработкой блока предварительной обработки информативной составляющей сигнала от датчиков в различных системах автоматизированного управления. Поясняется необходимость предварительной нормализации сигнала для последующей его вторичной обработки. Обоснован выбор современной элементной базы для разработки тракта в виде дискретно-аналоговых динамически программируемых электронных схем. Сформированы рекомендации по применению математического аппарата и исследованию моделей. Приведен пример реализации фрагмента тракта первичной обработки сигнала в специализированной среде графического программирования с последующим его моделированием. Сформулированы рекомендации практического характера для разработки устройств подобного класса. При разработке используется традиционный математический аппарат.

АСУ, дискретно-аналоговые схемы, сигналы, тракт обработки.

Современные производства, как правило, базируются на основе различных автоматизированных системы управления (АСУ). Главное назначение АСУ заключается в проведении эффективного анализа производительности каждого из объектов подобных систем, благодаря которому специалист принимает решения по улучшению всего рабочего процесса. Активное участие специалистов в процессе управления указывает на то, что сама АСУ не является полностью автоматической, а основывается на совокупности человеко-компьютерных комплексах. Хотя само появление такого класса систем относится ко второй половине прошлого века, тем не менее, массовое использование их в современном производстве началось относительно недавно.

С точки зрения классификации АСУ включает в себя несколько подсистем, в том числе для формирования определенных воздействий на объект управления – технологический объект (конвейер, станок с ЧПУ, робот-манипулятор и т. п.) в соответствии с определенным критерием. Рассматриваемый подкласс относится к АСУ технологическими процессами на предприятии (АСУТПП). АСУ для управления техпроцессами обладает определенной автономностью с точки зрения принятия решения и алгоритмов функционирования внутри контролируемого ею производственного процесса. Так же в ее состав входит уникальное оборудование, состоящее

из различных электронных систем, которые в свою очередь, могут содержать тракт первичной (предварительной обработки) сигнала от аналоговых датчиков (рис 1).

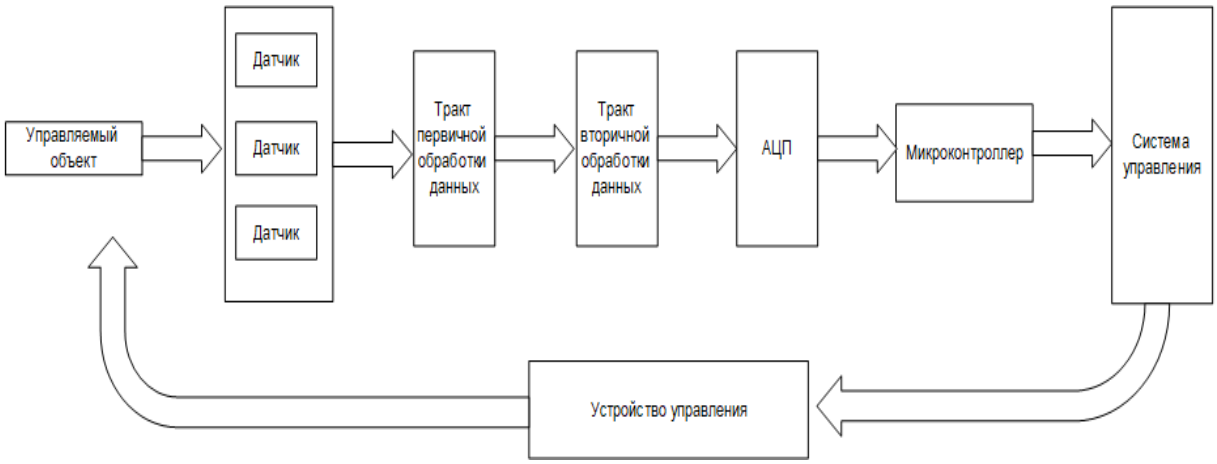


Рис. 1. Структурная схема АСУ

Несмотря на преимущества цифровых датчиков (возможность исключить искажения сигнала при его передаче), при создании АСУТП не всегда имеется возможность полностью отказаться от аналоговых первичных измерительных преобразователей. Отличительная особенность аналогового датчика – наличие статической помехи в виде постоянной составляющей сигнала, различных помех от внешних источников (электросеть, мобильный телефон, а также малая величина амплитуды полезного сигнала). Поэтому возникает необходимость предварительной нормализации выходного сигнала от такого датчика для подготовки к последующей вторичной обработки. Для этого между датчиком и цифровой системой обработки АСУТП устанавливается аналоговый тракт предварительной обработки сигнала для приведения его к оптимальному виду для максимизации эффективности его обработки цифровым трактом. Самая главная задача предварительной обработки – это повышение соотношения сигнал-шум, а значит максимизация энергии полезного сигнала. Данная задача решается комплексно с использованием, в том числе, полосовой фильтрации сигнала [1].

Классическая реализация тракта предварительной обработки сигнала обычно базируется на дискретных элементах. Из-за того, что при создании первичного тракта используются аналоговые элементы, (операционные усилители, транзисторы, резисторы, конденсаторы, компараторы, и многое другое) аналоговая часть занимает большую часть платы и имеет следующие недостатки: большие массогабаритные показатели, отсутствие возможности динамического изменения конфигурации схемы, высокая погрешность и низкая температурно-временная стабильность. Устранением указанных недостатков занимаются многие компании в разных странах мира, проекти-

руя системы с высокой точностью обработки сигнала. Одной из них является фирма «Anadigm», занимающаяся разработкой специализированных дискретно-аналоговых систем на кристалле – ПАИС. В состав данных микросхем входит множество основных и вспомогательных элементов, которые в совокупности обеспечивают гибкость проектирования, легкость настройки и отладки, реализуемых на них основе систем обработки сигналов от аналоговых датчиков.

«Сердцем» ПАИС являются специализированные блоки (КАБы) в количестве четырех штук на каждом кристалле (рис. 2). При создании схемы дискретные элементы (конденсаторы, операционные усилители и др.) программно коммутируются между собой в нужной комбинации. Такое решение позволило перенести процесс разработки систем обработки сигналов на новый уровень, аналогичный архитектурам ПАИС.

Дискретно-аналоговые (импульсные) системы занимают промежуточное положение между аналоговыми и цифровыми. Для качественного сравнения основных характеристик (табл.) дискретно-аналоговых систем с обычными аналоговыми и цифровыми был взят динамически программируемый дискретно-аналоговый сигнальный процессор от фирмы «Anadigm» с индексом AN2031E04.

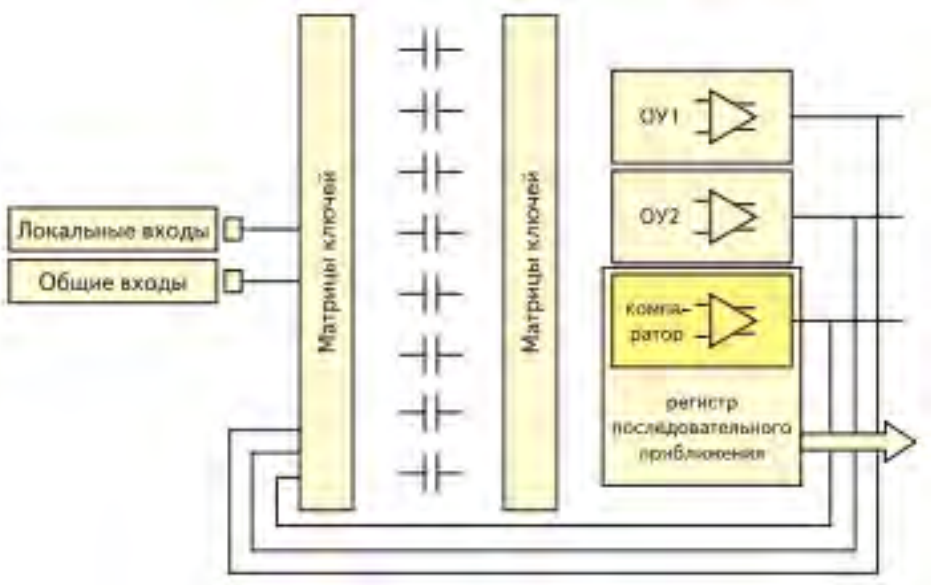


Рис. 2. Структура КАБ

ТАБЛИЦА. Сравнения основных характеристик дискретно-аналоговых систем с обычными аналоговыми и цифровыми

Параметр / Тип	Аналоговые	Цифровые	Дискретно-аналоговые
Соотношение сигнал-шум, дБ	< 60	> 100	90
Точность преобразования сигнала, %	1	0,01	0,1

Параметр / Тип	Аналоговые	Цифровые	Дискретно-аналоговые
Возможность динамического перепрограммирования	нет	нет	да
Максимальная частота обрабатываемого сигнала, МГц	15	5	2
Энергопотребление, мВт	1–100	10–500	< 125

Важно помнить, что тракт первичной обработки сигналов с аналоговым датчиком наиболее уязвим к помехам. Для предотвращения появления помех в электронных блоках обработки проектируемых АСУ необходимо правильно размещать соответствующее оборудование внутри системы. Чаще всего, для уменьшения воздействия внешних помех во всех каскадах обработки сигнала целесообразно применять межблочное экранирование, фильтрацию сигналов, проводить тщательные расчеты при конфигурировании и размещении блоков внутри стоек приборов [2].

Главное отличие схем дискретно-аналоговой обработки сигналов от цифровых систем заключается в том, что в последних сигнал может иметь только конкретные значения как по времени, так и по амплитуде. В импульсных же системах дискретизация сигнала происходит только по временной шкале (рис. 2). Такая особенность позволяет получать выходной сигнал на выходе дискретно-аналоговых систем с исключительно малыми искажениями.

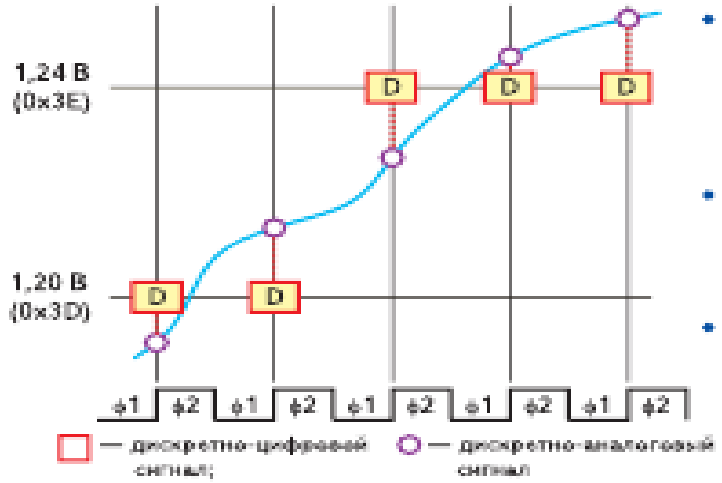


Рис. 2. Представление процесса аналоговой и цифровой дискретизации

Для описания процедуры обработки сигнала в импульсных системах как нельзя лучше подходит математический аппарат, применяемый для аналогичных задач в цифровых системах – *z*-преобразование. Ключевой особенностью применения данного аппарата является наличие неких выборок непрерывного сигнала с периодом, равным частоте дискретизации. Если

на вход цифровой системы поступает некое воздействие вида $x(nT)$, то выходной сигнал $y(nT)$ может быть описан с помощью следующей зависимости [3]:

$$H(z) = \frac{Y(z)}{X(z)} = K \frac{\prod_{k=1}^{m}(z - z_{zk})}{\prod_{k=1}^{n}(z - z_{pk})}, \quad (1)$$

где K – вещ. коэффициент; z_{zk} и z_{pk} – нуль и полюс (1).

Известно, что для расчетов аналоговых схем широко применяется преобразования Лапласа. Для возможности определения свойств аналоговых цепей, например, для определения устойчивости подходит передаточная функция системы, на вход которой подается сигнал, вызывающий реакцию на выходе. Реакция описывается выражением [3]:

$$H(s) = \frac{Y(s)}{X(s)} = K \frac{\prod_{k=1}^{m}(s - s_{zk})}{\prod_{k=1}^{n}(s - s_{pk})}, \quad (2)$$

где s_{zk} и s_{pk} – нуль и полюс системы; K – вещественный множитель (2).

В настоящее время аналоговые системы на кристалле, предназначенные для обработки сигнала функционируют на основе внутренних программ для создания которых предназначен специализированный пакет – «Anadigm Designer 2».

В качестве примера показана реализация в данной среде фрагмента тракта первичной обработки сигнала порогового обнаружителя (рис. 3, см. ниже). Для формирования полезного сигнала и помехи используются соответствующие генераторы-имитаторы.

FPAA1 – блок фильтрации (полосовая и режекторная фильтрация) и суммирования сигналов от двух независимых источников и FPAA2 – блок автоматического регулирования усиления (АРУ).

В заключении можно сделать следующий вывод о том, что применение аппаратно-программных систем на кристалле, предназначенных для построения схем предварительной обработки сигналов от датчиков является востребованным при проектировании электронных систем АСУ. В качестве математического аппарата при анализе моделей дискретно-аналоговых систем можно рассматривать аппарат передаточных функций в z-области.

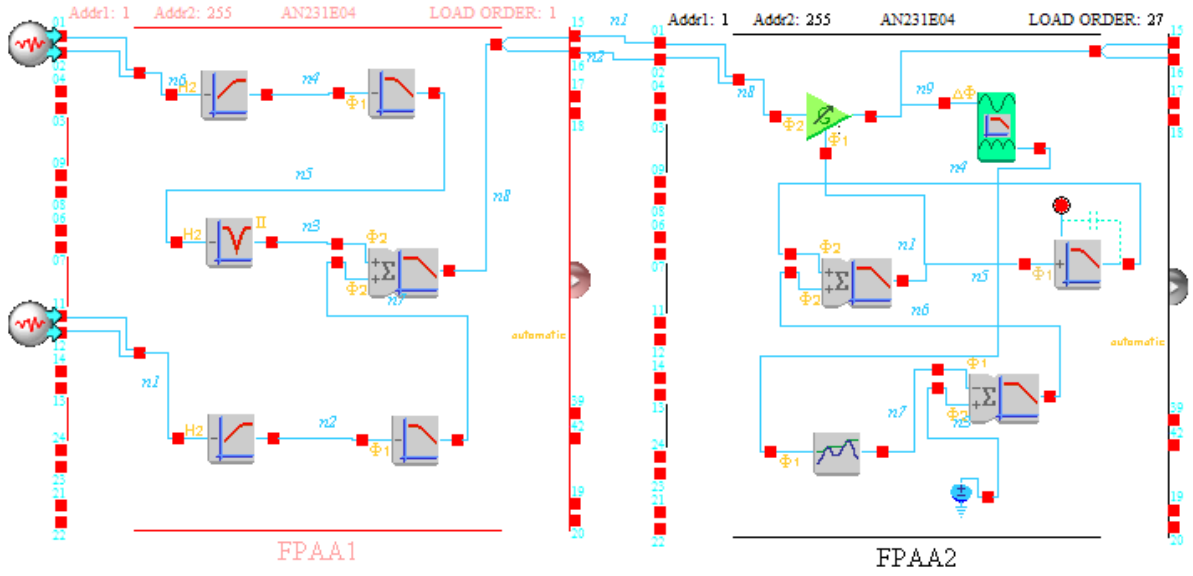


Рис. 3. Фрагмент тракта первичной обработки сигнала

Также следует отметить, что специально разработанный пакет для данного типа микросхем, обладающий интуитивно понятным разработчику интерфейсом, ускоряет процесс его обучения, а также ускоряет и оптимизирует саму процедуру проектирования в целом.

Список используемых источников

1. Полищук А. Программируемые аналоговые ИС Anadigm структура и принцип построения // Современная электроника. 2005. № 1. С. 24–26.

2. Щерба А. Компоненты и технологии № 12. М.: Современная электроника, 2007.

3. Волович Г. И. Схемотехника аналоговых и аналогово-цифровых электронных устройств. М. : Додэка XXI, 2011. 528 с. ISBN: 978-5-94120-254-6.

Статья представлена заведующей кафедрой АПС СПбГУТ, доктором технических наук, доцентом Г. В. Верховой.

УДК 681.17
ГРНТИ 50.09

ОЦЕНКА ЭФФЕКТИВНОСТИ КОМПОНОВКИ ЭЛЕКТРОННЫХ БЛОКОВ В АСУ

А. В. Ваганов, А. А. Ишкова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются вопросы, связанные с разработкой метода, предназначенного для оценки эффективности размещения электронных блоков в приборах системы управления предприятием с учетом таких важных критериев как: электромагнитная совместимость, распределение тепловых полей, прочностные характеристики, пыле- и влагозащищённость и др. Поясняется актуальность разработки данного метода на основе литературного обзора и анализа существующих способов оценки. Предложена идея построения алгоритма, позволяющего оценить общую эффективность размещения отдельных составляющих системы на основе анализа отдельных критериев.

Приведены рекомендации по применению математического аппарата и исследованию полученных моделей. Сформулированы рекомендации практического характера для разработки методов подобного класса.

компоновка, автоматизированные системы управления, электромагнитная совместимость, тепловой расчет, тракт предварительной обработки сигнала, оценка эффективности.

В настоящее время происходит интенсивное усложнение и увеличение масштабов промышленного производства, развитие экономико-математических методов управления, внедрение ЭВМ во все сферы производственной деятельности человека. Всё это служит толчком для создания и внедрения автоматизированных систем управления (АСУ), которые позволяют ускорить и упростить решение постоянно изменяющихся производственных задач, а также обеспечить рост производительности труда и качества выпускаемой продукции.

Разновидностью такой системы является АСУ управления технологическим процессом (АСУТП), обобщенный алгоритм функционирования которой представлен на рис. 1 (см. ниже).

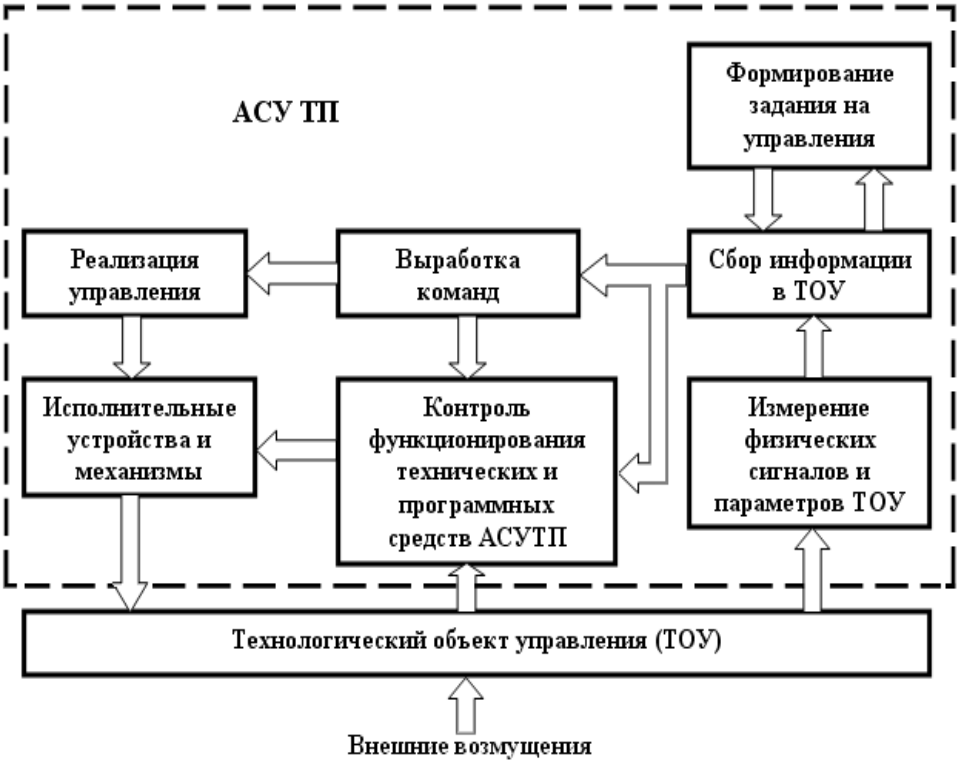


Рис. 1. Обобщенный алгоритм функционирования АСУ ТП

АСУ ТП представляет собой систему «человек-машина», призванную обеспечивать автоматизированный сбор и обработку информации, необходимый для оптимизации процесса управления [1].

АСУ ТП в зависимости от её назначения выполняет множество различных информационно вычислительных и управляющих задач, для реализации которых необходим определенный комплекс технических средств. Он представляет собой совокупность управляющих устройств, устройств передачи сигналов и данных, датчиков сигналов и исполнительных устройств. Обобщенная структура АСУ ТП представлена на рис. 2 (см. ниже), где: УО – управляемый объект, ИУ – измерительные устройства, ТПО – тракт предварительной обработки сигнала, Мц – цифровой мультиплексор, АЦП – аналого-цифровой преобразователь, МК – микроконтроллер, СУ – систему реагирования и управления, УУ – устройство управления.

В АСУ ТП входят множество всевозможных приборов, которые содержат модули различной степени сложности и назначения: усилители, фильтры, аналого-цифровые преобразователи, модули управления, контроля, передачи информации, питания и т. д. Таким образом, в связи со стремлением повысить надежность и корректность работы системы в целом возникает задача правильной компоновки блоков электронных устройств в приборах подобных систем. В процессе такой компоновки блоков внутри приборов очень важно учитывать такие аспекты, как электромагнитная и тепловая

совместимость, пыле- и влагозащищенность, а также устойчивость к внешнему механическому воздействию на модули и конструкцию прибора в целом.

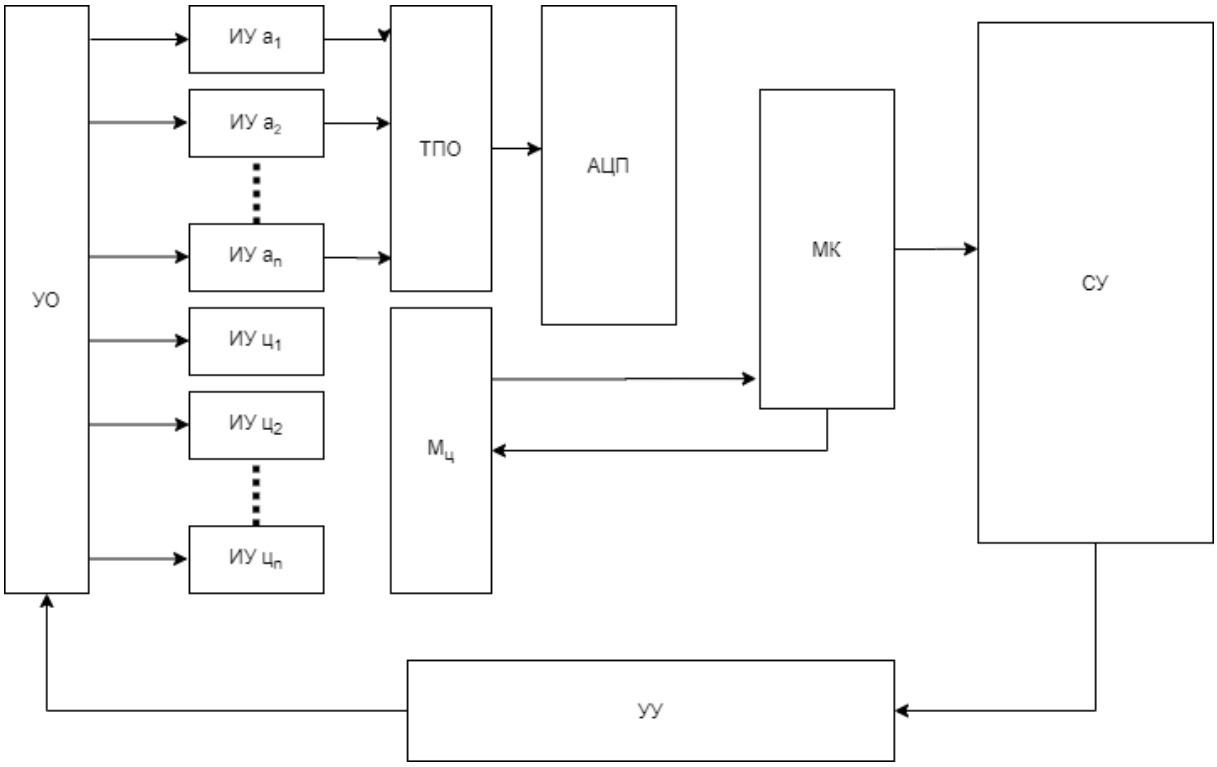


Рис. 2. Обобщенная структура АСУ ТП

На данный момент существуют формализованные математические методы, позволяющие оценить влияние взаимного расположения модулей в приборе на общее качество и надежность работы АСУ ТП.

Среди существующих стандартов, регламентирующих порядок оценки электромагнитной совместимости в электронных устройствах, можно выделить ГОСТ 29280-92 (МЭК 1000-4-92) [2], ГОСТ Р 51317.2.5-2000 (МЭК 61000-2-5-95) [3]. В части тепловой совместимости элементов в составе приборов АСУ могут быть применены следующие стандарты: ГОСТ 28236-89 (МЭК 68-3-1-74) [4], ГОСТ 16019-2001 [5].

Изучив данные стандарты более подробно, можно сделать вывод о том, что существующие методы чаще всего узконаправлены по сфере применения, учитывают лишь некоторые аспекты проектирования и размещения блоков электронных устройств в приборах или же сложны для применения и расчетов. Предлагаемый метод оценки эффективности компоновки электронных блоков в приборах АСУ позволяет учесть и оценить влияние различных мероприятий, направленных на улучшение перечисленные выше аспектов, и базируется на простом для понимания математическом аппарате.

Для упрощения понимания в настоящей статье принцип формирования метода будет рассмотрен на примере одного из аспектов - электромагнитной

совместимости для тракта предварительной обработки сигнала системы сбора данных от датчиков АСУ ТП (рис. 3), где ДУ – дифференциальный усилитель, ФНЧ – фильтр низких частот, ФВЧ – фильтр высоких частот, У – усилитель, РФ – режекторный фильтр, СУ – согласующий усилитель.

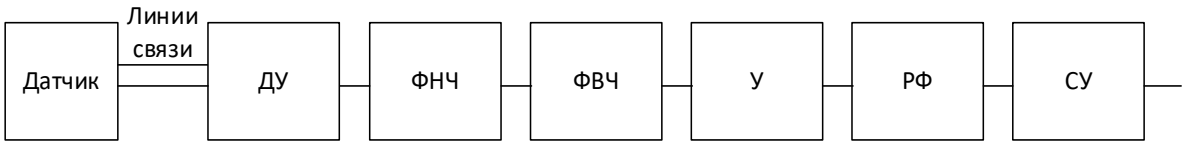


Рис. 3. Тракт предварительной обработки сигнала

Построение метода будет основываться на мероприятиях, позволяющих обеспечить максимизацию соотношение сигнал-помеха на выходе тракта с учетом его передаточной функции, которая в общем виде может быть записана следующим выражением:

$$G_{\text{тракта}}(S) = G_{\text{лс}}(S) * G_{\text{ду}} * G_{\text{у}} * G_{\text{фнч}}(S) * G_{\text{фвч}}(S) * G_{\text{рф}}(S) * G_{\text{су}},$$

где $G_{\text{лс}}(S), G_{\text{ду}}, G_{\text{у}}, G_{\text{фнч}}(S), G_{\text{фвч}}(S), G_{\text{рф}}(S), G_{\text{су}}$ – передаточные функции элементов тракта предварительной обработки сигнала.

При этом передаточные функции отдельных элементов тракта могут представлены в комплексном виде. Так для линии связи датчика и тракта передаточная функция имеет следующий вид:

$$G_{\text{лс}}(s) = \sqrt{(R_0 + sL_0) * (G_0 + sC_0)},$$

где R_0 – продольное активное сопротивление, L_0 – индуктивность петли, G_0 – поперечная активная проводимость утечки изоляции, C_0 – поперечная емкость между прямыми и обратными проводами.

Для расчета передаточной функции фильтра высоких частот используется зависимость вида:

$$G_{\text{фвч}}(s) = \frac{-G_s^2}{s^2 + \frac{2\pi f_0}{Q} s + 4\pi^2 f_0^2},$$

где G_s – передаточная функция по полосе пропускания, f_0 – частота среза, Q – добротность фильтра.

Среди помех, возникающих в тракте предварительной обработки сигнала, можно выделить пульсацию питающего напряжения с выхода блока питания, воздействие внешних помех на сам датчик, а также канал передачи данных.

Как правило, для минимизации помех в трактах как первичной, так и вторичной обработки сигнала эффективны следующие мероприятия: использование экранирования сигнального кабеля (витая пара, каоксиал), межблочное экранирование, организация соединений между каскадами в виде токовой петли или дифференциального входа-выхода, применение различных фильтров (полосовые, режекторные), правильное размещение самих блоков друг относительно друга внутри корпуса прибора.

В основу методики для оценки эффективности компоновки электронных блоков в АСУ в части электромагнитной совместимости в тракте предварительной обработки сигнала положена сравнение соотношений сигнал-шум до и после мероприятий, позволяющих минимизировать воздействие помех на конкретный участок тракта. Данный параметр можно рассчитать по формуле:

$$SN = \frac{P_{\text{С}}}{P_{\text{П}}} = \frac{U_{\text{С}}^2}{U_{\text{П}}^2},$$

где $P_{\text{с}}$, $P_{\text{п}}$ – мощность сигнала и помехи на выходе тракта, $U^2_{\text{с}}$, $U^2_{\text{п}}$ – действующее значение напряжение сигнала и помехи на выходе тракта.

Сравнение проводиться по формуле для каждого отдельного i-го мероприятия:

$$\delta SN_i = \frac{(SN_{i\ \text{до}} - SN_{i\ \text{после}})^2}{(SN_{i\ \text{до}} + SN_{i\ \text{после}})} * 100\%$$

где $SN_{\text{до}\ i}$ и $SN_{\text{после}\ i}$ – соотношения сигнал-помеха на выходе ТПОС до и после использования i-го способа минимизации влияния помех.

Общий алгоритм получения данной оценки показан на рис. 4 (см. ниже). Остальные аспекты оцениваются по аналогии, с учетом их специфики и существующего математического аппарата.

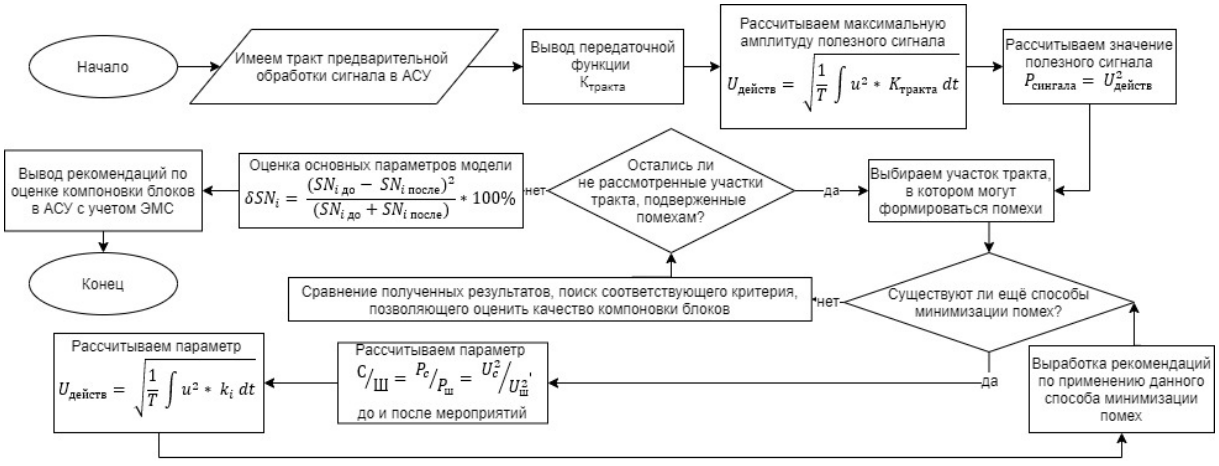


Рис. 4. Алгоритм оценки компоновки блоков по их электромагнитной совместимости

Результаты оценки удобнее представлять в виде нормированной диаграммы откликов модели, представленной на рис. 5.

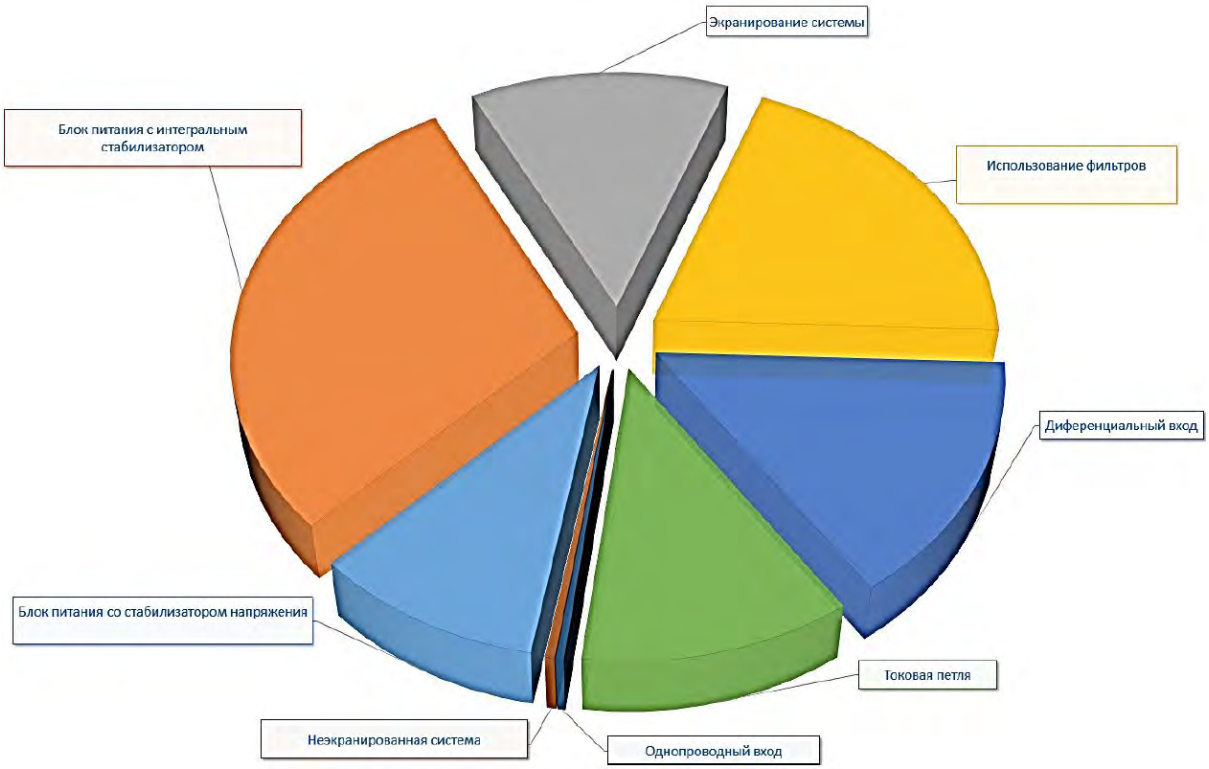


Рис. 5. Диаграмма откликов модели

Таким образом, предложенный в настоящей статье алгоритм оценки эффективности компоновки электронных блоков в АСУ позволяет в дальнейшем разработать комплексный метод, учитывающий все аспекты проектирования для систем различной сложности.

Список используемых источников

1. Бесекерский В. А., Попов Е. П. Теория систем автоматического управления. 4-е изд., перераб. и доп. СПб. : Профессия, 2003. 747 с.

2. ГОСТ 29280-92 (МЭК 1000-4-92) Совместимость технических средств электромагнитная. Испытания на помехоустойчивость. Общие положения. М. : Изд-во стандартов, 1992. 44 с.

3. ГОСТ Р 51317.2.5-2000 (МЭК 61000-2-5-95) Совместимость технических средств электромагнитная. Электромагнитная обстановка. Классификация электромагнитных помех в местах размещения технических средств. М. : Изд-во стандартов, 2001. 44 с.

4. ГОСТ 28236-89 (МЭК 68-3-1-74) Основные методы испытаний на воздействие внешних факторов. Часть 3. Дополнительная информация. Раздел 1. Испытания на холод и сухое тепло. М. : Изд-во стандартов, 1998. 43 с.

5. ГОСТ 16019-2001. Аппаратура сухопутной подвижной радиосвязи требования по стойкости к воздействию механических и климатических факторов и методы испытаний. М. : Изд-во стандартов, 2002. 12 с.

УДК 004.514
ГРНТИ 49.33.29

МЕТОДЫ И МОДЕЛИ РЕЗЕРВНОГО КОПИРОВАНИЯ ДЛЯ ЦИФРОВЫХ СРЕД УПРАВЛЕНИЯ

Г. В. Верхова, А. А. Григорьева

Санкт Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обеспечение непрерывного резервного копирования информации, хранящейся в современных средах управления, представляет собой одну из важнейших задач. Резервное копирование должно осуществляться достаточно часто, чтобы в случае сбоя была возможность вернуться к последней актуальной версии, и при этом необходимо обеспечить рациональное представление копируемой информации, чтобы избежать чрезмерного объема резервных копий. В докладе представлен анализ методов и моделей резервного копирования для современных сред управления. Приведены научно-обоснованные предложения по выбору и реализации методов и моделей резервного копирования для цифровых сред управления.

система резервного копирования, методы резервного копирования, цифровые среды.

В настоящее время постоянно возрастают объемы информационных потоков, сохраняемых данных, и как результат – повышается сложность их защиты и обеспечения надёжного хранения [1]. Это влечет ужесточение требований к технологиям резервного копирования, разработке новых эффективных методов, моделей и алгоритмов, используемых в данных технологиях. Каждый метод резервного копирования представляет собой компромисс между характеристиками процессов создания копий, операций восстановления данных и объемами резервных копий [2]. В данной статье рассматриваются методы и модели резервного копирования применительно к цифровым средам управления.

Кратко рассмотрим основные методы резервного копирования (табл., см. ниже), [3]. Классическим методом является метод полного резервного копирования, при котором обеспечивается копирование всех данных, вне зависимости от того, были они подвержены изменениям или нет [4]. Полная резервная копия является обязательной составляющей при использовании всеми другими методами резервного копирования. При дифференциальном резервном копировании изначально создается полная резервная копия данных, а затем, в последующие моменты создаются копии, которые содержат файлы, которые подверглись изменениям с момента совершения последней полой резервной копии. Метод инкрементного копирования

предполагает создание начальной полной резервной копии, после чего создаются копии файлов, которые были изменены с момента создания полной копии (для первого инкремента) или последнего инкремента (для второго и последующего инкрементов). Дельта блочное резервное копирование применяется в связке с инкрементным и дифференциальным методами. При его применении создаются копии только измененных частей данных (дельта-копии), что значительно экономит пространство, необходимое для хранения.

Современные цифровые среды призваны обеспечить единое киберпространство для функционирования технологий «Индустрии 4.0» и постиндустриального общества. Цифровые среды являются гетерогенными, однако содержат значительную долю структурированных данных. Учитывая особенность цифровых сред управления, можно предложить следующую модель *AM* резервного копирования:

$$AM \stackrel{\text{def}}{=} \langle A_1, A_2 \rangle, \quad (1)$$

где A_1 – модель резервного копирования, предоставляемая системами архивирования общего назначения, A_2 – модель резервного копирования, специфичная для цифровых сред управления, реализуемая в рамках данных сред.

В модели A_1 могут быть реализованы сценарии создания резервных копий в определенные моменты времени, используя технологии и рекомендации, применяемые к любым корпоративным информационным системам. В модели A_2 следует реализовать копирование механизмами цифровой среды управления с учетом модели данных (1).

$$A_2 = \{A_2^1, A_2^2\}, \quad (2)$$

где A_2^1 – алгоритм, реализующий дельта блочное резервное копирование; A_2^2 – алгоритм, реализующий инкрементное резервное копирование.

ТАБЛИЦА. Сравнительный анализ методов резервного копирования

Метод	Достоинства	Недостатки
Полное резервное копирование	Высокая надёжность. Быстрое восстановление данных. Простое управление. Все данные содержатся в одной резервной копии.	Требуется большой объем хранилища резервных копий. Генерируется большой сетевой трафик. Длительное время выполнения резервного копирования.
Инкрементное резервное копирование	Высокая скорость резервного копирования (копируются только блоки изменённых данных). Меньший объем хранилища резервных копий по сравнению	Низкая скорость восстановления данных (необходимо восстановить как начальную полную копию, так и все последующие блоки).

	с полным и дифференциальным копированием. Возможность создания большого числа точек восстановления версий.	Надёжность зависит от целостности всех блоков в цепочке (при повреждении одного из инкрементов, восстановление последующих версий не представляется возможным).
Дифференциальное резервное копирование	Резервное копирование осуществляется быстрее чем полное, но медленнее, чем инкрементное. Восстановление версии быстрее, чем при инкрементном копировании, но медленнее чем при полном. Более надежный способ (для восстановления требуется только полная и последняя резервная копия).	Каждая последующая копия выполняется дольше по времени и занимает больший объем в хранилище. Требует достаточно большого объема в хранилище резервных копий.
Дельта блочное резервное копирование	Минимальный объем хранилища резервных копий. Возможность создания максимально большого числа точек восстановления версий.	Восстановить версию можно только теми программам, которыми они были созданы. Невозможно «ручное» восстановление данных. Процесс восстановления данных достаточно медленный.

В модели (1) алгоритм A_2^1 применяется при сохранении пользователем информации в рамках отдельной записи (в ячейки таблицы базы данных или в поле базы данных NoSQL), или автоматическом сохранении. Алгоритм A_2^2 применяется при добавлении или модификации пользовательского файла, а также при создании новой версии документа, информация о котором хранится в базе данных.

Предложенная модель учитывает особенности современных цифровых сред управления, включая киберсреды виртуальных предприятий, и позволяет обеспечить гибкое управление резервным копированием информации, обеспечивая создание большого количества точек восстановления.

Список используемых источников

1. Chervenak A. L., Vellanki V., Kurmas Z., Gup-ta V. Protecting File Systems: A Survey of Backup Techniques // Proc. Joint NASA and IEEE Mass Storage Conference. 1998. PP. 17–31.

2. Kurmas Z., Chervenak A. Evaluating backup algorithms // Proc. of the Eighth Goddard Con-ference on Mass Storage Systems and Tech-nologies. 2000. PP. 235–242.

3. Комаров С. Сравнение способов резервного копирования. Официальный сайт провайдера Selectel. – URL: https://selectel.ru/blog/sravnenie-sposobov-rezervnogo-kopirovaniya (дата обращения: 17.06.2014).

4. Казаков В. Г., Федосин С. А., Иконников С. Е. Моделирование операций резервного копирования для прогнозирования использования объема репозитория // Труды

XV Всероссийской научно-методической конференции Телематика’2008. СПб. : Санкт-Петербургский государственный университет точной механики и оптики, 2008. С. 111–113.

УДК 004.421
ГРНТИ 28.19.23

ИССЛЕДОВАНИЕ АЛГОРИТМОВ АВТОМАТИЧЕСКОГО УВОДА ОТ ПРЕПЯТСТВИЙ АВТОНОМНОГО ПОДВОДНОГО АППАРАТА НА ОСНОВАНИИ ДАННЫХ ЭХОЛОКАЦИИ

Г. В. Верхова, Д. С. Колесов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Одной из основных и наиболее сложных проблем управления автономным беспилотным подводным аппаратом является осуществление навигации и ориентирования аппарата в подводном пространстве в условиях возможных препятствий. Ситуация усугубляется в условиях больших глубинах сложного рельефа донной поверхности. Рассмотрены вопросы возврата подводного аппарата на заданную траекторию, после совершенного маневра уклонения.

планирование пути, поиск пути, увод от препятствий, алгоритмы, беспилотный аппарат.

Осуществляя навигацию и ориентирование в подводном пространстве, автономный беспилотный подводный аппарат (БПА) может столкнуться с неотмеченными на навигационной карте препятствиями или движущимися объектами. Алгоритмы, ведущие подводный аппарат по заданной траектории, должны уметь реагировать на изменяющееся окружающее пространство и уводить аппарат от столкновения (рис. 1). Решения, принимаемые с помощью такого алгоритма, должны иметь высокую степень надёжности, сводя вероятность столкновения аппарата с препятствием к минимуму. После ухода от препятствия БПА должен возвратиться на запланированную траекторию движения.

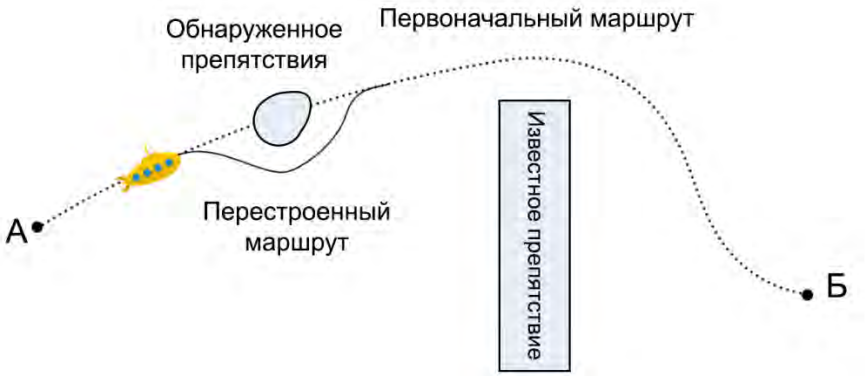


Рис. 1. Концепция увода беспилотного подводного аппарата от препятствий

Задача увода от препятствий является одной из подзадач планирования маршрута, наряду с предварительным построением маршрута. Алгоритмы планирования маршрута различаются по множеству критериев, основными из которых являются:

– время построения маршрута;
– тип окружающей среды (динамический, статический);
– точность построенного маршрута.

Для программ, работающих на небольших автономных платформах, дополнительно проводят разделение алгоритмов по количеству требуемой оперативной памяти.

Статические алгоритмы дают намного более точный результат, однако требуют больше времени на выполнение и не подходят для движения в динамически меняющемся пространстве. Их используют на этапе предварительного построения маршрута. Для своевременного и безопасного увода БПА от препятствий необходимо использовать быстрые алгоритмы, поэтому на этапе увода от препятствий используются динамические алгоритмы, которые дают менее точный результат, однако позволяют вносить изменения в маршрут в реальном масштабе времени. Размеры аппаратного оснащения беспилотного аппарата накладывают ограничения на объём используемой оперативной памяти.

Простейшими алгоритмами увода от препятствий являются алгоритмы семейства Bug, впервые упомянутые в работе В. Люмельского и А. Степанова [1]. Существует множество разновидностей данных алгоритмов, но наиболее часто используются следующие [2]:

– Bug 0 (рис. 2, а): При обнаружении препятствия, беспилотный аппарат двигается вдоль него, пока не сможет продолжить движение по направлению к цели.

– Bug 1 (рис. 2, б): При обнаружении препятствия, беспилотный аппарат огибает его полностью, в поисках точки наименьшего расстояния до цели, и продолжает движение с неё;

– Bug 2 (рис. 2, в): При обнаружении препятствия, беспилотный аппарат двигается вдоль него, пока не выйдет на первоначальную прямую траекторию к цели, и продолжает движение с этой точки.

– Tangent Bug (рис. 2, г): разновидность алгоритма Bug 0, улучшенная с помощью использования технологии компьютерного зрения, которая позволяет находить границы препятствия на некотором расстоянии.

Достоинствами Bug-алгоритмов являются: простата в использовании и реализации; малое время расчётов и быстрота выполнения. К недостаткам можно отнести: не работают при наличии движущихся препятствий; сложный и долгий обход невыпуклых препятствий; не учитывается воздействие водных потоков.

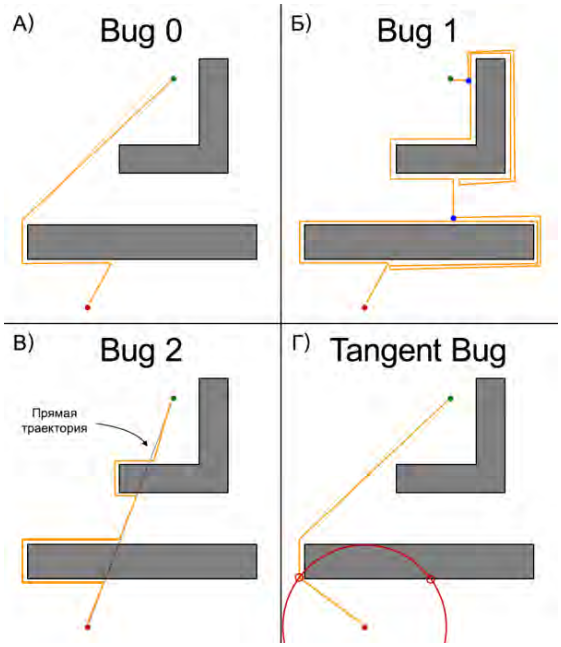


Рис. 2. Bug-алгоритмы: а) Bug 0, б) Bug 1, в) Bug 2, г) Tangent Bug

Для управления беспилотными аппаратами используются также более сложные в применении нечёткие регуляторы. Нечёткие регуляторы или нечёткие контроллеры, используют нечёткую логику, в которой принадлежность входящих данных к тому или иному элементу нечёткого множества может принимать любое значение между 0 и 1, а не только 0 или 1. Обычно элементы множества именуются от N_x (негативное) до P_x (позитивное), либо имеют лингвистические значения. Автором и теоретиком нечёткой логики является Л. Заде [3].

Данные об окружающем мире считываются с датчиков и классифицируются (рис. 3, см. ниже). Обычно определяется расстояние до препятствия и угол траектории движения объекта к препятствию или к цели. С помощью правил нечёткой логики вычисляются управляющие воздействия для определения базового направления и коррекции направления в зависимости от обнаруженных препятствий. Правила формируются только на основе входных данных, функции принадлежности которых должны быть сформулированы таким образом, чтобы обеспечить плавный переход между классами ситуаций.

Достоинствами нечётких регуляторов является: простота использования; простая модификация правил и возможность их оптимизации с помощью алгоритмов машинного обучения; плавное изменение управляющих и выходных сигналов. Недостатками нечётких регуляторов являются: достаточно высокая вероятность зайти в тупик; сложность полного описания поведения для всех возможных ситуаций; возможность неадекватной работы регуляторов при обнаружении небольших объектов.

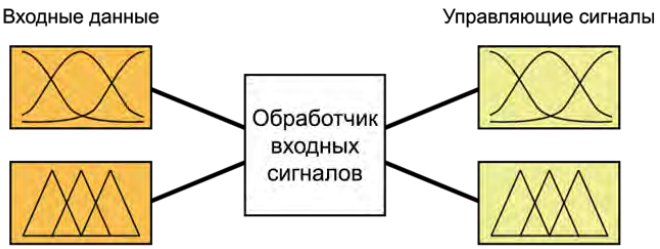


Рис. 3. Работа нечёткого регулятора

Схожим с нечёткими регуляторами принципом работы обладают нейронные сети. Нейронные сети – математическая модель, построенная по принципу организации и функционирования биологических нейронных сетей. Представляет собой систему соединённых синапсами простых искусственных нейронов. Первая нейронная сеть была создана Уорреном МакКалоком и Уолтером Питтсом [4].

На входные нейроны подаются данные об окружающем мире и цели. Обученная нейронная сеть производит вычисления значений нейронов на промежуточных слоях и выводит управляющие сигналы. Взаимодействие между нейронами происходит на основе значений линейных и нелинейных функций. Для обучения нейронной сети можно использовать программные модели или метод экспертных оценок.

Достоинства использования нейронных сетей: возможность работы с любыми наборами входных данных; быстрая работа после обучения; отсутствие необходимости понимания всех аспектов управления БПА для правильной работы нейронной сети. К недостаткам использования нейронных сетей можно отнести: необходимость создания программной модели для процесса обучения; долгое время обучения; отсутствие возможности добавления точных указаний системе управления БПА при различных ситуациях.

Метод потенциальных полей основан на физических заряженных частицах, которые генерируют отталкивающие и притягивающие поля. Вдоль пути следования создаётся притягивающее поле по направлению к цели движения. Препятствия представляются примитивными объектами или их совокупностью, которые генерируют отталкивающее поле (рис. 4). В каждый момент времени вычисляются значения поля в пределах заданного пространства, и по результатам вычисления принимается решение о последующем движении аппарата, благодаря чему аппарат может реагировать на динамически возникающие препятствия и возвращаться на прежний маршрут после их обхода.

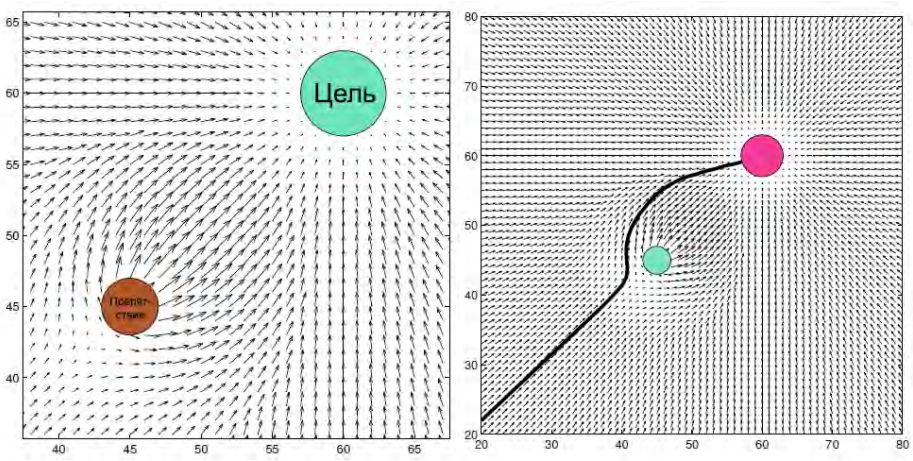


Рис. 4. Принцип работы метода потенциальных полей

Достоинствами данного метода являются: регулируемая скорость работы алгоритма; построение плавной траектории; возможность учёта движущихся препятствий и скорости течения. К недостаткам можно отнести: возможность попадания в локальный экстремум; требования к объему памяти выше, чем у других алгоритмов; необходимость множества вычислений на каждом шаге.

Результаты сравнительного анализа алгоритмов приведены таблице. Полученные результаты позволяют прийти к выводу, что метод потенциальных полей наиболее приемлемый для использования в современных беспилотных аппаратах ввиду более высокой надёжности и приемлемой скорости функционирования.

ТАБЛИЦА. Сравнение алгоритмов по критериям

	Скорость работы на каждом шаге	Скорость развёртывания и настройки	Требуемая память	Надёжность
Bug-алгоритмы	Очень быстрая	Очень быстрая	Малая	Низкая
Нечёткие регуляторы	Быстрая	Средняя	Малая	Средняя
Нейронная сеть	Быстрая	Долгая	Средняя	Средняя
Потенциальные поля	Средняя	Быстрая	Средняя	Высокая

Список используемых источников

1. Lumelsky V. J., Stepanov A. A. Path-planning strategies for a point mobile automaton moving amidst unknown obstacles of arbitrary shape [Электронный ресурс] // Algorithmica 2, 1987. PP. 403–430. URL: https://doi.org/10.1007/BF01840369 (дата обращения: 25.03.2020).

2. Бекасов Д. Е. Применение аппарата нечеткой логики при решении задачи поиска пути в неизвестном окружении [Электронный ресурс] // Молодежный науч.-техн. вестник. МГТУ им. Н.Э. Баумана: электрон. журн. 2012. № 5. С. 40. URL: https://www.math-melpub.ru/jour/article/viewFile/98/105 (дата обращения: 25.03.2020).

3. Zadeh L. A. Fuzzy sets // Information and control, vol. 8. 1965. PP. 338–353.

4. McCulloch W. S., Pitts W. A logical calculus of the ideas immanent in nervous activity // Bulletin of Mathematical Biophysics 5. 1943. PP. 115–133.

5. Sato K. Collision avoidance in multi-dimensional space using Laplace potential // Proc. 15th Conf. Rob. Soc. Jpn. 1987. PP. 155–156.

УДК 004.021
ГРНТИ 28.15.23

СТАБИЛИЗАЦИЯ МЕСТОПОЛОЖЕНИЯ АВТОНОМНОГО ПОДВОДНОГО АППАРАТА В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ТЕЧЕНИЯ

Г. В. Верхова, С. П. Присяжнюк, Н. С. Фёдоров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Автономные подводные телеуправляемые аппараты представляют собой перспективный вид подводной техники, способной решать широкий спектр задач в автоматическом и полуавтоматическом режимах. Достоинствами автономных подводных аппаратов является их относительная дешевизна и отсутствие риска для операторов. Данный вид техники может применяться для задач поиска и обследования подводных объектов, а также выполнения различных манипуляций. Работа автономных подводных аппаратов в условиях воздействия подводных течений требует привлечение мер по стабилизации положения аппарата. Задача стабилизации положения подводного аппарат является достаточно трудной и требует привлечения сложных математических алгоритмов и технических решений. В статье рассмотрены существующие подходы к стабилизации подводных телеуправляемых аппаратов в условиях постоянного внешнего воздействия течения, а также предложена иерархическая архитектура системы стабилизации, обеспечивающая инвариантность модулей, реализующих алгоритмы стабилизации, к датчикам и исполнительным механизмам.

подводные необитаемые телеуправляемые аппараты, стабилизация, подводные течения, МЭМС, ПИД-регулятор, унифицированная архитектура управления беспилотным подводным аппаратом.

Современные тенденции развития электроники и промышленности обусловили широкое применение мобильных роботизированных платформ в различных сферах промышленности и исследовательской деятельности.

Наблюдается непрерывное развитие и разработка роботизированных необитаемых подводных аппаратов военного и научно-исследовательского назначения и создание на их основе автоматизированных информационных комплексов, обладающих широким спектром возможностей для применения в различных областях [1]. Телеуправляемые подводные аппараты применяются для инспекции техногенных объектов, (опоры мостов, подводные кабели, трубопроводы), которые находятся под водой, и доступ к которым может быть затруднён вследствие глубины залегания, ограниченности пространства, а также воздействия опасных для человека факторов, таких как радиационное или химическое загрязнение.

Многие виды работ, выполняемые при помощи телеуправляемых подводных аппаратов, требуют выполнения операций с помощью механических манипуляторов, установленных на аппарате, что требует фиксированного положения подводного аппарата [2]. Данные виды работ требуют повышенной точности позиционирования телеуправляемого подводного аппарата оператором, что многократно осложняется в условиях наличия подводных течений и турбулентных потоков (завихрений), вызванных огибанием водными потоками объектов вблизи от необитаемого подводного аппарата, поэтому необходимо обеспечить стабилизацию автономного подводного аппарата.

Стабилизацию определённых параметров автономного подводного аппарата в условиях воздействия возмущающих факторов можно обеспечить с помощью систем автоматического регулирования, реализующих требуемый закон управления. В процессе управления регулятор производит вычисление ошибки или величины рассогласования $e(t)$ по формуле:

$$e(t) = r(t) - y(t),$$

где $r(t)$ – желаемое значение параметра, $y(t)$ – действительное значение параметра.

Для обеспечения стабильного управления различными параметрами в условиях воздействия внешних возмущений широко применяются ПИД-регуляторы (рис. 1). Пропорционально-интегрально-дифференциальный регулятор (ПИД-регулятор) является наиболее распространенной системой при управлении подводными объектами в режиме стабилизации курса и глубины [2].

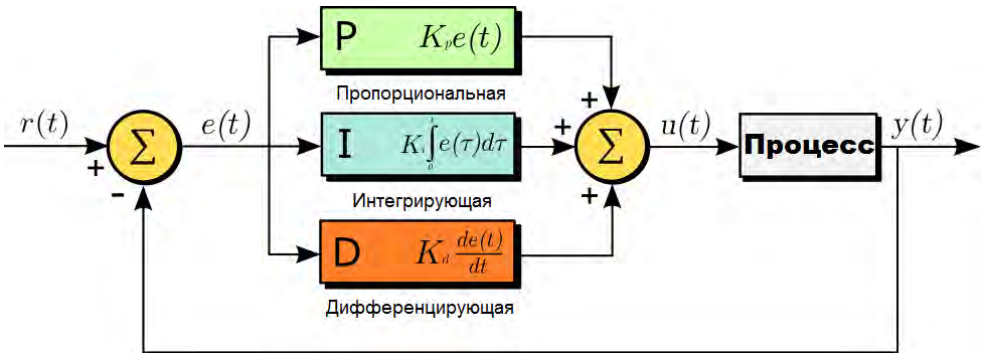


Рис. 1. Схема стабилизации при помощи ПИД-регулятора

ПИД-регулятор генерирует выходной сигнал, который представляет собой сумму трех составляющих сигнала управления: пропорциональной, интегральной и дифференциальной. Уравнение ПИД-регулятора имеет вид:

$$u(t) = K_p \cdot e(t) + K_i \cdot \int_0^t e(\tau)d\tau + K_d \cdot \frac{de(t)}{dt},$$

где $K_p \cdot e(t)$ – пропорциональная, $K_i \cdot \int_0^t e(\tau)d\tau$ – интегральная, $K_d \cdot \frac{de(t)}{dt}$ – дифференциальная составляющие управляющего сигнала.

ПИД-регуляторы достаточно просты в реализации в виде программы для микропроцессорной системы управления автономным подводным аппаратом, однако имеют ряд недостатков, среди которых невысокая эффективность при работе в нелинейных режимах движения, а также отсутствие возможности адаптивной перенастройки регулятора и смены алгоритма регулирования при смене среды и условий, в которых осуществляется стабилизация. Удержание подводного аппарата в стационарном положении требует стабилизации перемещения и поворота по трём осям. Для осуществления стабилизации регулятору необходимо получать информацию о текущих значениях отклонений указанных параметров от заданных значений. Учитывая свойства водной среды, получение таких данных при небольших отклонениях целесообразно получать при помощи акселерометра, совмещённого с гироскопом, и реализованного в виде микросистемного интегрального устройства (МЭМС) [3].

Значение отклонения от заданного положения вычисляется при помощи двойного интегрирования ускорения по выбранным осям. Так как акселерометр измеряет не абсолютное ускорение, а равнодействующую абсолютного ускорения и ускорения силы тяжести, то требуется дополнительная обработка поступающей информации для компенсации постоянной составляющей и подавления шумов.

При глобальном позиционировании подводного аппарата, а также при компенсации существенных смещений, такой способ теряет эффективность из-за падения уровня точности. Ввиду этого необходимо использование дополнительных способов позиционирования аппарата, таких как уточнение глубины при помощи датчиков давления, навигация с применением гидроакустических маяков, а также применения эхолокатора.

Микропроцессорной системе телеуправляемого аппарата приходится получать и обрабатывать большое количество информации, получаемой от различных датчиков и других устройств. Датчики положения, исполнительные механизмы манипуляторов, движители, системы связи и навигации, системы видеонаблюдения, установленные на телеуправляемой платформе, выполнены в виде отдельных модулей. В таких условиях создание монолитной узкоспециализированной системы обработки информации затруднено и нецелесообразно. Создаваемая система управления автономным подводным аппаратам должна строиться по модульному принципу, обеспечивая возможность инкапсуляции отдельных алгоритмов преобразования входящей информации, алгоритмов регулирования и выработки управляющих воздействий.

Разработка системы управления беспилотным подводным аппаратом должна строиться на базе обобщенной архитектуры, в которой идентифицированы функциональные модули и информационные связи между ними (рис. 2, см. ниже). Функциональные модули должны быть распределены по подсистемам (подсистема связи и передачи команд управления, подсистема управления двигательными устройствами, подсистема сбора информации с датчиков физических величин, подсистема стабилизации).

В предложенной архитектуре подсистема стабилизации является одним из унифицированных укрупненных функциональных модулей, что обеспечивает возможность её разработки и тестирования независимо от других подсистем. Дальнейшая декомпозиция подсистемы стабилизации на отдельные функциональные блоки обеспечивает высокую гибкость и универсальность за счёт возможности перенастройки и динамической замены блоков во время эксплуатации автономного подводного аппарата.

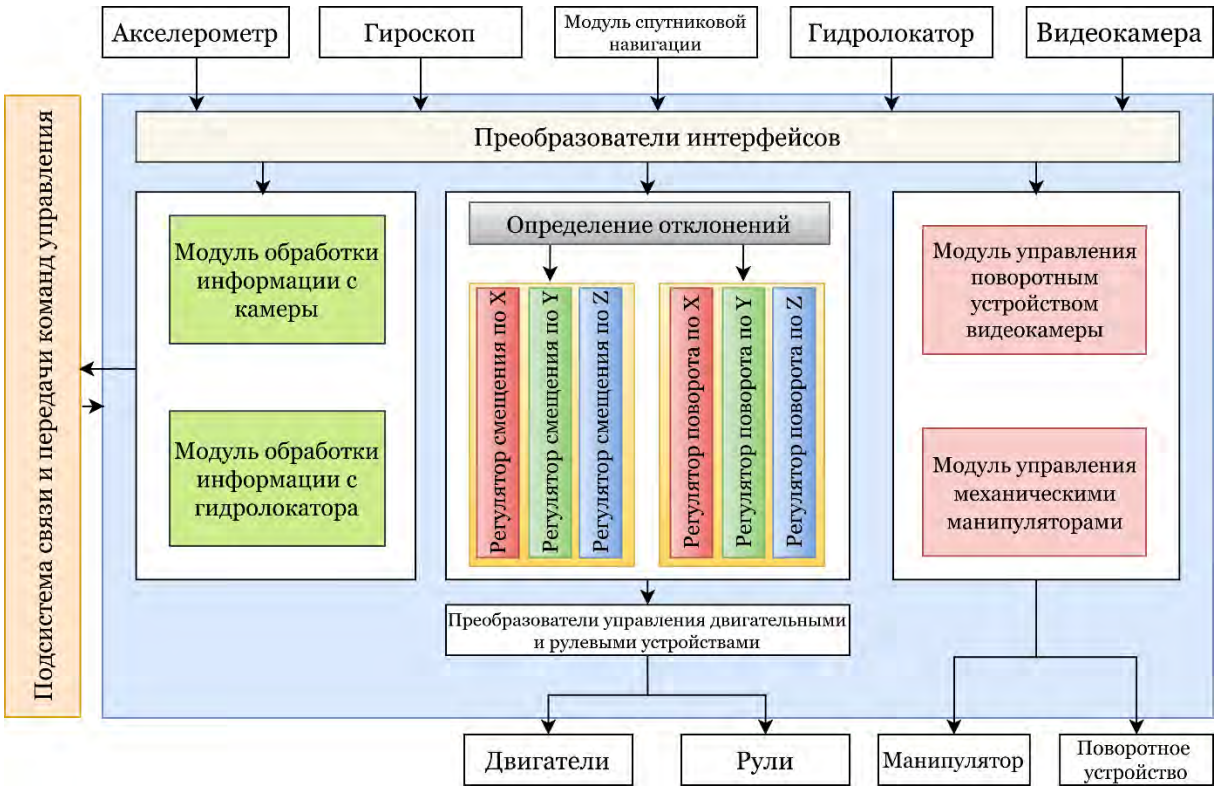


Рис. 2. Блочно-модульная иерархическая структура автономного подводного телеуправляемого аппарата

Список используемых источников

1. Бардачевский Н. Н., Безсуднов Е. Ю. Состояние и перспективы применения необитаемых подводных аппаратов в области гидрографических исследований и подводной навигации // Интерэкспо Гео-Сибирь. 2013. С. 124–128

2. Ваулин Ю. В., Костенко В. В., Павин А. М. Навигационное и алгоритмическое обеспечение ТНПА для эффективного решения задач идентификации донных целей и инспекции морских объектов [Электронный ресурс] // Технические проблемы освоения мирового океана : материалы пятой всероссийской научно-технической конференции. 2013. URL: http://www.imtp.febras.ru/images/stories/konf/tpomo-5-30-sentjabrja-4-oktjabrja-2013/pdf/sekcija1.pdf (дата обращения: 10.03.2020).

3. Матвеев В. В., Погорелов М. Г. Система измерения вертикальной качки волномерного буя // Известия Тульского государственного университета. Техничесекие науки. Вып. 9. Ч. 2. Тула : Изд-во ТулГУ, 2014. С. 267–275

УДК 004.514
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ МЕТОДОВ И АЛГОРИТМОВ ПОСТРОЕНИЯ И ОПТИМИЗАЦИИ МАРШРУТА ДВИЖЕНИЯ ПОДВОДНОГО АППАРАТА В УСЛОВИЯХ СЛОЖНОГО РЕЛЬЕФА ДОННОЙ ПОВЕРХНОСТИ

Г. В. Верхова, С. П. Присяжнюк, М. А. Хвостов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Одной из важнейших задач управления беспилотными транспортными средствами, работающими в автономном режиме с минимальным участием оператора, является построение оптимального маршрута движения в условиях сложного рельефа донной поверхности. Решение данной задачи требует выполнения сеточной аппроксимации пространства, в котором функционирует необитаемый подводный аппарат, преобразования сетки в граф и нахождения оптимального пути на данном графе. В статье представлены результаты анализа методов построения графа для определения оптимального пути подводного аппарата с учетом нескольких факторов. Рассмотрены сетки с равномерным, случайным распределением вершин, распределением вершин при триангуляции, отображения сеток на граф, а также алгоритмы поиска оптимального пути на полученных графах.

оптимизация маршрута, поиск оптимального пути, оптимизационные алгоритмы, графы, сеточная аппроксимация.

Одной из важнейших задач управления беспилотными подводными аппаратами, работающими в автономном режиме с минимальным участием оператора, является построение оптимального маршрута движения в условиях сложного рельефа донной поверхности. Решение этой задачи требует выполнения сеточной аппроксимации пространства, в котором функционирует необитаемый подводный аппарат, преобразования сетки в граф и нахождения оптимального пути на данном графе.

Задачу нахождения оптимального пути, можно свести к задаче поиска на графе, в котором вершины представляют точки сетки, аппроксимирующей акваторию, в которой функционирует необитаемый подводный аппарат. В данных задачах графы обычно бывают ориентированными, что означает, что по ребрам можно перемещаться только в одном направлении. Существует множество задач поиска на графах, которые относятся к NP-полным задачами, для которых в настоящий момент неизвестны алгоритмы, обладающие полиномиальной сложностью. Типичной NP-полной задачей является задача о коммивояжере.

Одним из наиболее популярных алгоритмов поиска оптимального пути на графе является алгоритм Дейкстры, а также его усовершенствованный вариант – *A**. В алгоритме *A** последовательность обхода вершин графа определяется эвристической функцией. Так же стоит отметить алгоритм поиска в ширину и алгоритм поиска в высоту, хоть они и не всегда оптимальны. Существуют модифицированные версии алгоритма A*, наиболее популярными из которых являются JPS (рис. 1) и IDA*.

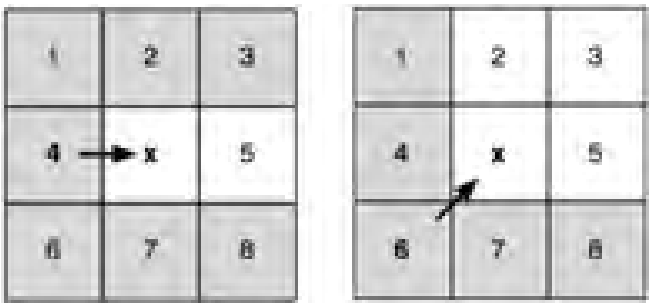


Рис. 5. Принцип работы алгоритма JPS

Функционирование перечисленных выше алгоритмов требует наличия графов, на которых будет осуществлять поиск. Как было отмечено выше, в случае оптимизации траектории движения автономного подводного аппарата в условиях сложного рельефа донной поверхности можно выделить несколько способов построения сеток и их отображения на граф. Самым простым и интуитивно понятным является равномерное распределение вершин графа в пространстве (рис. 2, см. ниже). Основным достоинством такого способа распределения вершин графа является возможность задавать расстояние между вершинами, и, таким образом, контролировать точность перемещения подводного аппарата. К недостаткам можно отнести существенное повышение вычислительной трудоемкости работы алгоритма при повышении точности определения траектории движения автономного подводного аппарата.

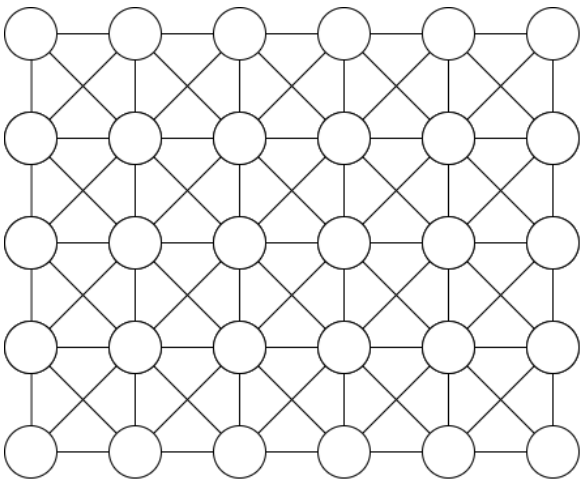


Рис. 6. Пример равномерно распределенного графа

Случайное распределение вершин аппроксимирующей сетки в пространстве акватории (рис. 3) может привести к аварии подводного аппарата, поэтому, для корректного определения траектории движения необходимо модифицировать алгоритмическую часть формирования сетки, а также поисковых алгоритмов. Однако используя эвристики, модифицирующие плотность вероятности распределения вершин аппроксимирующей сетки, можно значительно ее улучшить, делая распределение вершин более плотным у донной поверхности. Таким образом, повышается точ-

ность определения траектории движения подводного аппарата и увеличивается скорость работы алгоритма по сравнению со случаем равномерно распределенного графа.

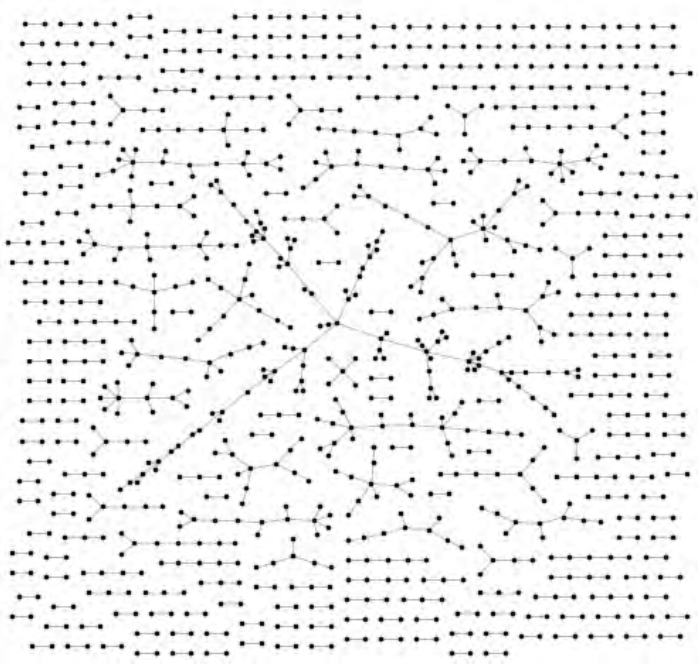


Рис. 7. Пример графа со случайным распределением

Третьим методом построения аппроксимирующей сетки и графа является метод триангуляции, который основан на копировании треугольных поверхностей, ограниченных ребрами графа (рис. 4).

Из результатов проведенного анализа следует, что для построения и оптимизации маршрута движения подводного аппарата в условиях сложного рельефа донной поверхности следует использовать комбинацию равномерного распределения вершин и модифицированного случайного распределения. Равномерное распределение вершин следует использовать в однородных частях акватории, а модифицированное случайное распределение – в близи донной поверхности.

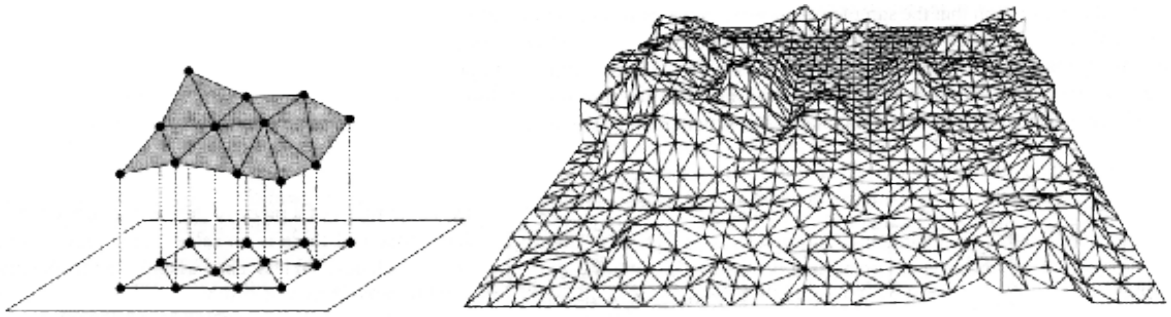


Рис. 8. Триангуляция поверхности и получение графа

Список используемых источников

1. Рафгарден Т. Совершенный алгоритм. Графовые алгоритмы и структуры данных. СПб. : Питер. 2020. 256 с. ISBN 978-5-4461-1272-2.

2. Дасгупта С., Пападимитриу Х., Вазирани У. Алгоритмы: пер. с англ. М. : МЦНМО. 2014. 320 с. ISBN 978-5-4439-0236-4.

3. Харари Ф. Теория графов. М. : Мир, 1973. 300 с.

4. Скворцов А. В., Мирза Н. С. Алгоритмы построения и анализа триангуляции. Томск : Изд-во Томского ун-та, 2006. 168 с. ISBN 5-7511-2028-5.

УДК 004.056.5
ГРНТИ 50.37.23

ЗАЩИЩЕННАЯ СИСТЕМА ТЕРМИНАЛЬНЫХ ПРОГРАММ НА ОСНОВЕ ЛУКОВИЧНОЙ ВИРТУАЛИЗАЦИИ ИСПОЛНЯЕМОГО КОДА

А. Н. Вихарев, Д. О. Маркин

Академия ФСО России

В статье описана защищенная система терминальных программ на основе луковичной виртуализации исполняемого кода. Описан объект защиты, разработан протокол защищенного взаимодействия, а также алгоритмы функционирования отдельных элементов системы защиты. Экспериментально подтверждена работоспособность системы.

виртуальная машина, обфускация, интерпретатор, байт-код, протокол защищенного взаимодействия.

Повсеместное внедрение информационных технологий, средств автоматизации и автоматизированных систем в повседневную жизнь, развитие цифровой экономики значительно повышает роль программного обеспечения в современной экономике. В связи с этим недостаточная защищенность программного обеспечения от анализа, нарушения его работоспособности, модификации и других угроз может привести к серьезным неблагоприятным последствиям различного характера и масштаба. Таким образом, проблема обеспечения защищенности программного обеспечения (ПО) является актуальной и требует применения новых методов и средств, способных обеспечить требуемый уровень защиты в современных условиях.

Проблема защиты программных реализаций на основе применения технологий виртуализации и других методов защиты затрагивалась в научных трудах Аранова В. Ю., Петрова А. С. [1, 2, 3], Речистова Г. С. [4], а также Казарина О. В., Варнавского Н. П., Захарова В. А., Кузюрина Н. Н. и Шокурова А. В. [5, 6], Зегжды П. Д., Бойко В. П., Заборовского В. С., Подловченко Р. И., Иванникова В. П., Сомборсона К., Викстромома Д. и др. В указанных работах отмечалась необходимость защиты программных реализаций от технологий обратной разработки, основанных, в том числе на методах статического и динамического анализа ПО.

Одним из наиболее эффективных способов защиты исходного текста ПО от анализа, не исключающий применения других методов, является

внедрение технологии виртуализации кода. Такой подход позволяет сформировать ПО, состоящее архитектурно из двух компонентов – виртуальной машины/интерпретатора или их множества и байт-кода, при этом в зависимости от наличия лицензии у пользователя (права на использование ПО) исполняемый байт-код может преобразовываться к виду, который сможет быть обработан встроенной виртуальной машиной или интерпретатором без ошибок. Данный подход описан в работах [7, 8].

В данной работе объектом защиты являются терминальные программы, передаваемые между узлами системы, обеспечивающей их исполнение на данных узлах [9, 10, 11]. Для защиты от анализа исполняемого кода таких терминальных в данной работе предлагается система на основе виртуализации исполняемого кода с применением луковичной и чесночной архитектуры.

Реализация концепции активных данных базируется на применения скриптовых языков программирования, таких как PHP, Perl, Python, Ruby, JavaScript и других, а также способности приложений, выполняющих роль интерпретатора, обрабатывать содержание данных (например, тела HTTP(s)-запросов) как программный код [12, 13]. Иллюстрация такого применения скриптовых языков в контексте реализации концепции активных данных представлена на рис. 1.

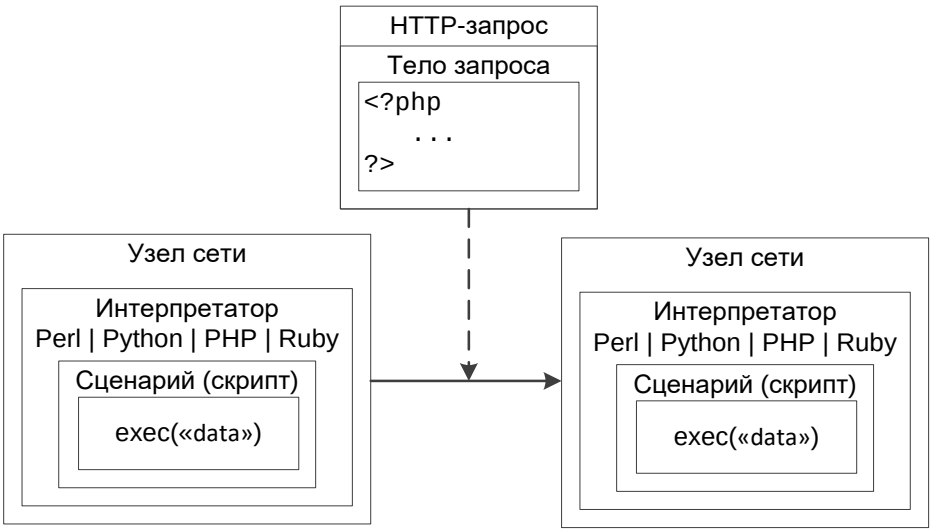


Рис. 9. Реализация концепции активных данных
на основе применения скриптовых языков

Эффективность такой реализации была проверена в работах [12, 13] на базе сети веб-прокси серверов с помощью ряда разработанных программных средств (свидетельства регистрации в Реестре программ для ЭВМ ФИПС №№ 2016617298, 2018660343).

Общая структурная схема системы, в которой осуществляется обмен и исполнение активных данных (терминальных программ) представлена на рис. 2, где ВМ – виртуальная машина.

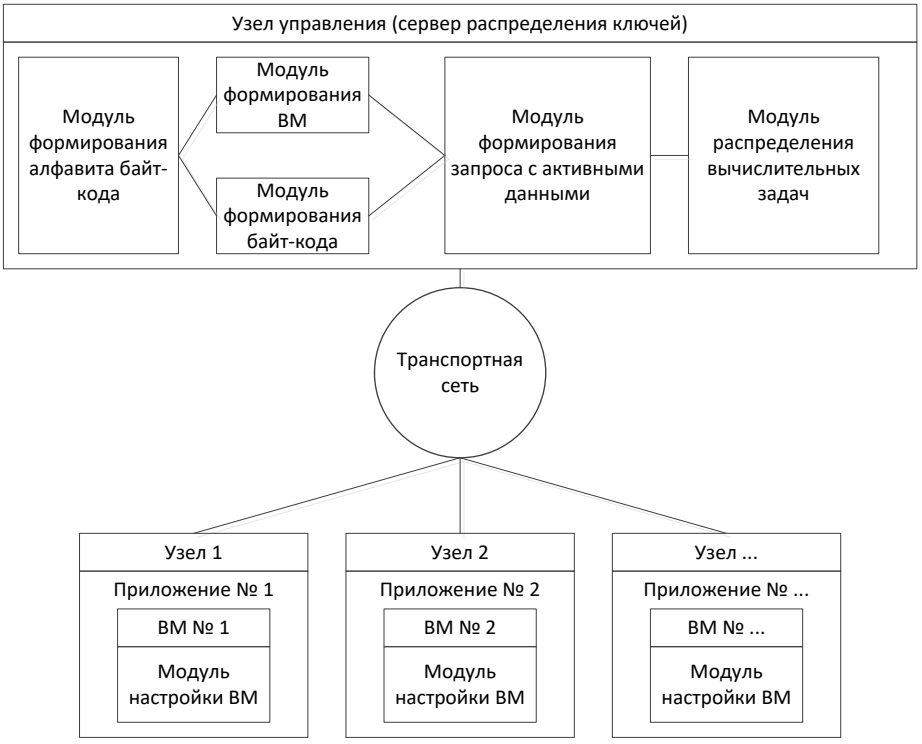


Рис. 10. Структурная схема система обмена терминальными программами

Рассмотренная модель системы защиты реализована в виде протокола. Указанный протокол реализует защищенное взаимодействие узлов распределенной системы терминальных программ.

Основные компоненты системы:

– веб-форма;

– управляющая программа;

– контроллер виртуальных машин (КВМ);

– множество реализаций виртуальных машин (ВМ);

– база данных (БД);

– опрашивающая программа.

Пример графического интерфейса с отображением статуса состояния виртуальных машин лабораторного стенда системы терминальных программ представлен на рис. 3.

Рис. 11. Интерфейс системы мониторинга состояния узлов

Протокол защищенного взаимодействия узлов распределенной системы терминальных программ реализуют несколько приложений:

– веб-приложение для управления параметрами системы;

– приложение опроса состояния узлов;

– приложение управления состоянием узлов;

– приложение контроллера узлов распределенной системы терминальных программ.

На рис. 4 (см. ниже) представлен интерфейс приложения управления состоянием узлов.

Таким образом, работоспособность системы защиты активных данных в распределенной вычислительной системе проверена экспериментально. Полученная система отвечает требованиям:

– авторизации исполняемого кода, передаваемого на узлы от системы управления;

– компрометация узлов не влияет на способность нарушителя использовать функционал нескомпрометированных узлов.

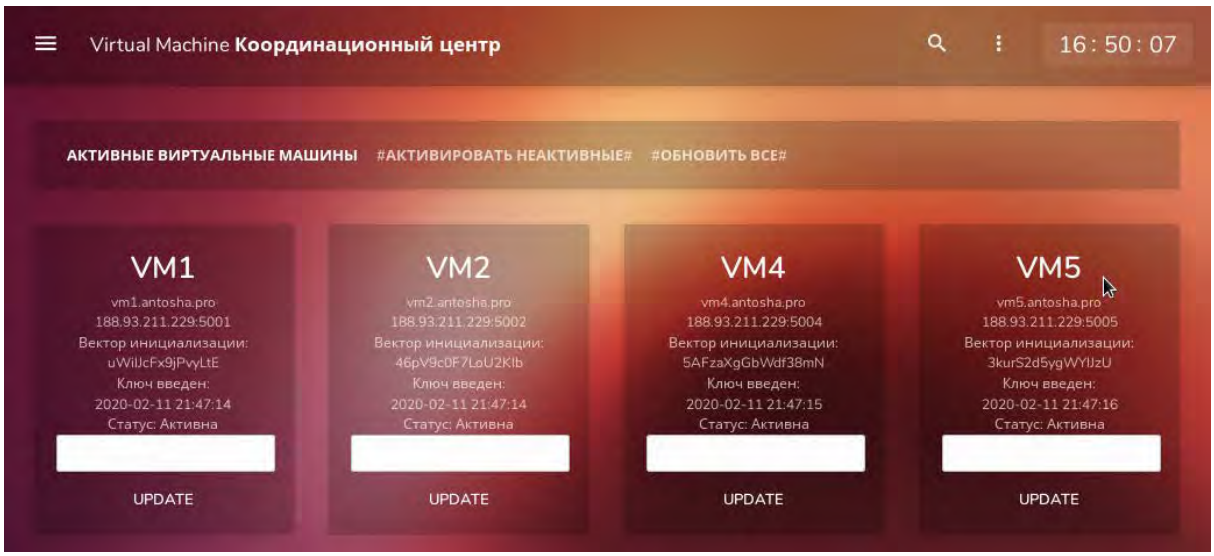


Рис. 12. Интерфейс приложения управления состоянием узлов

Выводы

В работе были предложена система защиты активных данных в распределенной вычислительной системе на основе применения виртуальных машин и протокол, ее реализующий. Сформированы требования к ней, на основе проведенного анализа условий функционирования. Разработаны и описаны модели угроз и нарушителя безопасности программного обеспечения распределенной вычислительной системе на основе активных данных.

Предложена математическая модель системы защиты активных данных от анализа на основе виртуализации исполняемого кода, а также программная реализация протокола защищенного информационного взаимодействия узлов системы на PHP, Python.

Экспериментально проверена и подтверждена работоспособность системы. Программные реализации элементов системы и протокола зарегистрированы в ФИПС (свидетельства регистрации в Реестре программ для ЭВМ ФИПС №№ 2016617298, 2018660343, 2019665285).

Список используемых источников

1. Петров А. С., Петров А. А. Методы защиты программного кода // Системы обработки информации. 2010. Вып. 3 (84). С. 68–71.

2. Петров А. С., Петров А. А. Технология защиты программного кода посредством применения виртуальной машины // Вестник ВНУ. 2009. № 9 (103), часть 1. С. 117–122.

3. Аранов, В. Ю. Метод и средства защиты исполняемого программного кода от динамического и статического анализа : автореф. дис. … канд. техн. наук : 05.13.19 / Аранов Владислав Юрьевич. Санкт-Петербург, 2014. 18 с.

4. Речистов Г. С., Елюгин Е. А., Иванов А. А. и др. Программное моделирование вычислительных систем : учеб. пособие / 2-е изд., испр. и доп. М. : МФТИ, 2013. 222 с.

5. Казарин О. В., Шубинский И. Б. Надежность и безопасность программного обеспечения. М. : Издательство Юрайт. 2018. 342 с.

6. Варнавский Н. П., Захаров В. А., Кузюрин Н. Н., Шокуров А. В. Современное состояние исследований в области обфускации программ: определение стойкости обфускации // Труды ИСП РАН. 2014. Т. 26. Вып. 3.

7. Kaiyuan Kuang, Zhanyong Tang, Xiaoqing Gong, Dingyi Fang, Xiaojiang Chen, Zheng Wang Enhanced virtual-machine-based code obfuscation security through dynamic bytecode scheduling // Computers & Security. 2018. № 74. PP. 202–220.

8. Barak B., Goldreich O., Impagliazzo R., Rudich S., Sahai A., Vadhan S., Ke Yang. On the (im)possibility of obfuscating programs // Advances in Cryptology – CRYPTO'01, Lecture Notes in Computer Science, v. 2139, 2001. PP. 1–18.

9. Кулешов С.В., Цветков О.В. Активные данные в цифровых программно-определяемых системах // Информационно-измерительные и управляющие системы. 2014. Т. 12. № 6. С. 12–19.

10. Александров В. В., Кулешов С. В., Цветков О. В., Зайцева А. А. Концепция построения инфотелекоммуникации (прототип SDR) // Труды СПИИРАН. 2008. № 6. С. 51–57.

11. Маркин Д. О. Макеев С. М., Вихарев А. Н. Комплекс алгоритмов защищенных туманных вычислений на основе технологии активных данных // Известия Тульского государственного университета. Технические науки. 2019. Вып. 3. С. 263–269.

12. Маркин Д. О., Галкин А. С., Архипов П. А. Организация анонимного доступа с помощью веб-прокси // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8, № 5. С. 44–49.

13. Маркин Д. О., Галкин А. С., Архипов П. А. Исследование устойчивости анонимной сети на основе технологий веб-прокси // Вопросы кибербезопасности. 2016. № 2 (15). С. 21–28.

УДК 004.942
ГРНТИ 28.17.31

ИНТЕЛЛЕКТУАЛИЗАЦИЯ ФУНКЦИОНАЛЬНО-СТОИМОСТНОГО АНАЛИЗА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И СИСТЕМ

Д. В. Волошененко, В. Л. Литвинов, Л. Д. Трофимова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрено внедрение машинного обучения в процедуру проведения функционально-стоимостного анализа (ФСА). Были выделены этапы проведения ФСА, проанализированы информационные характеристики этапов и процедур для определения информационной модели процесса ФСА. Проведено моделирование алгоритма машинного обучения для помощи в проведении ФСА объекта. Подведены итоги в указании достоинств и недостатков машинного обучения при проведении функционально-стоимостного анализа.

машинное обучение, интеллектуализация, функционально-стоимостной анализ, информационная модель.

Одним из научных способов для принятия управленческих решений выступает функционально-стоимостный анализ (ФСА). Он содержит группу методов, которые направлены на постоянный поиск ненужных затрат при производстве продукта или оказании услуги. Особенностью данного фактора выступает нацеленность на эффективное устранение затрат без ущерба для их качества и эффективности. Данные затраты входят в продукт или услугу, но не улучшают их качество и эффективность, не продлевают срок службы и не обеспечивают дополнительного удовлетворения клиенту. При устранении перечисленных затрат и условий, стоимость продукта или услуги может быть скорректирована, а качество продукта или оказания услуги будет прогрессировать.

Объектами ФСА могут выступать [1]: организационные и управленческие процессы и структуры, качество продукции, конструкция изделия, технологический процесс.

Эффективное проведение ФСА включает выполнение следующих основных этапов [2]:

1. Планирование и подготовка: уточняется объект и цели ФСА.
2. Информационный: сбор сведений об объекте.
3. Аналитический: составление функциональной структуры, определение стоимости и ценности отдельных функций, выбор направления работы.
4. Творческий: улучшение решения на основе привлечения эвристических, математических и экспериментальных методов, выбор лучших вариантов.
5. Рекомендательный: оформление протоколов и рекомендаций по реализации предложений.

Для ФСА характерно последовательное, поэтапное выполнение работ, начиная с выбора объекта анализа и сбора имеющейся информации и заканчивая выработкой предложений по изменению исследуемого объекта, направленных на снижение затрат.

Процесс проведения ФСА – это многократное получение информации об объектах, её обработка, анализ и принятие решений. Поэтому автоматизация путём использования информационных технологий для передачи обработки наиболее трудоёмких операций программным комплексам является необходимой задачей. Для решения задачи организации информационного обеспечения ФСА необходимо проанализировать с информационных позиций как сам процесс ФСА, так и объект, подвергаемый ФСА. Анализируя информационные характеристики этапов и процедур ФСА, информационные связи, которые возникают в ходе проведения ФСА, входные и выходные данные, структурно-логическую схему ФСА, получают информационную модель процесса ФСА.

Из числа методов поиска технических идей и решений, которые часто применяются на творческом этапе ФСА, является морфологический анализ. Данный метод может быть успешно применен для упорядоченного представления альтернатив решения сформулированных инженерных задач по совершенствованию, рационализации каждой функции. Для этого строится классификационная таблица или морфологическая матрица. В левой её части приводятся все функции изделия, а в правой – потенциально возможные способы их осуществления. Каждому способу в соответствующей ячейке матрицы приписываются величины затрат и полезного эффекта, рассчитанные или по смете, или по эмпирическим формулам. Исследуются все потенциальные, т. е. конструктивные и технологически реализуемые сочетания способов выполнения функций. Общее их число может быть значительным. Оно равно $N = m^n$ (N – число вариантов сочетания функций, m – число анализируемых способов выполнения одной функции, n – число выделенных функций) [3].

Для проведения всех этапов морфологического анализа есть возможность в использовании методов машинного обучения. Машинное обучение включает множество различных подходов и алгоритмов. Смысл машинного обучения состоит в использовании выбранных признаков для построения моделей, подходящих для решения поставленных задач. Для построения модели, в качестве основного алгоритма можно выбрать несколько подходов и использовать различные алгоритмы машинного обучения. Выбор алгоритма исходит не с точки зрения быстродействия или потребления памяти, а правильности получения конечного результата.

Построение алгоритма для анализа формулировок функций сводится к нескольким этапам. Разбиение формулировок на отдельные графемы и выделение морфологической структуры этих графем происходит с использованием словарных или бессловарных методов простыми вычислительными алгоритмами. Для проведения синтаксического и семантического анализа использование методов машинного обучения может обеспечить более точную и быструю обработку массивов данных при проведении ФСА. Синтаксический анализатор создает группы слов с одинаковым синтаксическим значением. Затем строится семантическое дерево, в котором группы слов относятся к одному из узлов. Узлы дерева относятся ко множеству различных типов отношений. Для поиска аналогичных формулировок используются различные типы отношений между словами. Простая структура данных отношений позволяет сократить временные издержки.

Для решения этой задачи машинного обучения, основанной на построении и анализе семантико-синтаксического дерева, подходит такие методы, как метод деревьев признаков, метод k-ближайших соседей (kNN) и нейронные сети [4]. Для решения данной задачи выбор нейронных сетей является одним из наиболее подходящих.

В этом случае поставленная задача может быть рассмотрена как задача классификации точек в *n*-мерном пространстве, при которой можно использовать метод обучение нейронной сети с учителем. С учётом специфики предметной области и анализа достоинств и недостатков известных нейронных сетей, можно выбрать следующие типы – многослойный персептрон и LSTM-сеть. В качестве входных данных сети, например, можно использовать набор параметров, полученный для соответствующей пары исследуемых слов в предложении и представленный в виде вектора действительных чисел. Выходные данные – числовой вектор «01» или «10», являющееся ответом на вопрос: «Найдено ли искомое отношение в тексте?» («01» – не найдено, «10» – найдено).

Для определения семантического смысла анализируемой пары слов будем каждое из них сопоставлять с каким-либо семантическим классом. Считается, что два слова принадлежат к одному семантическому классу, если они имеют одинаковый смысл в заданном контексте. Соответствия слов семантическим классам и определённому контексту определяются по начальной форме слов и хранятся в базе данных. Начальная форма слова и его морфологические характеристики вычисляются на этапе морфологического анализа. Для каждого из типов отношений используется собственный анализатор на основе нейронной сети. Данный анализатор имеет доступ к модулю морфологического анализа, чтобы выделять необходимые параметры, например, согласование слов по форме. Информация, содержащая начальную форму слова, его морфологические характеристики и принадлежность к семантическим классам в определённом контексте хранится в базе данных.

На данном этапе развития в современном мире машинное обучение, не может полностью заменить участие оператора при проведении ФСА. Стоит отметить, что небольшая часть работы все равно остается за человеком. Именно ему предстоит провести анализ данных, который показывает лишь предположительное указание о возможном результате и не может дать полную уверенность в результате и автоматически провести всю работу. Оператор более точно настраивает алгоритм работы модели, что позволяет систематизировать и упростить работу на предложенных данных. Актуальность данной задачи в современном мире заключается в улучшении характеристик выпускаемого товара или оказании услуг и повышении точности работы построенной модели, что является очевидным фактом для продолжения работы в данном направлении.

Список используемых источников

1. Моисеева Н. К., Карпунин М. Г. Основы теории и практики функционально-стоимостного анализа: учебное пособие. М. : Высшая школа, 1988. 192 с.

2. Герасимов В. М., Калиш В. С., Карпунин М. Г., Кузьмин А. М., Литвин С. С. Основные положения методики проведения функционально-стоимостного анализа: методические рекомендации. М. : Информ-ФСА, 1991. 40 с.

3. Одрин В. М., Картавов С. С. Морфологический анализ систем. Построение морфологических таблиц. Киев : Наукова думка, 1977.

4. Флах П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных. М. : ДМК Пресс, 2015.

УДК 687.016.5
ГРНТИ 64.33.14

СПЕЦИФИКА МОДЕЛИРОВАНИЯ ПЕРСОНАЛИЗИРОВАННЫХ ШВЕЙНЫХ ИЗДЕЛИЙ

Д. В. Волошинов, А. С. Гесь

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются особенности моделирования персонализированных швейных изделий. Описаны программные комплексы САПР, представленные на зарубежном и отечественном рынке. Приведены методы снятия индивидуальных мерок. Предложена методика проектирования и моделирования изделий с помощью свободного программного обеспечения.

индивидуальный пошив, 3Д моделирование одежды, антропометрические метки.

В настоящее время существует тенденция бурного развития информационных технологий в области трехмерного моделирования одежды. Важным фактором развития является усовершенствование систем автоматизированного проектирования. Данные системы используют не только в массовом швейном производстве, но также и при индивидуальном пошиве, при производстве компьютерной и игровой графики.

Примерами изделий индивидуального пошива могут служить:

– вещи нестандартной размерной сетки, например, больших размеров;

– одежда для инвалидов и людей с физическими особенностями;

– вещи индивидуального покроя – мужские костюмы, свадебные платья;

– профессиональная одежда, туристическое снаряжение (палатки, тенты и т. д.);

– пошив костюмов или элементов одежды для животных, например, комбинезоны для собак, попоны (согревающая накидка) для лошадей, сумки-переноски и др.;

– дизайнерские изделия, сумки, кошельки, седла, обивка салона и т. д.

Все эти изделия отличаются более высокой стоимость производства относительно массового производства, однако, они более комфортные, имеют лучшую посадку по фигуре и пожеланиям заказчика.

В процессе производства таких изделий возникают следующие вопросы:

– «Кто будет производить изделие?»

– «Как учесть индивидуальные пожелания заказчика, например, его антропометрические особенности?»

– «Какова стоимость готового изделия?».

Рассмотрим последовательно эти вопросы.

Ответом на первый вопрос является факт существования необходимости индивидуального пошива изделия, а значит, заказчик не смог найти подходящее ему изделие у массового производителя. Следовательно, заказчика интересует единичное изделие или мелкосерийное – штучное производство. Исполнителями такого производства чаще всего являются ателье по пошиву или частные мастера. Стоит отметить, что с развитием сети интернета и технологий моделирования одежды заказчики все чаще пользуются услугами частных мастеров, которые могут находиться в другом городе, регионе или стране.

Вернемся к вопросу учета индивидуальных особенностей. В последние годы данной проблеме уделяется все больше внимания.

К примеру, статья Гусевой М. А. посвящена важной проблеме индивидуального пошива – созданию индивидуального 3Д аватара человека, 3Д модели, которая бы отражала физиологические особенности заказчика. Данная задача решается при помощи снятия антропометрических измерений различных частей тела. Автор при помощи технологии Kinect от компании Microsoft создала 3Д библиотеку аватаров на основе 685 женских фигур, что в последующем позволило разработать систему индивидуальных антропометрических маркеров на теле человека, проецируемую на абрисы (контуры) типовой фигуры по фотографии [1].

Работа Василевской Л. В. посвящена разработке индивидуальных изделий для животных. Автор предлагает систему кинометрических меток, необходимых для измерения размерных признаков собак и систему прибавок к измеренным величинам, которые обеспечат комфорт животному при динамической активности [2].

Социальная значимость антропометрического измерения продемонстрирована в работе Григорьевой Е. В., где произведен анализ особенностей телосложения людей с нарушениями осанки [3]. Автором обусловлена неточность стандартных размерных признаков для людей с заболеваниями опорно-двигательного аппарата. Предложены дополнительные размерные признаки и методы обмера фигур по фотографии, позволяющие получить

недостающую антропометрическую информацию. Проблеме изготовления одежды для людей с нарушением осанки так же посвящены работы Гусевой М. А. и Yan Hong, авторы предлагают разрабатывать 3Д модель на основе произведенного 3Д сканирования фигуры и последующего моделирования ткани [4, 5, 6].

Выделим основные методы построения 3Д модели с учетом антропологических особенностей:

– измерение с помощью портного метра;

– использование антропологических маркеров на фотографии фигуры;

– использование 3Д сканирования фигуры.

В сфере швейного производства подобные методы получения 3Д моделей используются для последующего наглядного конструирования изделия, поиска творческих решений и визуализации изделия заказчику [7]. Наиболее популярными 3Д программами в индустрии моды и швейного производства являются Marvelous designer, CLO 3D, TUKA 3D. Имеют место применения САПР общего назначения, такие как AutoCAD, Rhino, 3Д пакеты: Maya, Blender, Zbrush.

Из отечественного программного обеспечения стоит выделить САПР СТАПРИМ, АССОЛЬ, Грация, Графис, Julivi. При рассмотрении данных комплексов программ был выявлен ряд недостатков.

Отечественные САПР швейной промышленности обладают устаревшим, не интуитивно понятным, интерфейсом пользователей. Программы содержат излишнее количество иконок, строк с параметрами, множество вложений в меню. Пользователю, знакомому с интерфейсами и принципами работы зарубежных аналогов, придется потратить значительное время для ознакомления с работой отечественных САПР.

Другим недостатком является ориентированность на плоскостное проектирование изделия, функции 3Д моделирования и визуализации либо отсутствуют полностью, либо сильно ограничена. В связи с этим было неоднократно замечено, что многие рядовые пользователи предпочитают строить лекала в отечественной САПР, а затем переносить чертеж в зарубежную САПР с целью построения 3Д модели и дальнейшей работы.

Определяющим фактором при использовании САПР является стоимость лицензии, например, для осуществления коммерческой деятельности. Построим таблицу сравнения стоимости индивидуальной лицензии (для одного лица) и корпоративной. Для сравнения с иностранными аналогами приведем стоимость в рублях по курсу ЦБ на 06.12.19: $1 – 63,71 руб. Результат сравнения представлен в таблице.

ТАБЛИЦА. Сравнение стоимости лицензированного ПО

САПР	Индивидуальная, руб.	Для малого бизнеса, руб.	Примечание
Marvelous Desinger	19 114 – годовая подписка 28 671 – одна версия навсегда	108 316–382 292	Коммерческая подписка зависит от количества компьютеров с ПО
CLO 3D	28 671 – для некоммерческого индивидуального использования	344 062	
САПР ГРАЦИЯ	Для Фрилансеров – 175 000 Для Любителей шитья – 75 000	Для Предприятий – 450 000 Для Ателье – 275 000	Аренда на год от 15 до 90 тыс. руб.
СТАПРИМ	220 000 Поставляется с технологий снятия мерок по фото – «ФОТООБМЕР»		
АССОЛЬ	–	129 000–534 000	Цена указаны на 2017 год
Julivi	От 35 368	От 102 568	

Данные, приведенные в таблице, позволяют утверждать, что:

– выявлена низкая конкурентоспособность отечественных аналогов с зарубежными в одном ценовом сегменте;

– высокая стоимость одноразового платежа вынуждает брать продукт в кредит или в рассрочку, или использовать не лицензированную версию, особенно высок процент «пиратства» среди частных мастеров и любителей шитья;

– среди отечественных мастеров существует тенденция вынужденного использования нескольких САПР для построения одного изделия, что повышает сложность производства и итоговую стоимость.

Результаты исследования САПР показали необходимость в разработке программы по открытой лицензии (*open source*), доступной бесплатно для широкого круга пользователей. Такой программой может служить создание дополнения (*addon*) к свободно распространяемому (лицензия GPL) 3Д редактору Blender.

На сегодняшний день Blender завоевывает позиции лидера в индустрии 3Д, благодаря наличию физически корректного рендеринга в окне редактирования модели, системы симуляции тканей и жидкостей, простоте освоения, свободному изменению кода под свои нужны, интеграции с языком программирования Python, а также многотысячному сообществу пользователей, среди которых крупные компании (*Nvidia, Netflix, Nasa* и т. д.). Отличитель-

ной особенностью является возможность производить моделирования на основе твердотельных моделей, например, симулировать ткани палатки на металлическом каркасе, обивку салона автомобиля и т. д., что или невозможно, или трудоемко в САПР швейной промышленности.

Наряду с достоинствами программного средства Blender, он не является полноценным САПРом, особенно в области двухмерного создания чертежа. Для решения данной проблемы предлагается интегрировать в него свободный двухмерный САПР, с помощью языка Python.

Примерами таких САПР являются:

– LibreCAD;
– QCAD;
– Simplex, за авторством д. т. н. Волошинова Д. В.

Отвечая на вопрос о стоимости итогового изделия, можно с уверенностью сказать, что использование свободно распространяемого программного обеспечения Blender + двухмерное САПР позволит снизить стоимость изделия и сроки выполнения заказа.

Список используемых источников

1. Гусева М. А., Гетманцева В. В., Андреева Е. Г., Петросова И. А. Параметризация цифровой антропометрической информации для 3D-проектирования швейных изделий // Территория новых возможностей. 2019. № 2. URL: https://cyberleninka.ru/article/n/parametrizatsiya-tsifrovoy-antropometricheskoy-informatsii-dlya-3d-proektirovaniya-shveynyh-izdeliy (дата обращения: 04.12.2019).

2. Василевская Л.В. [и др.] Разработка методики конструирования одежды для собак // Wschodnioeuropejskie Czasopismo Naukowe (East European Scientific Journal). 2016. № 10. С. 99–106

3. Григорьева З. Р., Иванчик Е. А., Горелова А. Е. Разработка методик проектирования одежды на фигуры с нарушениями осанки // Вестник Казанского технологического университета. 2016. № 12. URL: https://cyberleninka.ru/article/n/razrabotka-metodik-proektirovaniya-odezhdy-na-figury-s-narusheniyami-osanki (дата обращения: 05.11.2019).

4. Гусева М. А. [и др.] Параметризация цифровой антропометрической информации для 3D-проектирования швейных изделий // Территория новых возможностей. 2019. № 2. URL: https://cyberleninka.ru/article/n/parametrizatsiya-tsifrovoy-antropometricheskoy-informatsii-dlya-3d-proektirovaniya-shveynyh-izdeliy (дата обращения: 13.11.2019).

5. Гусева М. А. [и др.]Трехмерное сканирование как эрго-инструмент в инклюзивной антропометрии // Сб. науч.х тр. «Эргодизайн как инновационная технология проектирования изделий и предметно-пространственной среды: инклюзивный аспект», Часть 1. – М. : РГУ им. А. Н. Косыгина, 2019. URL: https://kosygin-rgu.ru/filemanag/Uploads/kafedra/hmkitik/2019/Сборник_2019 часть 1.pdf (дата обращения: 24.11.2019).

6. Visual-simulation-based personalized garment block design method for physically disabled people with scoliosis (pdps), Yan Hong [and others] // AUTEX Research Journal, Vol. 18, No 1, March 2018. URL: https://www.researchgate.net/publication/311924431_Visual-Simulation-Based_Personalized_Garment_Block_Design_Method_for_Physically_Disabled_ People_with_Scoliosis_PDPS (дата обращения: 17.12.2019).

7. Саиди Д. Р., Домуладжонова Н. А. Моделирование конструкции одежды по технологии 3Д // Universum: технические науки. 2019. № 1 (58). URL:

https://cyberleninka.ru/article/n/modelirovanie-konstruktsii-odezhdy-po-tehnologii-3d (дата обращения: 06.10.2019).

УДК 004.82
ГРНТИ 20.23.25

ИСПОЛЬЗОВАНИЕ TELEGRAM БОТ ДЛЯ ТЕХНИЧЕСКОЙ СЛУЖБЫ ПОДДЕРЖКИ

Д. В. Волошинов, Е. С. Казначеева, Е. С. Хайбрахманова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время инновации и технологии внедряются во все сферы жизнедеятельности. Идет активное применение новейших систем. Для того, чтобы идти в ногу со временем для большинства сотрудников офисов использование мессенджера на телефоне облегчит связь с отделом технической службы поддержки, для экономии времени и точного описания проблемы.

telegram бот, мессенджер, техническая поддержка.

Проблема грамотного составления запроса или вопроса, относящегося к отделу технической поддержки достаточно распространенная. Большинство сотрудников, как крупных офисных корпораций, так и небольших фирм ежедневно сталкиваются с проблемами на своих компьютерах и офисной технике. Даже простой звонок в отдел к техническим специалистам занимает много времени, причем часто бывает не дозвониться из-за обилия вопросов и занятости сотрудников.

В связи с этим, существует возможность использования в современном мире – актуальных средств связи со множествами функций для упрощения работы. Например, при личном обращении сотрудника в отдел технической поддержки, с просьбой установить офисное программное обеспечение (ПО) надо составить обращение письменное, или на сайте, и ожидать выполнения, в большинстве случаев срок исполнения запроса варьируется от одного до трех дней. Также бывают указаны некорректные данные, которые замедляют процесс решения. Оптимальным решением в таком случае послужит использование онлайн-мессенджера для составления обращения по ремонту.

Система мгновенного обмена сообщениями, мессенджер (англ. *Instant messaging*, IM) – службы мгновенных сообщений для обмена сообщениями в реальном времени через Интернет. Могут передавать текстовые сообщения, звуковые сигналы, изображения, видео.

Telegram бот – это робот-помощник, готовый выполнить любое рутинное занятие, специальный программный код, выполняющий определённые команды пользователя.

Вся переписка с ним ведётся через обычный чат. Пользователь даёт боту команды, которые он готов выполнять круглосуточно. Основная задача бота – это ответить на вопрос пользователя, согласно своей программе. Боты помогают, экономят время и просты в своем управлении. На сегодня роботы Телеграмм могут:

– проводить обучение;

– развлекать и играть;

– работать поисковиками в интернете;

– скачивать текстовую информацию, видео или аудио;

– помогать с напоминанием тех или иных задач;

– участвовать в групповых чатах, допустим, для согласования времени встречи, оптимальной для всех участников;

– комментировать нужные статьи;

– использоваться для управления умным домом и др.

Другими словами, они, как посредники между человеком и многочисленными веб-службами. Их большой плюс – это общая оболочка, внутри приложения Телеграмм находится вся информация, которую люди привыкли искать через поисковые системы Интернета: Яндекс и Гугл. Несомненный плюс в экономии времени за счёт уменьшения личного обращения к специалистам.

Принцип работы онлайн-помощника очень прост. Необходимо найти помощника на телефоне и написать ему текстовое сообщение (команду), после этого поступит ответ через доли секунды. Достоинства такого процесса:

– круглосуточная помощь – поскольку работу бота остановит только авария на сервере, что случается редко;

– удобство использования – большинство команд находится в меню бота, а ответы поступают мгновенно;

– для работы используются ресурсы сторонних серверов, мощность самого устройства не задействована;

– безопасность – боты никак не украдут данные, поскольку для них они скрыты, они работают только с командами из чата;

– установка дополнительных программ не требуется.

Рассмотрим работу онлайн-помощника на примере информирования о погоде в различных городах. Для этого пользователь вводит текст, содержащий фразы «погода» и «название города» (рис. 1):

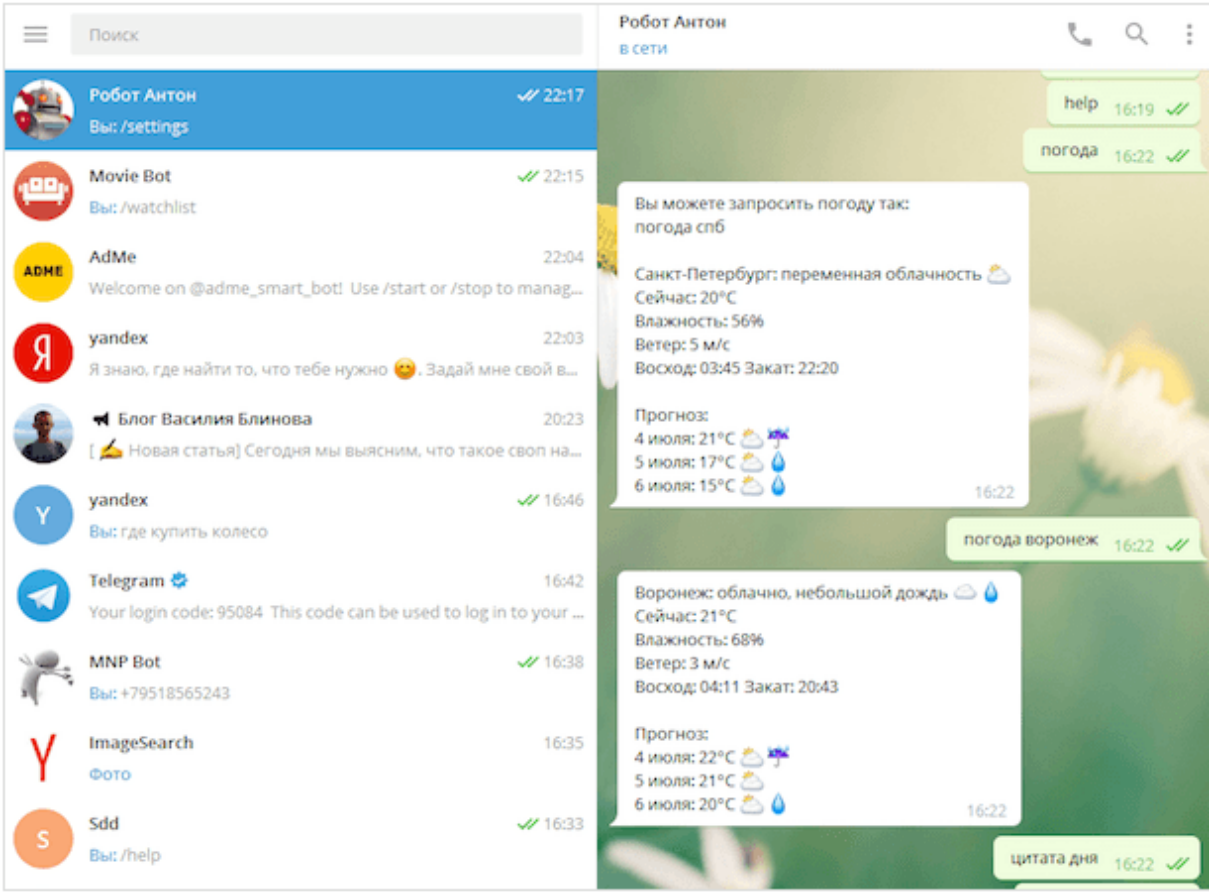


Рис. 1. Пример онлайн-помощника погоды

Для работы помощника со службой технической поддержки запрос будет разделен на следующие категории:

– составление запроса на ремонт техники;
– задать вопрос онлайн-помощнику;
– составление запроса на заправку картриджа;
– составление запроса на установку программного обеспечения;
– задать вопрос специалисту.

Реализация данного процесса осуществляется с помощью следующих этапов [1]:

1. Подготовка базы знаний по всем вопросам и обращениям к онлайн-помощнику.
2. Написание кода.
3. Отладка и тестирование.
4. Запуск процесса.

Рассмотрим третий этап – это написание кода с помощью библиотеки Python и обертку Telegram API [2]. Платформа позволяет писать обработку сообщений в обычных функциях с декораторами, что удобно (рис. 2).

```
@bot.message_handler(commands=['start', 'help'])
def send_welcome(message):
    bot.reply_to(message, "Welcome to Support_Bot!")
```

Рис. 2. Написание кода Python

Так выглядит код, который реагирует на команды "/start", "/help" (рис. 3), а также приветствует новых пользователей бота (при первом открытии бота автоматически отправляется команда "/start").

```
@bot.message_handler(commands=['on'])
def subscribe_chat(message):
    if message.chat.id in team_users:
        bot.reply_to(message, "You are already an operator")
    else:
        user_step[message.chat.id] = TEAM_USER_LOGGING
        bot.reply_to(message, "Enter team secret phrase:")
```

Рис. 3. Код приветствия

После этого происходит описание нестандартных команд, обращение к базе знаний за справочной информацией, дополнение изображениями и запуск помощника.

Используя онлайн-помощник отмечены следующие преимущества:

– в запросе автоматически формируются данные о заявителе;

– техническая поддержка или консультация происходит в прямом режиме;

– простота и удобство.

Список используемых источников

1. Введение в теорию искусственного интеллекта [Электронный ресурс]. URL: http://www.aiportal.ru/articles/introduction

2. Макграт Майк. Программирование Python для начинающих. М. : Изд.-во Эксмо, 2018. 194 с.

УДК 514.144.1; 414.18; 519.685
ГРНТИ 27.21.21

РАЗРАБОТКА АЛГОРИТМИЧЕСКОГО КОМПЛЕКСА ДЛЯ РЕШЕНИЯ ЗАДАЧ КОНСТРУКТИВНОЙ ГЕОМЕТРИИ

Д. В. Волошинов, А. В. Соловьева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена вопросам автоматизированного синтеза конструктивных геометрических моделей, позволяющих осуществлять программирование геометрически-обусловленных задач визуально-графическими средствами. В статье сформулированы требования к системам подобного рода и представлена система геометрического моделирования Симплекс, разрабатываемая авторами настоящей статьи

конструктивное геометрическое моделирование, Симплекс, системы визуального проектирования.

Конструктивное геометрическое моделирование является одним из направлений математической науки, в котором геометрическое построение, выполняемое с помощью простейших геометрических инструментов, рассматривается как некоторый преобразователь (функция), устанавливающий соответствие между объектами, на основе которых выполняется построение, и объектами, составляющих его результат. На протяжении длительной исторической эпохи конструктивная геометрия являлась основным средством решения научных и прикладных задач, связанных с представлением и передачей информации о форме предметов окружающей действительности. Работы великих математиков и геометров, таких как Я. Больяи, Н. А. Лобачевский, М. Клейн, К. А. Андреев [1, 2] и др. позволили рассматривать геометрию не только как науку о представлении формы физических предметов, но и как средство представления качественной информации о явлениях и процессах окружающей действительности в отвлеченно-абстрактном виде. На основе таких представлений стали развиваться средства моделирования, позволяющие осуществлять визуальную интерпретацию сложных многомерных данных [2] и использовать информацию такого рода в виде графиков и номограмм в инженерном деле и научных расчетах.

Бурное развитие компьютерных технологий в конце XX века послужили отправным моментом появления отрицательного отношения к практическому приложению геометрического инструментария как к средству,

не отвечающему требованиям точности и трудоемкости выполнения проектных работ. Появилась тенденция к вытеснению геометрических методов из практики реального проектирования, что привело к почти неограниченному доминированию методов аналитической математики над методами геометрии. Безусловно, сложившаяся ситуация объясняется относительной простотой программирования устройств, основанных на дискретном принципе действия, что согласуется с принципами аналитической ветви математики. Форма и геометрия, оперирующая ее категориями, стала рассматриваться не как инструмент познания, а как конечный пункт проектной деятельности средствами аналитики. Именно с этим обстоятельством связано стремление практически любого исследователя, применяющего геометрию в своих изысканиях, привести полученные с ее помощью результаты в аналитическую форму, допускающую их реализацию на ЭВМ.

Практически единственным примером приложения геометрии к информационным технологиям стали системы подготовки чертежно-графической документации и САПР, предназначенные для нужд машиностроительного производства и имитационного моделирования, так называемых 3D-систем. Говоря об этом, следует особо подчеркнуть, что интерфейс таких систем всегда разрабатывался как инструмент визуально-графического взаимодействия пользователя с системой, что лишний раз подтверждает исключительную важность той роли геометрического представления информации, которую играет геометрическое моделирование имеет при ее синтезе и интерпретации информации о форме и ее восприятии человеком.

Несмотря на серьезные достижения в области автоматизации проектирования системы 3D оказываются практически неспособными решать те задачи, которые могут быть сформулированы средствами конструктивного геометрического моделирования, в особенности тех задач, которые выходят за рамки представления формы в трехмерном физическом пространстве. Более того, те особые условия, которые накладывает природа на форму технических объектов, в частности, на поверхности изделий авиационного машиностроения [4], требуют реализации специальных геометрических преобразований [5], которые в рамках систем твердотельного 3D моделирования неосуществимы из-за концептуальных различий в подходе к проектированию вычислительных ядер этих систем с принципами конструктивного геометрического моделирования.

В связи с вышеизложенным становится актуальной задача разработки систем геометрического моделирования нового вида, которые позволили бы, с одной стороны, решать практически важные задачи с использованием мощного теоретического арсенала геометрической науки, с другой стороны, такие системы должны снять инструментальные ограничения, присущие традиционным способам производства документа, содержащего геометро-

графическую информацию, и ликвидировать необходимость перевода геометрического метода в сугубо аналитическую форму для его представления в виде программы вычислительного устройства [6, 7, 8].

Результатом исследований в обозначенной области является разработка системы конструктивного геометрического моделирования Симплекс, осуществляемая на кафедре ИКД СПбГУТ. Концепция системы полностью соответствует методу конструктивного геометрического моделирования и позволяет решать геометрически обусловленные задачи методами синтетической геометрии.

Разработка системы ведется в соответствии с соблюдением следующих требований:

1. Процесс синтеза геометрической модели является программированием, однако этот процесс не требует написания программы на каком-либо алгоритмическом языке. Программирование осуществляется визуально и неотличимо от действий, выполняемых обычно при традиционном черчении. Тем не менее, результатом такого черчения является программа, преобразующая изменяющиеся исходные данные в выходной результат.

2. От пользователя не требуется знать аналитические интерпретации геометрических операций. Все проектирование осуществляется исходя исключительно из геометрических представлений информации о форме.

3. В системе реализуется аппарат проективной геометрии, то есть команды системы рассчитаны на работу с бесконечно удаленными объектами, что позволяет разрабатывать программы, имеющие универсальный характер.

4. Система реализует аппарат мнимой геометрии [9, 10, 11, 12], что также способствует унификации геометрических алгоритмов и освобождает их от исключительных ситуаций, неизбежно проистекающих в аффинной евклидовой геометрии, на основании которых строятся системы САПР.

5. Система рассчитана на реализацию дискретно-непрерывных конструктивных геометрических моделей, что позволяет ставить и решать задачи, требующие многомерной интерпретации данных.

6. Система позволяет осуществлять логический синтез и анализ команд и данных, которые используются геометрическим процессором системы. Это позволяет разрабатывать автоматически генерируемые геометрические алгоритмы на основе метаправил без непосредственного участия человека и получать геометрические модели и графические документы, которые не могут быть выполнены человеком в силу чрезвычайной трудоемкости и высокой степени сложности. Именно такие алгоритмы возникают при реализации моделей многомерных пространств.

7. Система должна быть способной синтезировать отторгаемые программы, которые можно использовать в других информационных средах

для выполнения вычислительной работы. В настоящее время система Симплекс генерирует эквиваленты внутреннего представления алгоритмов на языках ObjectPascal, MikroPascal, JavaScript, MaxScript. Такие программы могут быть подключены к соответственным средствам разработки и функционировать в этих системах, полностью интерпретируя действия геометрических моделей, реализованных в системе Симплекс визуально-графическим способом.

8. Система служит средством реализации геометрического эксперимента, при которой исследователь сложной геометрической модели может проверять гипотезы, а возможно, и предугадывать способы проведения исследований и изысканий для получения новых научных результатов.

9. Система должна быть простой в использовании. Способ взаимодействия с ней должен сводиться к элементарным действиям, практически неотличимым от традиционных ручных методов работы с геометрической информацией.

10. Система должна быть информационным средством педагогической деятельности, обеспечивающим самые современные технологии представления геометрических знаний и ведения учебного процесса, в том числе в дистанционной форме.

11. Система должна обеспечивать высококачественный уровень документирования геометрической информации, обеспечивающей высокое качество ее полиграфического исполнения и производства научной нотации.

Перечень обозначенных выше требований и проблем удалось решить за счет разработки алгоритмического комплекса конструктивного геометрического моделирования, который в настоящее время насчитывает более 350 геометрических функций, а также за счет разработки среды проектирования, реализующей управление всеми вычислительными процессами и потоками данных в системе.

Список используемых источников

1. Клейн Ф. Неевклидова геометрия. М.-Л. : Объединенное научно-техническое издательство НКТП СССР, 1936. С. 344.

2. Андреев К. А. О геометрических соответствиях в применении к вопросу о построении кривых линий. М. : Университетская типография (М. Катков) на Страстном бульваре, 1879. С. 7.

3. Филиппов П. В. Начертательная геометрия многомерного пространства и ее приложения. Изд. 2-е. М. : ЛЕНАНД, 2016. – 282 с.

4. Котов И. И. Геометрические основы ключевых способов построения поверхностей // Труды ВЗЭИ. М., 1959. Вып. 10. С. 15–36.

5. Иванов Г. С. Конструирование технических поверхностей (математическое моделирование на основе нелинейных преобразований). М. : Машиностроение, 1987.

6. Волошинов Д. В. Геометрическая лаборатория. Закладываем основы // Качество графической подготовки: проблемы, традиции и инновации: материалы VII международной интернет-конференции. Февраль – март 2017 г. Пермь, 2017.

7. Волошинов Д. В. Геометрическая лаборатория. Новый геометрический инструмент // Качество графической подготовки: проблемы, традиции и инновации: материалы VII международной интернет-конференции. Февраль – март 2017 г. Пермь, 2017.

8. Волошинов Д. В. Геометрическая лаборатория. Инструменты ортогональности // Качество графической подготовки: проблемы, традиции и инновации: материалы VII международной интернет-конференции. Февраль – март 2017 г. Пермь, 2017.

9. Пеклич В. А. Высшая начертательная геометрия. М. : Изд-во АСВ, 2000. 344 с.

10. Пеклич В. А. Начертательная геометрия : учебник для вузов. М. : Изд-во АСВ, 1999. 248 с.

11. Пеклич В. А. Мнимая начертательная геометрия : учеб. пособие. М. : Изд-во АСВ, 2007. 104 с.

12. Гирш А. Г. Наглядная мнимая геометрия. М. : Маска, 2008. 200 с.

УДК 004.056.55
ГРНТИ 03.81.43

ИССЛЕДОВАНИЕ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА LSB С ИСПОЛЬЗОВАНИЕМ КЛЮЧЕЙ ДЛЯ ОПРЕДЕЛЕНИЯ ОБЛАСТИ ВСТРАИВАНИЯ ДАННЫХ В ГРАФИЧЕСКИХ КОНТЕЙНЕРАХ

П. А. Волынкин, О. А. Кононюк

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В целях обеспечения конфиденциальности передаваемых данных и защиты авторских прав на цифровые форматы мультимедиа в условиях развитой структуры сетевого обмена данными применяются методы цифровой стеганографии. Наиболее популярным из стеганографических методов является метод замены наименьшего значащего бита ввиду своей низкой вычислительной сложности и высокой полезной нагрузки. В данной статье рассматриваются модификации данного метода с использованием стеганографических ключей для четкого определения или адаптивного выбора областей встраивания информации. В качестве носителя информации определены графические файлы ввиду своей избыточности и широкого распространения.

защита информации, стеганография, графические файлы, НЗБ, секретный ключ.

С развитием цифровых технологий многие типы данных стали подвержены копированию и распространению с нарушением авторских прав, что увеличило потребность в исследовании и развитии цифровой стеганографии, цель которой заключается в сокрытии внутри таких данных информации, подтверждающей права собственности. Информация, подлежащая

сокрытию, называется сообщением. Среда, выступающая в качестве носителя скрываемой информации, называется контейнером (*cover*). В качестве контейнеров чаще выступают цифровые форматы мультимедиа, содержащие избыточные пространства данных, модификация которых не приводит к заметным искажениям контейнеров. Контейнер, содержащий в себе скрытые данные называется стегоконтейнером (*stego object*), не содержащий – пустым контейнером. Использование форматов мультимедиа в качестве контейнеров подразумевает автоматизацию процессов внедрения и извлечения исходных сообщений ввиду эффективной манипуляции данными и выполнения стеганографических алгоритмов современными компьютерами.

На рис. 1 приведена структурная схема типичной стегосистемы. На вход системы поступают секретное сообщение, данные контейнера и дополнительный стеганографический ключ. На основании поступающих данных алгоритм кодирования создает стегоконтейнер, передающийся по каналу связи стегосистемы, где канал передачи информации считается подверженным воздействиям неавторизованного пользователя, обладающего представлением о реализации стеганографической системы, но не имеющем информации о используемом ключе шифрования. Алгоритм декодирования получает на вход стегоконтейнер и стеганографический ключ для извлечения исходного секретного сообщения.

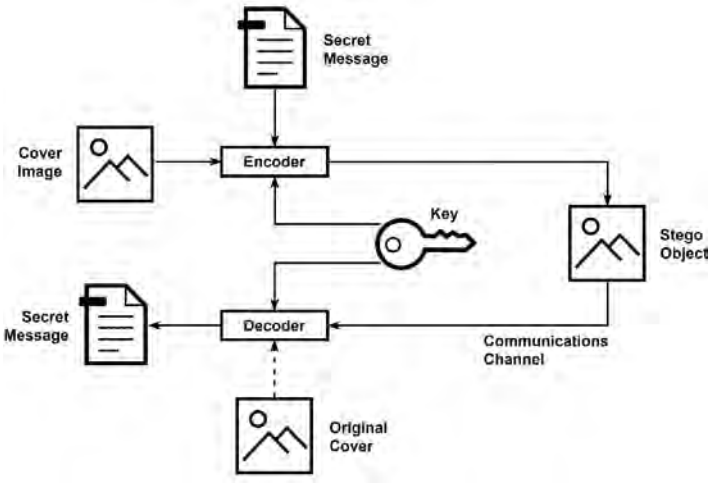


Рис. 1. Структурная схема типичной стегосистемы

Метод замены наименьшего значащего бита (НЗБ) или LSB (*Least Significant Bit*) является наиболее широко используемым стеганографическим методом сокрытия данных в пространственной области, основанном на замене наименьших значащих бит пикселей контейнера значениями потока битов сообщения, поскольку небольшие изменения в цветах пикселей являются незаметными для глаза [1]. Метод LSB обладает большой полезной нагрузкой (12,5 % от объема контейнера в случае замены одного НЗБ

в байте), но имеет низкую надежность, т. к. любые модификации контейнера способны изменить встроенное сообщение. Для повышения надежности и стойкости к стегоанализу метода LSB используются некоторые виды ключей, определяющих области встраивания сообщения.

1. Ключ определяет порядок байта, предназначенного для записи одного бита скрываемого сообщения. В данном варианте ключ преобразуется в двоичную запись, где «1» – выбор байта для записи, «0» – пропуск байта;

2. Ключ определяет разряд младшего значащего бита, где «1» – запись бита сообщения во второй разряд байта контейнера, «0» – в первый разряд;

3. Ключ используется в качестве начального числа генератора псевдослучайных чисел (ГПСЧ), который генерирует случайную последовательность положительных целых чисел n_i. Пиксели контейнера нумеруются как P_j, а биты сообщения скрываются в пикселях $P_{1+n_1}, \dots, P_{1+n_1+\cdots+n_i}$. В случае, если индекс $1 + n_1 + \cdots + n_i$ превышает размер изображения, он будет вычисляться по модулю размера изображения. В результате возможно возникновение коллизий, из-за чего необходимо ведение записи индексов всех раннее модифицированных пикселей. При достижении алгоритмом одного и того же пикселя, генерируется следующее псевдослучайное число, и выбирается другой пиксель для записи бита сообщения;

4. Ключ не используется. Данный вариант прочитывает изображение по сложному маршруту и скрывает один бит данных в каждом прочитанном пикселе. Например, пиксели могут отбираться по кривым Пеано, Гильберта (рис. 2) или Мортона (рис. 3), которые посещают точку квадратного участка единожды;

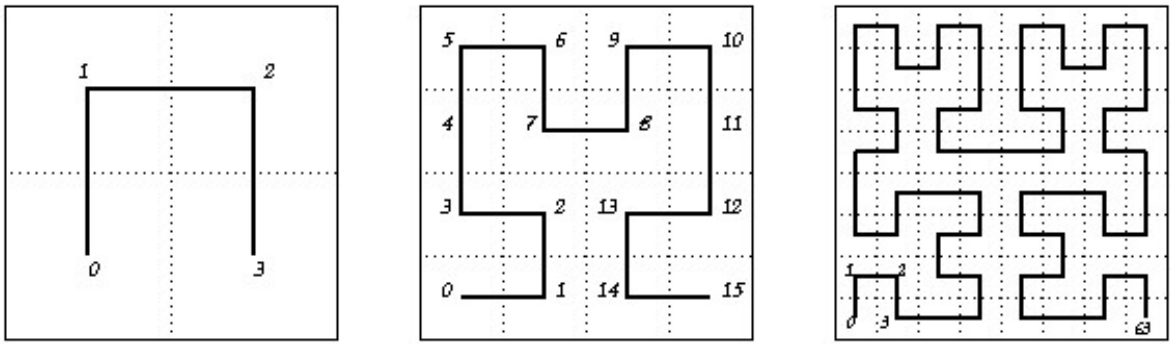


Рис. 2. Кривая Гильберта

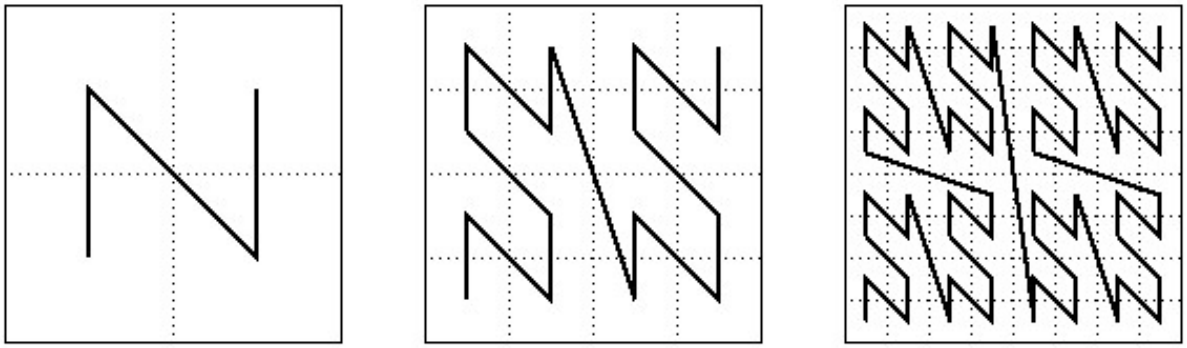


Рис. 3. Кривая Мортона

5. Ключ и защищенная хэш-функция f_K используются для генерации последовательности уникальных адресов пикселей, в которых скрываются биты сообщения. Безопасная хэш-функция обладает свойством: если $z = f_K(x)$, то вычислительно невозможно найти $y \neq x$ такой, что $z = f_K(y)$. При данном использовании ключа предполагается, что в качестве контейнера выступает изображение размера $x * y$, где x – горизонтальное измерение. Ключ K разделен на три части: K_1, K_2, K_3. Для определения номера P и координат пикселя (X, Y), в который будет осуществлена запись i-го бита сообщения, производятся следующие действия:

1) $Y' = i \; div \; x$;
2) $X' = i \; mod \; y$;
3) $Y'' = \left(Y' + f_{K_1}(X')\right) mod \; y$;
4) $X = \left(X' + f_{K_2}(Y'')\right) mod \; x$;
5) $Y = \left(Y'' + f_{K_3}(X)\right) mod \; y$;
6) P = $Y * x + X$.

В каждом действии функция $f_K(i) = H(K°i)$ для каждого параметра K (закрытого ключа) создает различную псевдослучайную перестановку $\{0, \dots, N-1\}$, где N – количество доступных бит для записи (полезная емкость) контейнера. Действия 3 и 4 равномерно распределяют биты скрываемого сообщения в байтах контейнера размерностью $x * y$, а применение 5 действия необходимо для предотвращения атаки на основе открытых текстов [2].

6. Использование операторов Собеля, Прюитта и Кэнни для выделения границ изображения и последующего определения зон вставки данных сообщения [3].

Для файлов форматов BMP и GIF данные сообщения могут быть скрыты как в растровом изображении, так и в палитре, представленной таблицей из 256 строк (256 различных цветов) и трех столбцов (3 байта

для определения трех компонентов цвета). В случае использования палитры запись значений бит скрываемого сообщения производится в НЗБ цветовых компонент палитры. В типичной палитре размером 256*3 можно осуществить запись сообщения в 768 бит (96 байт). Следующий метод модификации палитры предполагает перестановку строк таким образом, чтобы НЗБ строк принимали значения битов скрываемого сообщения. При использовании данного метода в палитре из 256 строк возможна запись около 200 бит информации. В растровом изображении все указатели, ссылавшиеся на переставленную строку должны быть изменены в соответствии с перестановкой.

В случае использования растрового изображения для скрытия данных, изменения НЗБ указателей может сильно исказить контейнер, т. к. смежные строки палитры могут содержать разные спецификации цвета. Решение данной проблемы достигается за счет сортировки палитры таким образом, чтобы смежные строки определяли похожие цвета. Сортировка записей компонент RGB цветов происходит в соответствии с их евклидовой нормой:

$$N = \sqrt{R^2 + G^2 + B^2}.$$

Описанные способы применения ключей в стеганографическом методе LSB затрудняют получение скрытой информацией неавторизованным лицом, но являются малоэффективными для противодействия методам стегоанализа, что определяет потребность разработки адаптивных методов LSB стеганографии.

Список используемых источников

1. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. М. : МК-Пресс, 2006. 286 с.

2. Aura T. Practical invisibility in digital communication. Lecture Notes in Computer Science, 1996. Vol. 1174, Springer-Verlag. PP. 265–278.

3. Chethan K. S., Sinchana G. S., Nataraj K. R. Choodarathnakara A. L. Analysis of Image Quality using Sobel Filter // IEEE Third International Conference on Inventive Systems and Control (ICISC). 2019. PP. 526–531.

УДК 004.896
ГРНТИ 20.19.29

АЛГОРИТМ ВОССТАНОВЛЕНИЯ ПРОПУСКОВ В НОМИНАТИВНЫХ СОЦИОЛОГИЧЕСКИХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ МЕТОДА МНОЖЕСТВЕННОЙ ИМПУТАЦИИ

А. А. Воробьев, А. А. Воронецкий

Академия ФСО России

В статье рассматриваются результаты анализа различных видов пропусков, возникающих в ходе проведения социологических опросов и используемых на практике актуальных методов для восстановления социологических данных, измеряемых в номинативных шкалах. Основным результатом анализа методов стал выбор метода множественной импутации. Для повышения возможностей данного метода использовался подход по переводу переменных, измеряемых в номинальной и порядковых шкалах в фиктивные с использованием дихотомизации.

Для решения задачи выбора независимых фиктивных переменных, обеспечивающих повышение качества восстановления (точности прогнозирования), были проведены серии экспериментов и сформулированы на их основе правила, которые в дальнейшем были реализованы в алгоритме нахождения пропущенных значений в социологических данных на основе метода множественной импутации.

социологический опрос, восстановление неполных данных, неопределившиеся респонденты, метод множественной импутации, статистический эксперимент, алгоритм.

С целью получения актуальной информации о состоянии развития общества проводятся социологические опросы. Сбор сведений производится путем взаимодействия интервьюеров с определенной совокупностью опрашиваемых респондентов. Достоверность информации, полученной таким образом, зависит от многих факторов, например, от квалификации интервьюеров, репрезентативности выборки, процента неопределившихся респондентов и др.

В работе исследуется возможность снижения влияния одного из факторов на качество социологических исследований, а именно большой процент неопределившихся респондентов, которые считаются пропусками в социологических данных.

Известно, что наличие пропусков в социологических данных приводят к снижению точности прогнозирования. Так в [1] описаны проблемы использования неполных данных в социологических исследованиях.

Исследование возможностей по восстановлению неполных данных с использованием метода мультиномиальной логистической регрессии (МЛР) представлено в [2] и было начальным этапом работы. Однако, как показали дальнейшие исследования, с учетом известных ограничений метода МЛР и проведенных экспериментов, было принято решение об исследовании возможностей альтернативного метода – множественной импутации.

В исследовании был применен известный подход к переводу переменных, измеряемых в номинальных и порядковых шкалах, в фиктивные переменные, с использованием дихотомизации. По результатам экспериментов подтвердилась гипотеза о влиянии стандартизированных остатков на точность восстановления данных. Результаты эксперимента представлены в [3].

В результате исследования был предложен алгоритм по восстановлению социологических данных, содержащих случайные пропуски, с помощью метода множественной импутации (рис.).

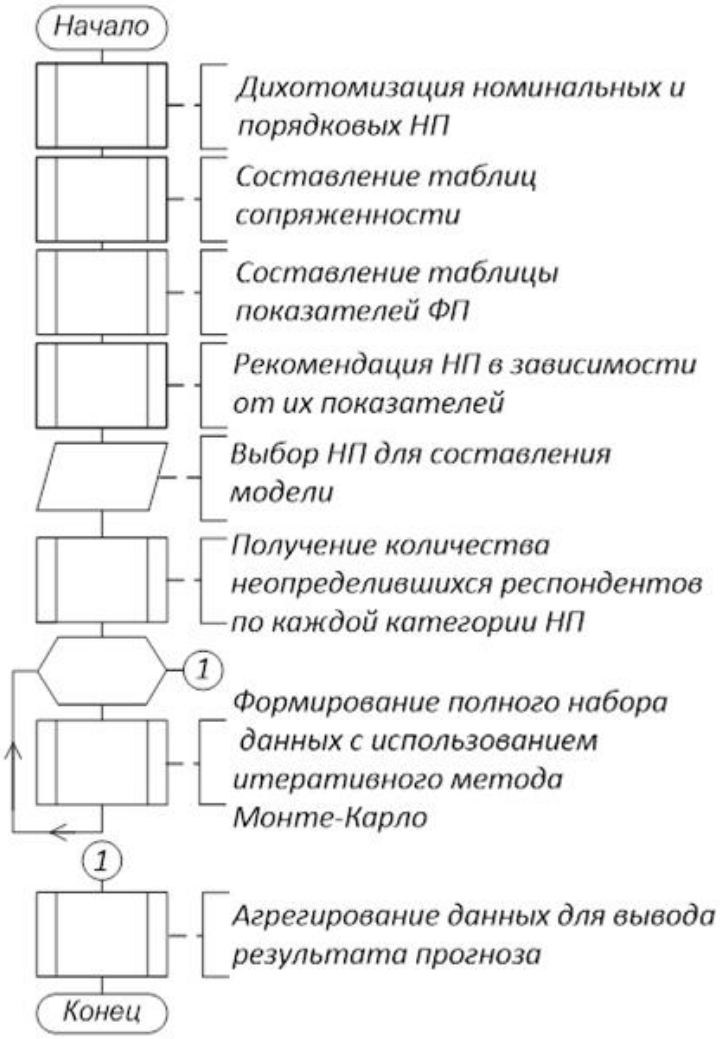


Рис. Алгоритм нахождения пропущенных значений в социологических данных на основе метода множественной импутации

Исходными данными для работы алгоритма является таблица, в которой столбец содержит значения определенной переменной (в случае социологического опроса – ответы на один вопрос анкеты). Строка – наблюдение в неполных данных (ответы на все вопросы одного респондента). После ввода исходных данных необходимо выбрать зависимую переменную, прогноз которой необходимо получить вследствие перераспределения неопределившихся респондентов. Далее производится обработка данных в виде дихотомизации независимых переменных и составления таблиц сопряженности полученных фиктивных переменных с зависимой переменной. Следующим этапом является расчет описанных в эксперименте показателей независимых переменных, на основании которых формируется выбор независимых переменных аналитик в модели в соответствии со следующими правилами:

– использование независимых переменных в роли предикторов в модели предлагается в зависимости от двух показателей КСО и СЗСО;

– на основе восстановления различных данных социологических исследований эмпирическим путем было выявлено, что КСО независимой переменной должен быть 30–35 % от максимального значения, встречаемого среди всех переменных в данных, а СЗСО равен 48–52 %;

– если независимых переменных недостаточно в заданных интервалах значений, интервалы поочередно расширяются, до тех пор, пока не будет найдено нужное количество независимых переменных.

Формируется рассчитанное количество полных наборов данных с импутированными значениями, которые сформированы с использованием итеративного метода Монте-Карло. Результаты прогноза зависимой переменной, а также результаты частотного анализа импутированных значений формируются автоматически после агрегирования полученных на предыдущем этапе полных наборов данных. Предложенный алгоритм реализован в программе для ЭВМ [4].

По результатам экспериментов подтвердилась эффективность перевода независимых номинальных и порядковых переменных в фиктивные переменные при прогнозе на неполных данных, содержащих случайные пропуски. При работе с данным видом пропусков целесообразно использовать метод МИ, так как он позволяет использовать большое количество независимых переменных в модели без затрачивания большого количества вычислительных ресурсов. Также вследствие проблематичности использования теста хи-квадрат Пирсона на неполных данных в работе статистическую значимость независимых переменных предлагается оценивать с помощью стандартизированных остатков таблицы сопряженности зависимой и независимой переменной.

Найдены эмпирически рекомендуемые значения показателей независимых переменных на конкретных социологических данных. Предлагаемый

алгоритм и программу восстановления пропущенных значений в социологических данных на основе метода множественной импутации необходимо апробировать на других социологических данных.

Список используемых источников

1. Зангиева И. К. Проблема пропусков в социологических данных: смысл и подходы к решению // Социология: 4М. 2011. № 33 С. 28–56.

2. Афанасьев В. В., Благий В. А., Воробьев А. А. Алгоритм перераспределения неопределившихся респондентов на основе мультиномиальной логистической регрессии // Вестник Евразийской науки. 2019. № 3. URL: https://esj.today/PDF/30ITVN319.pdf

3. Vorobiev A. A., Voroneckiy A. A., Krut` O. V., Kladova E. A., Karmazina N. K Research of possibilities of the multiple imputation method for redistributing uncertain respondents // Modern informatization problems in economics and safety (MIP-2020'ES) : Proceeding of the XXVth International Open Science Conference (Yelm, WA, USA, January 2020) / Editor in Chief Dr. Sci., Prof. O. Ja. Kravets – Yelm, WA, USA: Science Book Publishing House, 2020. PP. 77–82. ISBN 978-1-62174-129-9.

4. Воробьев А. А., Макеев С. М., Воронецкий А. А. Программный модуль нахождения пропущенных значений в социологических данных на основе метода множественной импутации. Свидетельство о регистрации программы для ЭВМ RU 2020610508, 15.01.2020. Заявка № 2019666655 от 18.12.2019.

УДК 004.056.5
ГРНТИ 81.93.29

ОСОБЕННОСТИ И ПОКАЗАТЕЛИ КАЧЕСТВА УСТРОЙСТВ ВВОДА ИДЕНТИФИКАЦИОННЫХ ПРИЗНАКОВ КАК СОВРЕМЕННЫХ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ КОНТРОЛЯ ДОСТУПА К ОБЪЕКТАМ ИНФРАСТРУКТУРЫ

Д. М. Воронцов, Н. В. Михайличенко, И. Б. Паращук

Военная академия связи

Рассматриваются результаты анализа особенностей устройств ввода и считывания идентификационных признаков, предназначенных для контроля доступа к объектам информационной инфраструктуры, к элементам и ресурсам информационных систем. Предложен вариант формулировки показателей качества устройств такого класса, ориентированных на возможность их количественного оценивания в интересах поддержки принятия решений по оптимальному выбору конкретных изделий для реальных задач контроля доступа.

устройство ввода идентификационных признаков, контроль доступа, показатель качества, несанкционированный доступ, объект информационной инфраструктуры.

Совершенствование существующих и создание новых программно-аппаратных средств (ПАС) контроля доступа (КД) к критически важным объектам информационной инфраструктуры, а также к автоматизированным рабочим местам современных вычислительных, информационных и телекоммуникационных систем и сетей развивается по нескольким эволюционно-технологическим маршрутам [1].

Разрабатываются и модифицируются средства КД в составе операционных систем. Они призваны осуществлять идентификацию и аутентификацию пользователей, разграничивать их доступ к информационным и аппаратным ресурсам, реализовывать динамический мониторинг (наблюдение), оперативный аудит, анализ целостности данных на объектах информационной инфраструктуры (ОИИ), на автоматизированных рабочих местах телекоммуникационных сетей и в базах (системах хранения) данных. Непрерывно развиваются механизмы защиты информации, которые встраиваются в операционную систему на ОИИ, совершенствуются механизмы и алгоритмы взаимодействия с внешними носителями, средства тестирования программ и аппаратуры защиты, средства маркировки кода. Кроме того, изучаются новые и модифицируются существующие компоненты общего программного обеспечения (ПО) и функционального ПО, например, такие, как модули дополнительной аутентификации, средства взаимодействия с ядром системы защиты информации (СЗИ) и модули разграничения доступа на ОИИ.

Важным эволюционно-технологическим путем развития остается создание и внедрение внешних средства КД, программно-аппаратных модулей КД к внешним носителям, модулей защиты доступа к внутренним техническим элементам информационной инфраструктуры, а также средств доверенной загрузки и устройств ввода идентификационных признаков (УВИП) пользователей на ОИИ [2].

Появление в информационном пространстве новых угроз, способных нанести существенный, а иногда, и непоправимый ущерб информационным ресурсам ОИИ, обуславливает актуальность этого эволюционно-технологического и научно-практического направления. Возникает угроза нарушения баланса, поскольку ранее считалось, что при обеспечении должного контроля физического доступа к системным блокам компьютеров, серверов и хранилищ, а также при правильной эксплуатации систем доверенной загрузки, защищаемые данные находились в безопасности.

Все это предопределяет важность и своевременность рассмотрения особенностей современных УВИП – этих относительно новых программно-аппаратных средств КД к ОИИ, актуальность формулировки и анализа по-

казателей качества этих устройств с целью обоснования оптимального выбора лучших из них. При этом принято считать, что УВИП находят все более широкое применение в качестве систем сбора и обработки информации, как интегрированные системы безопасности, предназначенные для ввода запоминаемого кода, ввода биометрической информации и считывания кодовой информации с идентификаторов. В состав УВИП обычно входят считыватели и идентификаторы. Считыватель – устройство в составе УВИП, предназначенное для считывания (ввода) идентификационных признаков, а идентификатор (носитель идентификационного признака) – уникальный признак субъекта или объекта доступа. В качестве идентификатора может использоваться запоминаемый код, биометрический признак или вещественный код. Идентификатор, использующий вещественный код – предмет, в который занесен идентификационный признак в виде кодовой информации (жетоны, карты, электронные ключи, брелоки, браслеты и т. д.). Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности) реализуется в рамках процедуры аутентификации [3]. Идентификация субъекта доступа представляяет собой его распознавание по присущему или присвоенному только данному субъекту идентификационному признаку. За реализацию данных процедур идентификации и аутентификации отвечают устройства, которые мы привыкли называть УВИП.

Один из подходов к классификации УВИП определяет ключевой способ считывания идентификационных признаков (ИП), поэтому различают устройства с ручным вводом, контактные, дистанционные (бесконтактные) и комбинированные. Ручной ввод ИП подразумевает их контактное считывание, непосредственный контакт идентификатора и считывателя, он осуществляется пользователем ОИИ либо нажатием кнопок (клавиш), либо поворотом регуляторов и переключателей или другим подобным способом. В отличие от этого, не требует непосредственного контакта идентификатора и считывателя дистанционный (бесконтактный) способ считывания. Считывание ИП происходит либо при поднесении идентификатора на определенное расстояние к считывателю (радиочастотный метод), либо при внесении идентификатора в поле сканирования считывающего устройства (инфракрасный метод). Сочетание разных способов считывания практикуется при комбинированном способе ввода ИП.

Основными особенностями КД на основе УВИП являются уникальные операции и их очередность. Она реализуется путем последовательных: аппаратной идентификации и аутентификации пользователя ОИИ на основе УВИП; аутентификации; шифрования и хранения конфиденциальных данных. К конфиденциальным данным относятся сами ИП, ключи и контрольные суммы. Яркими особенностями обладают УВИП, основанные на контроле и анализе биометрических ИП.

Сущность биометрической идентификации и аутентификации – считывание и сравнение предъявляемого биометрического признака пользователя ОИИ (отпечатка пальцев, рисунка сетчатки и радужной оболочки глаза, термограммы и формы лица, особенностей речи, геометрии руки, узора, кровеносных сосудов ладони человека и т. д.) с имеющимся образцом (эталоном). Биометрические УВИП для ОИИ могут быть бесконтактными (дистанционными) и контактными, а тот факт, что биометрия позволяет идентифицировать человека, а не устройство, определяет достаточно высокий уровень защиты.

Например, очень популярны сканеры (считыватели) отпечатков пальцев, они обычно реализуются в виде подключаемых к одному из портов компьютера отдельных устройств. Иногда они встраиваются в корпуса мониторов на рабочих местах ОИИ, в компьютерные мыши или клавиатуры. Их популярность обусловлена не только тем, что при сканировании этот способ не вызывает дискомфорта у пользователя, но и тем фактом, что уже много лет дактилоскопический отпечаток пальца считается одним из наиболее устойчивых идентификационных признаков (не меняется со временем, при травме пальца весь естественный папиллярный узор полностью восстанавливается).

Самыми популярными в использовании на различных ОИИ являются такие УВИП, как биометрические замки. Это связано с тем, что, в связи с большим разнообразием изделий определенным объектам или службам можно подобрать рациональное устройство такого типа или комбинацию устройств, соответствующих показателю цена-качество. Примером могут служить замки компании Samsung: замок H-GANG и замок FL1000.

Например, врезной биометрический замок Samsung SHS-P718 обладает высоким уровнем безопасности и имеет мировое признание. Основным достоинством является его универсальность, так как имеет несколько вариантов способов открытия и поддается модернизации. Способы открытия: по паролю, по отпечатку пальца, по карте, с помощью пульта.

Возможность двойной аутентификации позволяет увеличить уровень безопасности. Так же одной из особенностей является то, что данное устройство может работать в результате аварийного отключения электроэнергии, так как имеет собственный источник питания со сроком службы на 3500 открываний. Недостатки – малые диапазоны рабочей температуры и влажности, что ограничивает его использование вне помещения.

Второй пример – накладной биометрический замок H-GANG GUARDIAN TR811, он является упрощенным аналогом модели SHS-P718. Главное различие устройств в том, что данный замок имеет лишь два способа открытия: по отпечатку пальца и по паролю. Также отсутствует двойная аутентификация, но все это компенсируется значительно сниженной

стоимостью. Недостатки диапазонов рабочей температуры и допустимой влажности практически не отличаются от диапазонов предыдущей модели.

Существует и применяется на ОИИ автономный биометрический замок FL1000, который значительно отличается по своим возможностям и характеристикам от вышеперечисленных изделий. Способы открытия: по ИП лица, по паролю, механическим ключом. Есть возможность двойной аутентификации, но главной особенностью является способность к фотографированию при попытке неавторизированного прохода. Устройство может сохранить до шести фотографий, отснятых автоматически при попытках прохода с не пройденной авторизацией. Работает автономно, без питания от сети, что расширяет круг применения данного устройства на различных объектах. На случай проблем с питанием от основного источника питания, есть запасная батарея. Преимущество – может работать при любой влажности и более высоких температурах, но очень уязвим к низким температурам. Вместе с тем, из-за медленного темпа работы, ограничения условий применения и уровня цен, при эксплуатации устройств такого типа приходится расплачиваться снижением пропускной способности. Выбор того или иного УВИП для конкретного ОИИ должен быть основан на значениях показателей, характеризующих качество устройств такого класса. Под показателем качества принято понимать количественную характеристику одного или нескольких свойств этих ПАС КД. При этом количественная характеристика свойств ПАС КД рассматривается применительно к определенным условиям их создания и эксплуатации.

К ключевым свойствам, характеризующим качество УВИП для КД на ОИИ, на наш взгляд, можно отнести [2]: уровень защиты УВИП; производительность УВИП; надежность УВИП; устойчивость УВИП; эргономичность УВИП; затраты (ресурсопотребление) на установку и эксплуатацию УВИП. К показателям качества, количественно характеризующим эти особенности и свойства можно отнести конкретные параметры (вариант).

С позиции анализа уровня защиты, обеспечиваемого УВИП: количество способов открытия УВИП; количество контролируемых и анализируемых ИП; уровень (глубина анализа ИП) идентификации и аутентификации должностных лиц и пользователей ОИИ; уровень проверки целостности ИП пользователя ОИИ. С позиции контроля производительности УВИП: интенсивность обработки ИП; время реакции УВИП на попытку несанкционированного доступа (НСД); время задержки реакции УВИП на попытку НСД. С позиции точки зрения контроля надежности УВИП: время безотказной работы УВИП; время замены (без настройки) УВИП в случае выхода из строя. С позиции контроля устойчивости УВИП: время восстановления УВИП после пограничных сбоев; количество видов воздействия, которым может противостоять данное устройство. Для анализа эргономичности УВИП можно

использовать: время доступа пользователя к рабочему месту ОИИ при применении УВИП; время, необходимое на полную настройку одного комплекта УВИП и другие.

Таким образом, рассмотрены особенности и показатели качества устройств ввода идентификационных признаков как современных программно-аппаратных средств контроля доступа к объектам информационной инфраструктуры. Важно, что существующие типы таких устройств предназначены каждый для конкретных целей и для определенных уровней защищаемых элементов ОИИ, их эксплуатация должна осуществляться комплексно, с учетом уровня существующих угроз [4]. Особенности архитектуры и алгоритмов применения устройств ввода идентификационных признаков обуславливают ряд разнообразных свойств, численно характеризуемых показателями качества защиты информации. Именно поэтому выбор УВИП должен осуществляться с учетом значений их показателей качества, которые предложены в данной статье.

Список используемых источников

1. Васильков А. В., Васильков А. А., Васильков И. А. Информационные системы и их безопасность : учебное пособие. М. : Форум, 2011. 528 с.

2. Паращук И. Б., Воронцов Д. М., Михайличенко Н. В. Актуальные вопросы защиты информации на центрах обработки данных с использованием систем доверенной загрузки и устройств ввода идентификационных признаков // Информационная безопасность регионов России (ИБРР-2019). XI Санкт-Петербургская Межрегиональная конференция. Материалы конференции. СПб. : СПОИСУ, 2019. 596 с. С. 219–221.

3. Мартынова Л. Е., Умницын М. Ю., Назарова К. Е. и др. Исследование и сравнительный анализ методов аутентификации // Молодой ученый. 2016. № 19. С. 90–93.

4. Авраменко В. С., Бобрешов-Шишов Д. И., Беденков В. Н., Маликов А. В. Определение актуальных угроз безопасности информации в инфокоммуникационных системах на основе аппарата нечеткой логики // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). VI Международная научно-техническая и научно-методическая конференция: сб. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 3. С. 13–18.

УДК 004.58
ГРНТИ 20.51.23

ТЕРМИНОЛОГИЧЕСКИЙ БАЗИС ОЦЕНКИ ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСОВ: ОБЗОР СТАНДАРТОВ

А. В. Вострых

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается проблема измерения качества пользовательских интерфейсов программных продуктов, с помощью метрик и понятий, используемых в стандартах. Проведён сравнительный анализ существующих методических указаний и нормативно-технической документации, в том числе международных стандартов, с фиксацией недостатков и неточностей при определении понятий и критериев оценки пользовательских интерфейсов.

пользовательский интерфейс, пригодность использования, стандарты, термины и определения, опыт пользователя, параметры оценки интерфейсов.

Интерфейс является средством взаимодействия человека с прикладным программным обеспечением, поэтому от качества пользовательского графического интерфейса (ГПИ) в значительной степени зависит эффективность этого взаимодействия. Существующие в настоящее время подходы и концепции проектирования взаимодействия, а также оценки ГПИ имеют общие недостатки, выражающиеся в отсутствии формализации критериев оптимальности интерфейсов и их описания как объекта математического моделирования [1, 2].

Проведённый анализ настоящей статьи показал, что сложность формализации известных на сегодняшний день подходов оценки ГПИ отчасти заключается в неясном изъяснении и представлении характеристик качества программных продуктов и их интерфейсов в существующих стандартах [3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16].

Используемые для идентификации характеристик качества ГПИ в анализируемых стандартах термины и понятия имеют ряд серьёзных недостатков:

– одни и те же понятие имеют различное смысловое наполнение;

– в состав идентичных понятий входят различные составляющие, даже в стандартах, реализующих эти понятия в смежных областях;

– идентичные по написанию понятия и термины могут использоваться для описания сущностей из различных научных областей.

Проблема предстаёт в явном виде даже при поверхностном рассмотрении понятийной структуры характеристик качества ГПИ, а именно основополагающего понятия, призванного объединить все существующие характеристики качества в одном термине.

В настоящее время в русскоязычной научной литературе и отечественных стандартах широко используется понятие «юзабилити» (от англ. *Usability*) заимствованное из зарубежных источников. На данный момент в мировом научном сообществе понятие является устаревшим, так как международные стандарты уже продолжительное время используют более объёмное и конкретизированное понятие «опыт пользователя» или «опыт взаимодействия» (англ. *User eXperience*) [17].

Обратимся к рассмотрению действующих стандартов из области оценки и реализации программного обеспечения и его ГПИ [3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] на предмет проверки смысловой и содержательной частей понятия «юзабилити».

Так в стандартах [7, 9, 10, 14, 11, 15] понятие «юзабилити», определяемые как «пригодность использования» и является свойством системы, которое характеризуется тремя показателями: результативность, эффективность и удовлетворенность.

В ГОСТ Р ИСО 9241-11-2010 [11] помимо стандартного определения «юзабилити» идентичного [7, 9, 10, 14, 15], в разделе 4 «Обоснование и полезность используемого подхода» сказано, что «юзабилити» зависит также от оценки производительность труда, условиях использования и удовлетворенности пользователей. В разделе 5 «Установление и измерение пригодности использования» сказано, что для оценки юзабилити, необходимо установить цели и выделить из результативности, эффективности и удовлетворенности пользователя, а также характеристик условий использования, измеряемые и поддающиеся проверке подкомпоненты (задачи, оборудование, среда, пользователь). В приложении «D» п. 2 «Анализ процесса взаимодействия» сказано, что юзабилити зависит от свойств программы, таких как «функциональность», «надежность» и «компьютерная эффективность».

В стандартах [7, 8] понятие юзабилити включает в себя эмоциональные и эстетические аспекты.

ГОСТ Р ИСО/МЭК [12] определяет «юзабилити» как «практичность», которая является атрибутом программного обеспечения, относящимся к его возможности восстанавливать уровень качества функционирования после повреждений. Понятие «пригодность» использованная в стандартах [7, 9, 10, 14, 15] для определения «юзабилити», в данном стандарте является атрибутом оценки программного обеспечения, относящимся к наличию и соответствию набора функций конкретным задачам.

ГОСТ 28806-90 [13] определяет «юзабилити» как «удобство использования» программы и ГПИ, определяемое усилиями, необходимыми для её использования.

ГОСТ Р ИСО/МЭК [16] также, как и стандарт [13] определяется «юзабилити» как «удобство использования», но использует понятие «степень использования» вместо «усилий пользователя». Также в определение «юзабилити» включены эффективность, результативность и удовлетворенность, как основные составляющие понятия.

Несмотря на то, что понятие «юзабилити» считается «родительским» для остальных характеристик качества человеко-ориентированных ГПИ [17, 18, 19, 20, 21], в стандартах [6, 7, 8, 9, 10] оно входит в состав понятия «доступность».

В свою очередь, например, в ПНСТ 169-2016 [10] «доступность» является составляющей понятия «человеко-ориентированное качество».

Таким образом, нарушается принцип единства связей и подчинённости в терминологической иерархии характеристик качества ГПИ используемых в стандартах [3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16].

В некоторых стандартах, например, серии ГОСТ Р ИСО 14915 [3, 4, 5] понятие «юзабилити» не используется вообще, даже в форме «пригодность использования» и «удобства использования», но его составляющие: «результативность», «эффективность» и «удовлетворенность» употребляются без привязки к основному понятию, употребляясь в контексте эргономических требований. Помимо понятия «юзабилити» и его составляющих: «результативность», «эффективность» и «удовлетворенность» в стандартах [3, 4, 5] используются следующие характеристики качества: информативность, устойчивость к ошибкам, пригодность для изучения, безопасность работы системы, пригодность для выполнения производственного задания, управляемость (контролируемость), соответствие ожиданиям пользователей, пригодность для обучения, пригодность к индивидуализации, пригодность для обмена информацией, привлекательность, пригодность для восприятия и понимания. Данные понятия не имеют чёткой сформированной структуры и зависимостей между собой, в стандартах [3, 4, 5] они представлены как самостоятельные характеристики, дополняющие стандарт [6].

Серия стандартов [6, 7, 8, 9] и некоторые отдельные стандарты [10, 11, 14] включают в себя некоторые характеристики качества программ и их ГПИ, используемые в [3, 4, 5], а также дополнительные: факторы окружающей среды (в которые входят физическая, социальная и техническая среды и риск использования (табл. 1). Для этих стандартов также характерно отсутствие какой-либо понятийной структуры и иерархии, как и в [3, 4, 5].

Наиболее «контрастно» от остальных стандартов по форме представления информации отличаются ГОСТ Р ИСО/МЭК 9126-93 [12], ГОСТ 28806-

90 [13] и ГОСТ Р ИСО/МЭК 25010-2015 [16]. Данные стандарты имеют чёткую структуру [12, 13] и разделение по направлениям [12, 13, 16]. Представляется возможным провести сравнительный анализ только ГОСТ Р ИСО/МЭК 9126-93 [12] и ГОСТ 28806-90 [13], так как ГОСТ Р ИСО/МЭК 25010-2015 [16] представляет собой многоуровневую модель оценки программных продуктов.

Несмотря на различия в наименовании характеристик в стандартах [12, 13] их смысловые наполнения эквивалентны. Основное отличие между ГОСТ Р ИСО/МЭК 9126-93 [12] и ГОСТ 28806-90 [13] заключается в численном преимуществе [12] на одну характеристику в свойстве «Мобильность» – пункт «соответствие».

В тексте ГОСТ Р ИСО/МЭК 25010-2015 [16] по каким-то причинам отсутствует представление структуры 40 понятий, входящих в состав многоуровневой модели оценки качества программ (представлен список в виде таблицы в пункте 4.2 «Термины к модели качества продукта» таблица 4), поэтому крайне сложно представить модель реализации данной структуры и отношения связей между характеристиками. В Приложении А, таблица А.1 стандарта [16] представлено неоднозначное сравнение характеристик и подхарактеристик настоящего стандарта со стандартом [12] в виде таблицы, некоторые из указанных характеристик стандарта [12] в данной таблице не нашли подтверждения в тексте оригинального документа. Это может быть связанно с выявленной раннее проблемой, различного смыслового «обрамления» одних и тех же понятий.

Сопоставим значения понятий и параметров рассмотренных стандартов [3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] в таблице.

ТАБЛИЦА. Показатели качества по стандартам [3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]

[3, 4, 5]	[6, 7, 8, 9, 11, 14, 15]	[12, 13]	[16]
–	Доступность Пригодность использования результативность эффективность удовлетворенность	–	Доступность
–	Риск использования	–	Защищенность от ошибки пользователя
Информативность	Информативность	–	
Управляемость (Контролируемость)	Управляемость (Контролируемость)	–	Управляемость
Соответствие ожиданиям	Соответствие ожиданиям	Практичность	Интероперабельность

[3, 4, 5]	[6, 7, 8, 9, 11, 14, 15]	[12, 13]	[16]
пользователей Пригодность для изучения Пригодность для индивидуализации Пригодность для восприятия и понимания	пользователей Пригодность для обучения Пригодность для индивидуализации	Понятность	Определимость пригодности
		Обучаемость	Изучаемость
		Простота использования	Удобство использования
Устойчивость к ошибкам	Устойчивость к ошибкам	Надежность	Отказоустойчивость
		Стабильность	Надежность
		Устойчивость к ошибке	Защищенность
		Восстанавливаемость	Восстанавливаемость
		–	Конфиденциальность
Привлекательность	–	–	Эстетика пользовательского интерфейса
–	–	Функциональность пригодность	Функциональная пригодность
–	–	Правильность	Функциональная корректность
–	–	Комплексируемость	Совместимость
–	–	Согласованность	Функциональная полнота
–	–	Защищенность	Завершенность
–	–	–	Функциональная целесообразность
–	–	Эффективность	Уровень производительности
–	–	Времяемкость	Временные характеристики
–	–	Ресурсоемкость	Использование ресурсов
–	–	Сопровождаемость	Сопровождаемость
–	–	Анализируемость	Анализируемость
–	–	Изменяемость	Модифицируемость
–	–	Устойчивость	–
–	–	Тестируемость	Тестируемость

[3, 4, 5]	[6, 7, 8, 9, 11, 14, 15]	[12, 13]	[16]
–	–	–	Модульность
–	–	–	Возможность многократного использования
–	–	Мобильность	Переносимость
		Адаптируемость	Адаптируемость
–	–	Простота внедрения	Устанавливаемость
–	–	Соответствие	Готовность
–	–	Взаимозаменяе-мость	Взаимозаменяе-мость
–	–	–	Сосуществование
–	–	–	Целостность
–	–	–	Неподдельность
–	–	–	Отслеживаемость
–	–	–	Подлинность

Результаты проведенного анализа позволяют сделать некоторые частные выводы:

– в стандартах и некоторых сериях стандартов отдельные понятия совпадают как по обозначению, так и смысловому наполнению, другие же термины не находят своих аналогов или входят в состав различных групп оценок качества;

– отчётливо прослеживается использование псевдосинонимов характеристик качества, что затрудняет восприятие информации (например, «пригодность для изучения», «пригодность для обучения», «обучаемость», «изучаемость» и т. д.);

– в существующих стандартах недостаточно (а то и вовсе не) учитываются психологические особенности современного пользователя [19];

– только в стандартах [12, 13] понятия гармонично сгруппированы по подгруппам, в остальных [3, 4, 5, 6, 7, 8, 9, 10, 11, 14, 15, 16] они рассредоточены по всему тексту со ссылками на зависимые стандарты из одной области использования. Например, стандарт [10] расширяет список параметров стандарта [9]. Такие манипуляций приводят к неточностям в стандартах и явным ошибкам: в стандарте [3] в п. 5.2.1 «Общие положения» сказано, что мультимедиа-приложения должны быть разработаны в соответствии с семью принципами проектирования диалога, одним из которых является «пригодность для изучения», согласно стандарту [6]. В п. 5.2.3 стандарта [3] вводятся дополнительные принципы, которые относятся к мультимедиа-приложениям, их четыре и одним из них также,

как и в основных является «пригодность для изучения». Ни в одном из стандартов [3, 6] не приводится какое-либо пояснение по данному факту явной тавтологии.

Все выявленные недостатки действующих сегодня стандартов из области проектирования и оценки программных продуктов и их ГПИ вынуждают специалистов по проектированию интерфейсов самостоятельно вводить понятия и разрабатывать авторские метрики. Из этого следует, что неизбежно среди всего этого множества будет отсутствовать общность и унификация. Полученные таким образом результаты будет трудно или даже невозможно сравнить.

Создание на основе существующих стандартов и последних исследований [1, 2 ,19, 21] новой системы метрик, позволит логически упорядочить как смысловые группы понятий, так и сами метрики, повысив точность и содержательность оценки. Этим будет сделан очередной шаг в сторону формализации критериев оптимальности интерфейсов и их описания как объекта математического моделирования.

Список используемых источников

1. Ахунова Д. Г., Вострых А. В. Преимущества перехода на целеоринтированное проектирование интерфейсов для мобильных пользователей информационных систем // V Всероссийская научно-техническая конференция с международным участием «РОСИНФОКОМ-2019», 2019. С. 5–9.

2. Копов С. А., Макарычев П. П., Шибанов С. В. Разработка метрик измерения юзабилити на основе деятельностного подхода // Труды международного симпозиума надежность и качество. 2010. С. 504–508.

3. ГОСТ Р ИСО 14915-1-2016 Эргономика мультимедийных пользовательских интерфейсов. Часть 1. Принципы проектирования и структура от 02 ноября 2016 года №ИСО 14915-1-2016.

4. ГОСТ Р ИСО 14915-2-2016 Эргономика мультимедийных пользовательских интерфейсов. Часть 2. Навигация и управление мультимедийными средствами от 02 ноября 2016 года №ИСО 14915-2-2016.

5. ГОСТ Р ИСО 14915-3-2016 Эргономика мультимедийных пользовательских интерфейсов. Часть 3. Выбор и сочетание медиаформ от 25 ноября 2016 года №ИСО 14915-3-20 16.

6. ГОСТ Р ИСО 9241-110-2016 Эргономика взаимодействия человек-система. Часть 110. Принципы организации диалога.

7. ГОСТ Р ИСО 9241-129-2014 Эргономика взаимодействия человек-система. Часть 129. Руководство по индивидуализации программного обеспечения.

8. ГОСТ Р ИСО 9241-161-2016 Эргономика взаимодействия человек-система. Часть 161. Элементы графического пользовательского интерфейса.

9. ГОСТ Р ИСО 9241-210-2016 Эргономика взаимодействия человек-система. Часть 210. Человеко-ориентированное проектирование интерактивных систем.

10. ПНСТ 169-2016/ISO/DIS 9241-220 Эргономика взаимодействия человек-система. Часть 220. Процессы обеспечения, выполнения и оценки человеко-ориентированного проектирования в организации.

11. ГОСТ Р ИСО 9241-11-2010 Эргономические требования к проведению офисных работ с использованием видеодисплейных терминалов (VDT). Часть 11. Руководство по обеспечению пригодности использования.

12. ГОСТ Р ИСО/МЭК 9126-93. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению.

13. ГОСТ 28806-90 «Качество программных средств. Термины и определения».

14. ГОСТ Р 55241.50-2014/ISO/TR 16982:2002 Эргономика взаимодействия человек-система. Методы обеспечения пригодности использования в человеко-ориентированном проектировании.

15. ГОСТ Р ИСО 9241-20-2014 Эргономика взаимодействия человек-система. Часть 20. Руководство по доступности оборудования и услуг в области информационно-коммуникационных технологий.

16. ГОСТ Р ИСО/МЭК 25010-2015 Информационные технологии (ИТ). Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов.

17. Головач В. Дизайн пользовательского интерфейса V1.1 : учебное пособие. 2009. 146 с. URL: https://litmy.ru/knigi/design_i_arhitektura/384009-dizajn-polzovatelskogo-interfejsa-v11.html

18. Бирман И. Пользовательский интерфейс [Электронный ресурс]. Издательство Бюро Горбунова. 2017. С. 105. URL: https://litmy.ru/knigi/design/192405-elektronnyy-uchebnik-polzovatelskiy-interfeys.html

19. Самойлов К. В. Подходы к определению юзабилити // Психологический журнал. 2013. Т. 34. № 4. С. 106–108.

20. Гарретт Дж. Веб-дизайн: книга Джесса Гарретта. Элементы опыта взаимодействия». Пер. с англ. СПб. : Символ□Плюс, 2008. 192 с.: ил. ISBN-10: 5-93286-108-8 ISBN-13: 978-5-93286-108-0

21. Вострых А. В. Сравнительный анализ методов оценки человеко-машинных интерфейсов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. С. 179–184.

Статья представлена научным руководителем, профессором кафедры БИС СПбГУТ, доктором технических наук, профессором М. В. Буйневичем.

УДК 004.91
ГРНТИ 50.49

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА С ЦЕЛЬЮ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ НАУЧНОЙ И ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТЬЮ ВУЗОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Р. В. Галиев, И. Б. Саенко

Военная академии связи

В современных условиях системы электронного документооборота все больше приобретают статус обязательного элемента IT инфраструктуры. Благодаря таким системам промышленные предприятия и коммерческие компании повышают эффективность своей деятельности. В рамках работы будет предоставлены современные существующие системы электронного документооборота в рамках государственных учреждений, больших предприятий, а также мелких организаций. Кроме этого будут подобраны характеристики и возможности СЭД для улучшения эффективности управления в научной и образовательной деятельностью вузов Российской Федерации.

электронный документооборот; электронный документ; управление вуза.

В подразделениях вузов возникает потребность в применении комплексных средств автоматизации в связи с интенсивным ростом информационных потоков в подразделениях вузов. Данные средства могут повысить оперативность, гибкость и мобильность принятия управленческих решений. Переход от бумажного к электронному документообороту представляет собой одну из актуальных и первоочередных задач автоматизации вуза [1, 2, 3]. Кроме того, усложнение бизнес-процессов современных вузов существенно влияет на их конкурентоспособность, исходя из чего требуется оптимизировать деятельность структурных подразделений и при необходимости организационных структур.

Целью изучения данной темы является анализ и выбор положительных качеств современных систем электронного документооборота организаций. Формирование современного документооборота в вузе как базового структурного элемента деятельности организации позволит повысить эффективность вуза за счет внедрения системы электронного документооборота СЭД/ECM, а также провести оптимизацию бизнес-процессов, обеспечить

возможность использования данных в соответствии нормативными требованиями и ускорить время выполнения операций сотрудниками при обработке документов [4, 5].

Были рассмотрены современные системы автоматизации делопроизводства в небольших организациях и больших предприятиях. Были выписаны наиболее современные и актуальные характеристики и возможности.

В большинстве систем электронного документооборота идет упор на эффективное хранение, а также поиск нужных документов (архивация). Кроме того, поддерживаемость системы на различных программных платформах, как зарубежных, так и отечественных. К вопросу о хранении документов предполагается хранение всех документов от изображений, таблиц, диаграмм и видеофайлов до полноценных программных продуктов – исходных кодов программ и документации к ним.

При рассмотрении вопроса о доступе к документам предполагается разделение прав доступа. Разграничение доступа в СЭД выражается в её разделении на несколько подсистем или модулей. Подсистемы, входящие в состав почти любой СЭД, направлены на решение типовых задач обработки документов: регистрация и контроль движения служебной корреспонденции, подготовка и регистрация документов, контроль распорядительных документов, поручений.

Многие системы поддерживают интеграцию с офисными приложениями, такими как MS Office, LibreOffice. Эффект от интеграции системы электронного документооборота, в первую очередь, выражается в исключении повторного ввода данных, облегчении взаимодействия пользователей различных систем, упрощении подготовки сводной отчетности и анализа данных из разных систем, а также в облегчении работы конечного пользователя [6, 7].

Любая система электронного документооборота содержит в себе динамическое управление и контроль исполнения работ. Данная возможность позволяет эффективно быстро узнавать и управлять, и уведомлять пользователей об изменениях в документах.

В связи с переходом программного обеспечения на отечественные программные платформы, многие системы поддерживают кроссплатформенность.

Исходя из всего вышесказанного, можно определить главные составляющие успешной системы электронного документооборота:

1) Архивируемость.
2) Разграничение доступа.
3) Интеграция с приложениями.
4) Управление и контроль.
5) Кроссплатформенность.

Нами планируется разобрать способы, методы и подходы к реализации данных возможностей, чтобы выбрать оптимальный вариант разработки системы электронного документооборота для использования ее в Военной академии связи им. Маршала Советского Союза С. М. Буденного.

Список используемых источников

1. Линев А. А. Импортозамещение СЭД: возможности и риски // Делопроизводство. 2015. № 3. С. 35–38.

2. Клишин А. П., Стась А. Н., Газизов Т. Т., Кианицын А. В., Бутаков А. Н., Мытник А. А. Основные направления информатизации деятельности Томского государственного педагогического университета // Вестник Том. гос. пед. ун-та. 2015. Вып. 3 (156). С. 110–118.

3. Стародубцев Ю. И. Мальцева У. В. Подход к созданию двухэтапного комплексного метода оценки экономической деятельности предприятия // Экономика и менеджмент систем управления. 2015. Т. 16. № 2–1. С. 172–177.

4. Клишин А. П., Волкова Н. Р., Еремина Н. Л., Мытник А. А., Клыжко Е. Н. Подходы к автоматизации документооборота в вузе // Вестник НГУ. Серия: Информационные технологии. 2017. Т. 15, № 1. С. 36–46.

5. Давлятова М. А., Стародубцев Ю. И. Алгоритм определения параметров инновационного развития предприятий связи // Научно-технические ведомости Санкт-Петербургского государственного политехнического института. Экономические науки. 2018. Т. 11. № 4. С. 251–262.

6. Закалкин П. В., Сагдеев А. К., Стародубцев Ю. И., Сухорукова Е. В. Проблема формирования системы динамической защиты государственных информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сборник научных статей: в 3-х томах. СПб. : СПбГУТ, 2016. Т. 3. С. 239–243.

7. Стародубцев Ю. И., Алисевич Е. А., Терентьев Г. А. Информационная модель рынка с субъектами, обладающими разноуровневыми ресурсами // Проблемы экономики и управления в торговле и промышленности. 2015. № 2 (10). С. 78–83.

УДК 004.514
ГРНТИ 81.95.33

ФОРМИРОВАНИЕ ЭТАПОВ РАЗРАБОТКИ ИНТЕРФЕЙСА МОБИЛЬНОГО ПРИЛОЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ ПРИНЦИПОВ UX/UI ДИЗАЙНА

Е. В. Германова, А. В. Федорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена актуальному в настоящее время направлению разработки графических интерфейсов. Рассматриваются этапы разработки интерфейса мобильного приложения, которые представляются в виде последовательности шагов, формирующих жизненный цикл разработки пользовательского интерфейса. В основу разработки этапов проектирования положены принципы UX/UI дизайна, базирующиеся на изучении опыта пользователей и законов графического дизайна и их совместном применении при подготовке к этапу проектирования приложений и самому проектированию.

мобильное приложение, поэтапная разработка, пользовательский интерфейс, UX/UI дизайн.

В настоящее время направление разработки мобильных приложений актуально и востребовано. Одним из основных действий при создании мобильного приложения является разработка его интерфейса. Интерфейс показывает возможность взаимодействия между двумя или более системами и их компонентами. Пользовательский интерфейс – это интерфейс, который обеспечивает передачу информации между пользователем и программой [1]. Существуют различные подходы к разработке пользовательского интерфейса. Поэтапная разработка пользовательского интерфейса необходима для уменьшения времени разработки и увеличения эффективности. В зависимости от типа интерфейса, поставленных целей и задач, временных ресурсов и прочих факторов, этапы могут различаться [2]. На рис. (см. ниже) показан один из вариантов поэтапной разработки пользовательского интерфейса, позволяющий стандартизировать этот процесс.

Использование принципов UX/UI дизайна при разработке пользовательского интерфейса позволяет улучшить качество разрабатываемого продукта, помогает принимать правильные решения при разработке интерфейса и создавать эффективные приложения, которые помогут пользователям достигать целей.

Взаимодействие пользователя с интерфейсом – это UX-дизайн. UX означает «опыт пользователя». То, как пользователь будет воспринимать

этот интерфейс – это UI-дизайн. UI означает «пользовательский интерфейс». UI – то, как выглядит интерфейс и то, какие физические характеристики приобретает. UX-дизайн отвечает за структуру приложения, информационную архитектуру функциональность, удобство и простоту использования приложения. UI-дизайн отвечает за то, какие цвета, шрифты, кнопки, формы заявок, анимация, изображения будут использоваться в интерфейсе [3].

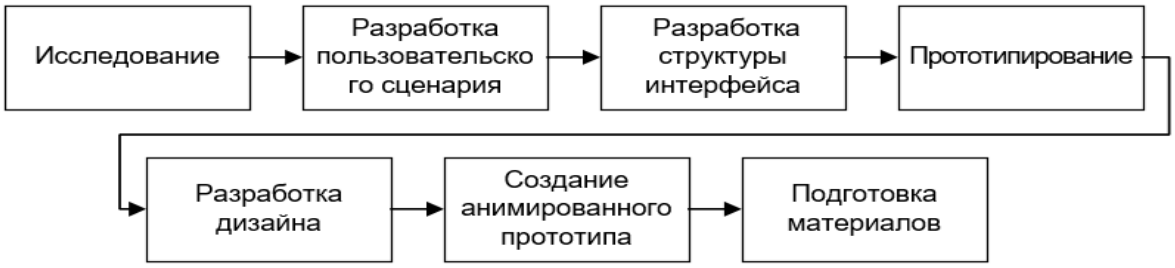


Рис. Этапы разработки пользовательского интерфейса

Рассмотрим более подробно этапы разработки пользовательского интерфейса, акцентируя внимание именно на том, какие принципы UX/UI дизайна применяются на каждом этапе разработки интерфейса.

I.Этап исследования

На этапе исследования собирается информация об аналогах разрабатываемого интерфейса, проводятся исследования аудитории, проводится анализ похожих приложений, выявляются плюсы и минусы готового интерфейса. Если мы говорим о применении принципов UX дизайна на этом этапе, то здесь существует два вида UX исследований: качественные и количественные. Качественные исследования направлены на получение информации об удобстве использования, актуальности, популярности. Такие данные позволяют понять, как ведут себя пользователи и как адаптировать их запросы под проектируемый интерфейс. Количественные исследования направлены на получение конкретных данных. Производится сбор статистики, например, как часто пользователи пользуют функциями, как часто они совершают действия при взаимодействии с интерфейсом. Вся эта информация представляется в цифровом виде, после чего производится анализ. Анализ показывает, насколько функции востребованы у пользователей, и легко ли пользователи достигают цели. Изучение аудитории помогает определить профиль будущих пользователей, чтобы создать подходящий интерфейс.

Исследование аудитории можно проводить разными методами [4].

1. Полевое исследование. Проводится наблюдение за пользователями, когда они находятся в привычных для себя условиях.

2. Исследование фокус-групп. Здесь проводится опрос группы людей, которые относятся к целевой аудитории.

3. Интервью. Проводится для того, чтобы выявить отношение пользователя к разрабатываемую интерфейсу, его ожиданий и желаний, для анализа пользовательского опыта.

4. Онлайн опросы. Опрос состоит из ряда вопросов, которые позволяют понять предпочтения и мнения пользователей на заданные темы.

5. *Usability* тестирование. Здесь пользователи оценивают приложение при тестировании. Оценки пользователей показывают, насколько им нравится приложение и насколько им удобно пользоваться. Тестирование показывает какие изменения необходимо внести, чтобы улучшить приложение.

II.Разработка пользовательского сценария

На этом этапе, в первую очередь, создается профиль будущего пользователя. Профиль пользователя содержит информацию о возрасте человека, интересах, социальном статусе, финансовом положении, месте работы. Дальше, на основе профиля создается пользовательский сценарий. Пользовательский сценарий – это краткая история, которая описывает, как пользователь достигает поставленной цели, взаимодействуя с интерфейсом. Пользовательский сценарий нужно писать так, чтобы его можно было протестировать. Потом на основе пользовательского сценария уже можно определить размер экранов, кнопок, сложность переходов, установить ограничения для проектирования. Благодаря детальному рассмотрению взаимодействия пользователя с приложением формируется правильная структура приложения, которая в будущем будет формировать положительный пользовательский опыт. Пользовательский сценарий помогает выявить потребности, предугадать поведение, желания и поведение пользователя.

III.Разработка структуры интерфейса

Структура интерфейса разрабатывается на основе пользовательского сценария. Она представляется в виде схемы. Такая схема представляет собой пользовательский маршрут, который показывает основные экраны проектируемого приложения и их взаимодействие с пользователем. Структуру интерфейса следует строить так, чтобы пользователь поэтапно получал необходимую информацию, а не всю сразу. Структурная схема является наилучшим представлением пользовательского опыта. Она помогает понять, как люди взаимодействуют с интерфейсом приложения, и когда им нужно выполнить действие. В основе схемы лежит порядок действий, которые пользователь будет выполнять, используя приложение. Структурная схема отражает в себе все экраны приложения и все возможные переходы между ними, функциональность экранов, формирование структуры меню и

различных элементов навигации [5]. Схема формируется из последовательных шагов, которые, в конечном счете, формируют пользовательский опыт. На этом этапе следует следить за тем, чтобы была понятная и простая навигация, чтобы каждый экран отражал одну главную функцию. Здесь применяется принцип последовательности.

IV.Прототипирование

На основе структуры приложения создается прототип. Прототип – это интерактивный макет, который можно представить в разных степенях точности. Он создаётся для того, чтобы показать, как будет работать интерфейс, не вдаваясь в подробности графики. Прототип представлен в виде последовательности экранов. Прототипы создаются в специальных программах, таких как: Figma, Sketch, Adobe XD. Экраны показаны серо-белыми прямоугольниками, в которых расположены кнопки, поля, линии и примеры написания текста. Такой прототип позволяет определить главные функции, расположение кнопок, и сколько информации будут содержать экраны. Здесь применяется принцип расставления приоритетов и направления внимания. На этом этапе параллельно с этапом дизайна и анимированного прототипа применяются: эффект Рессторф, эффект края, закон Хикка, закон близости, законы композиции, принцип визуальной иерархии, группировки объектов [6].

V.Разработка дизайна и стилизация

После того, как прототип готов, наступает этап внешнего оформления интерфейса. В первую очередь, необходимо разработать мудборд. Мудборд – это набор фотографий, изображений, текстур, элементов типографики, цветовой палитры в одном стиле. Такой набор формирует приблизительную цветовую гамму и стилистику. При выборе цвета и формы следует пользоваться цветовым кругом и законами композиции. Цвет в интерфейсе выступает в качестве расставления акцентов. Когда дизайн концепция определена, начинается процесс оформления прототипа. Этот процесс включает в себя выбор типографики, цвета, толщины линий, создаются иконки, иллюстрации, кнопки и другие элементы экрана. Также на этом этапе могут вноситься правки в прототип. Здесь применяются следующие принципы UI дизайна: гибкости, узнаваемости, согласованности, последовательности [6].

VI.Разработка анимированного прототипа

Следующий шаг – это разработка анимированного кликабельного прототипа. Анимированный прототип является самым высокоуровневым прототипом. Это окончательная модель интерфейса приложения. Она содержит в себе все визуальные и функциональные элементы интерфейса и работает

как конечный продукт. Он эмулирует реальное взаимодействие пользователя с интерфейсом. Он позволяет нажимать кнопки, использовать формы ввода информации, показывает переходы между экранами. Также здесь проектируется анимация. Анимация является способом коммуникации приложения с пользователем. Она позволяет пользователю оставаться в курсе всех событий, происходящих в приложении, и в разы повышает usability (удобство использования) интерфейса. Этот этап показывает, как будет работать конечный продукт. При разработке анимированного прототипа применяются принцип единства, принцип ясности (в любом месте пользователь должен понимать, где он находится). Также комбинируются принципы UX/UI дизайна из предыдущих этапов.

VII.Подготовка материалов

Завершающим этапом в разработке пользовательского интерфейса является подготовка материалов для разработчиков. Когда интерфейс разработан, необходимо передать все материалы разработчикам для дальнейшего использования в разработке приложения. Следует передать UI кит, элементы интерфейса. UI-кит – это готовый набор графических элементов пользовательского интерфейса (шрифты, иконки, изображения и готовые текстуры).

Таким образом, поэтапная разработка экономит время создания интерфейса, позволяет структурировать процесс разработки. Поэтапная разработка интерфейса позволяет быстро добраться до конечной цели и вносить изменения в процессе разработки. Использование принципов UX/UI дизайна на каждом из этапов разработки интерфейса позволяет улучшить качество получаемого продукта и получить тот продукт, с которым будет удобно пользоваться.

Список используемых источников

1. Сверчков Д. С. Разработка человеко-машинного интерфейса и его применение в системах управления // Труды Крыловского государственного научного центра. 2018. Спец. вып. 1. С. 184–190.

2. 8 этапов процесса разработки интерфейса мобильного приложения [Электронный ресурс]. URL: https://habr.com/ru/company/skillbox/blog/416641/ (дата обращения: 03.03.2020).

3. UX/UI дизайн: что это такое? [Электронный ресурс]. URL: https://skillbox.ru/media/design/ux_ui_dizayn_chto_eto_takoe/ (дата обращения: 03.03.2020).

4. UX исследования для маркетплэйса [Электронный ресурс]. URL: https://ru.wiki.rademade.com/ux-research (дата обращения: 03.03.2020).

5. LeahBuley. The User Experience Team of One: A Research and Design Survival Guide264 pages. Rosenfeld Media, 264 pages.

6. Принципы гештальта в дизайне интерфейсов, которые знает, пожалуй, каждый UX/UI-дизайнер [Электронный ресурс]. URL: https://medium.com/начинающему-ux-

дизайнеру/принципы-гештальта-в-дизайне-интерфейсов-которые-знает-пожалуй-каждый-ux-ui-дизайнер-9a2d4c702884 (дата обращения: 03.03.2020).

УДК 331.108.26
ГРНТИ 82.01.85

АНАЛИЗ СУЩЕСТВУЮЩЕГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В СФЕРЕ УПРАВЛЕНИЯ ПЕРСОНАЛОМ

Г. С. Глазков, С. В. Хорошенко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Управление персоналом подразумевает под собой большое количество различных инструментов, методологий и концепций. Для начинающего или некомпетентного руководителя небольшой компании существующие возможности в сфере управления персоналом могут казаться сложными и непонятными. Рассмотрены направления развития сферы кадрового менеджмента, проведен сравнительный анализ имеющихся программных решений в сфере управления персоналом, а также предложены варианты программных реализаций управления персоналом для начинающих руководителей.

информационные системы, управление персоналом, кадровый менеджмент, программное обеспечение.

На данный момент в мире всё большую популярность приобретает проектная деятельность и организация стартапов. Ежегодно проводятся множество грантовых конкурсов, хакатонов и запускаются бизнес-акселераторы, как для студентов, так и для молодых предпринимателей. В процессе проведения таких мероприятий для людей или организаций выделяются денежные субсидии и премии на реализацию идей и их дальнейшее развитие с последующим выходом продукта или компании на рынок.

В таких реалиях появляется всё больше молодых предпринимателей, жаждущих основать свое собственное дело, для развития которого им придется управлять персоналом, используя различные инструменты и методологии.

Успех в компании во многом зависит от инновационного управления в организации, а конкретно от деятельности системы управления персоналом и отдела кадров. [1] И сейчас руководителю предоставляется выбор – организовывать работу с персоналом уже известными методами или изучать и применять на практике инновационные методологии.

Можно выделить три фундаментальных направлений инноваций в сфере управления:

1. Кадровый маркетинг – подготовка компетентного кадрового потенциала компании;

2. Технологический кадровый менеджмент – изучение способов применения новых информационных технологий в работе с персоналом;

3. Образовательный кадровый менеджмент – средства и возможности подготовки кадров и их образовательный процесс.

Условие, которое объединяет все три направления развития в сфере – они базируются на принципах, которые противопоставлены традиционному управлению персоналом. Как пример – инновационные методы управления заставляют отходить от материального стимулирования сотрудника, ведь в ситуациях, где необходимо нестандартное решение задачи, материальное вознаграждение приведет к снижению необходимой продуктивности [2].

С точки зрения инноваций технологического менеджмента именно для сферы управления персоналом можно отметить развивающийся сегмент рынка программного обеспечения.

Сейчас рынок информационных систем по управлению персоналом делится на две части. Первая связана с учётно-расчетными функциями и ведением кадрового делопроизводства. Вторая относится к повышению эффективности работы персонала, покрывая процессы подбора, адаптации и обучения персонала, оценке его потенциала и эффективности. У этих частей рынка различные степени зрелости, тенденции развития и объемы (http://www.tadviser.ru/index.php/).

В контексте инноваций нужно говорить о второй части рынка, так как с точки зрения количества возможностей она является наиболее перспективной за счёт использования комплексных решений, позволяющих получать ранее недоступные ввиду разрозненности программных решений и возникающие на смежных процессах данные.

В области управления талантов в России самым известным программным средством является «ТопФактор: Управление талантами» от «1С: Предприятие». В его функционал входят: оценка персонала, его развитие и обучение по результатам оценки, адаптация сотрудника при приеме на должность, ранжирование сотрудников, управление кадровым рисками и вовлеченностью. Так же «ТопФактор» предоставляет возможность конструировать отчётность и интеграции с «1С: Зарплата». За счёт последнего пункта «ТопФактор» уже отрывается от своих ближайших конкурентов по российскому рынку, так как мало у кого есть возможность интегрировать собственный сервис для расширения функционала, тем более что этот сервис использует достаточно большая аудитория предпринимателей.

Плюсы программы: предоставление компании личного консультанта, для помощи с настройкой системы, возможность использования в виде облачного сервиса, что облегчает весь процесс интеграции продукта в работу предприятия, и долгое время нахождения на рынке, что вызывает доверие у потребителя и позволяет компании развивать продукт на основании обратной связи со своих же пользователей.

Минусы программы: для более широкого охвата данных и показателей сотрудников необходимо использовать остальные продукты инфраструктуры «1С: Предприятие», высокая стоимость программного обеспечения, недоступная для сектора малого бизнеса и начинающих предпринимателей.

Если оценивать пользовательский интерфейс по количественному методу модели GOSM, то он разработан с соблюдением норм и оптимальным расположением элементов для минимальной затраты времени, необходимого для управления талантами. Говоря о графической составляющей можно утверждать, что интерфейс разработан строго без лишних украшений. Интерфейс программы продемонстрирован на рис.

Рис. Интерфейс программы «ТопФактор»

В сравнение российскому продукту можно взять «SAP SuccessFactor» американского производства. В её функциональные возможности входит: базовое управление персоналом и расчёт зарплаты, управление учётом рабочего времени, оценка эффективности и вознаграждения сотрудников, подбор и адаптация персонала, планирования персонала и аналитика результатов его работы.

Плюсы программы: предоставление рекомендаций на основе лучших практик управления талантами, интеграция с любыми системами расчётно-учетного функционала, реализация корпоративной социальной сети и самый главный плюс программного обеспечения «SAP SuccesFactor» – это

наличие мобильного приложения, приближающего кадровые операции к сотрудникам.

Минусы программы: отсутствие кастомизации под нужды определенной компании, то есть если какого-либо функционала не хватает, то нужно искать другой продукт, чтобы дополнить или заменить SuccesFactor, высокая цена на продукт.

«SAP SuccesFactor» также, как и «ТопФактор» является частью инфраструктуры продуктов по управлению кадрами. Но подход к его интеграции в работу предприятия отличается – SuccesFactor более самостоятельный продукт, он не зависим от функционала сторонних сервисов компании SAP и способен сам покрыть все потребности по управлению талантами.

Теперь стоит рассмотреть не комплексные продукты, покрывающие практически все потребности больших компаний, а программы, которые представляют собой решение одной, конкретной задачи.

Такие программные продукты, в первую очередь, отличаются ценовой политикой, которая построена очень гибко и часто предусматривает даже бесплатные тарифы, если пользователю необходимо подключить малое количество сотрудников.

Также программное обеспечение в сфере управления кадрами для малого бизнеса ввиду отсутствия большого количества функциональных возможностей может легко интегрироваться в только начавшее свой путь предприятие или разрабатываться строго для определенного потребителя

Например, у только что открывшейся стоматологической клиники будет выбор: использовать для управления персоналом комплекс программных продуктов от компании «1С» или внедрить информационную систему «DENTIST+», которая создана специально для подобного рода предприятий и способна эффективно организовать рабочий процесс, составлять графики, хранить и записывать документы, включая бухгалтерию клиники, получать удобные отчёты за каждый день, неделю или месяц.

В то же время малое предприятие, используя специализированный продукт, имеет возможность дополнить его функционал другой программой, как если стоматологической клинике не хватит функционала контролирования персонала на рабочем месте, то она может дополнить «DENTIST+» сервисом «Yaware.Timetraker», который обеспечит контроль как за административным составом, так и за нахождением докторов на своих местах.

Помимо приобретения комплексных или узкоспециализированных программных решений, у компании есть возможность заказать разработку собственной информационной системы, которая будет реализована только под нужды компании. Экономически этот вариант находится приблизительно на одном уровне с приобретением узконаправленного программного обеспечения, если рассматривать наличие в них идентичного функционала,

и беря во внимание, что плата за разработку – это единоразовая трата, а за готовый продукт необходимо платить меньше, но ежемесячно.

Получается, что у начинающего предпринимателя есть несколько путей развития процессов управления персоналом, и выбор будет зависеть от его временных и экономических возможностей:

1. Есть время и деньги – в таком случае есть возможность обратиться за разработкой собственной информационной системы. Для этого необходимо иметь чёткое представление о необходимых возможностях на годы вперед. Например, если изначально не предусмотреть в системе её масштабируемость, то во время расширения компании придется искать новые программные решения, вместо обновления имеющегося.

2. Есть деньги, но нет времени – если у руководителя есть желание и средства для грамотной организации труда сотрудников, то изучив рынок программного обеспечения он может приобрести программное решение, удовлетворяющее все его запросы. При анализе рынка стоит обратить внимание на множество факторов: насколько хорошо у компании разработчика работает служба поддержки, обратная связь от пользователей, облачный это сервис или интегрируется локально.

В ходе анализа имеющихся на сегодня тенденций в сфере управления персоналом выявлено то, что сейчас существует три фундаментальных направления инноваций, включающих технологическое развитие сферы. Оно же, в свою очередь, разделяется на технологические продукты двух видов: учетно-расчётные и управление талантами. Исходя из того, что у второго вида больше вариантов развития, её программные решения разобраны подробнее. На примере русского и американского продуктов описаны возможности комплексных систем, выявлены их преимущества и недостатки. Отталкиваясь от минусов представлены преимущества узконаправленных систем и заказ их разработки индивидуально под нужды компании с описанием предполагаемых сценариев начинающих руководителей. При выборе одного из двух вариантов работы с программным обеспечением, руководитель должен основываться на текущих денежных ресурсах компании и оценивать необходимость предприятия в такого рода технических средствах.

Список используемых источников:

1. Голянич В. М., Кудрявцева Е. И. Инновационные технологии в кадровом менеджменте // Управленческое консультирование. 2013. № 2 (50). 245 с.

2. Синева Н. Л. Менеджмент организации: моделирование инновационной деятельности: учебно-методическое пособие. Нижний Новгород : Нижегородский государственный педагогический университет им. К. Минина. 2015. 76 с.

УДК 004.422.81; 658.5
ГРНТИ 50.53.19

АВТОМАТИЗАЦИЯ ПРОЦЕДУР ЖИЗНЕННОГО ЦИКЛА РЕЗУЛЬТАТОВ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВУЗА

П. А. Глыбин, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются системотехнические решения по построению системы автоматизированного учета и сопровождения результатов интеллектуальной деятельности образовательного учреждения (вуза) на принципах построения систем управления жизненным циклом продукции. Предложена интерфейсная среда форм отчетных документов, сведения из которых являются информационной основой для принятия решений по обеспечению коммерциализации нематериальных активов (НМА) вуза и по поддержанию объектов интеллектуальной собственности в актуальном состоянии в процессе их жизненного цикла. Использование оригинальных программных решений позволяет обеспечить полноту и достоверность сведений, имеющих юридическую значимость для ведения документооборота коммерциализируемых НМА.

результаты интеллектуальной деятельности, автоматизированный учет движения нематериальных активов.

Одной из основных функций образовательного учреждения (вуза) является управление научными исследованиями и результатами интеллектуальной деятельности (РИД) (см. пример на рис. 1).

Основными задачами автоматизации в процессе жизненного цикла результатов интеллектуальной деятельности (РИД) образовательного учреждения (вуза) являются автоматизация следующих процедур [1]:

– первичной регистрации РИД в ходе образовательного процесса вуза (на примере изобретений, программ для ЭВМ и баз данных);

– учета комплектности заявительных документов вуза для регистрации РИД в Роспатенте;

– сопровождения заявительных документов вуза при регистрации и получении документов на объект интеллектуальной собственности (ОИС);

– постановки ОИС на бухгалтерский учет вуза как нематериальных активов (НМА), коммерциализации НМА вуза и снятия с бухгалтерского учета из-за прекращения сроков их использования.

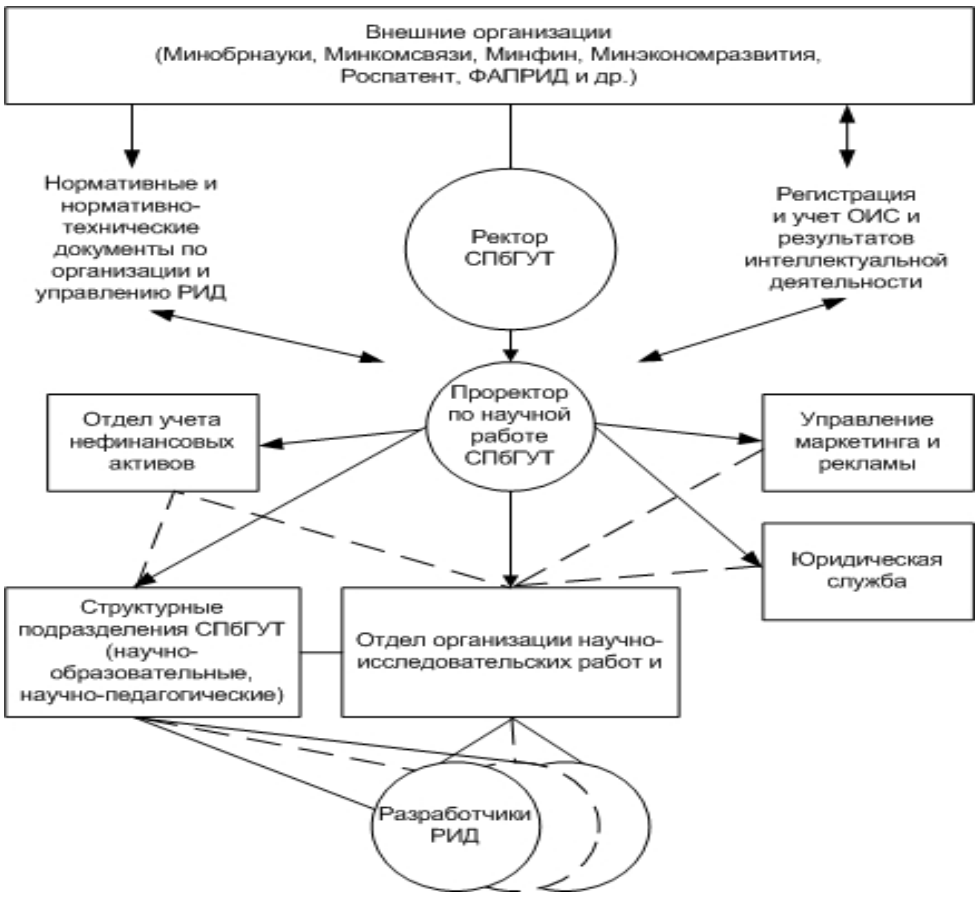


Рис. 1. Структура системы управления правами на РИД в СПбГУТ

Процедуры (см. рис. 2) имеют различную продолжительность, которая зависит от типа РИД, проработанности заявительных документов, стоимости НМА, планируемых сроков их использования и других условий.

Рис. 2. Обобщенные процедуры жизненного цикла РИД

При автоматизации процедур первичной регистрации РИД целесообразно применять шаблонные формы представления данных на основе требований нормативных и нормативно-технических документов федеральных органов исполнительной власти уполномоченных в этой сфере деятельности, а также локальных регламентов (документов) отрасли и организации (учреждения) [2].

Типовые формы представлены на рис. 3.

Форма 1. Учетные данные первичной регистрации РИД вуза

Внутренний регистрационный номер	Дата поступления	Автор	Контакты автора	Данные об авторе	Название	Заявляемый объект (Тип РИД)	Описание
0001	0002	0003	0004	0005	0006	0007	0008

Форма 2. Учетные данные комплектности заявительных документов на РИД вуза

Внутренний регистрационный номер	Данные об экспертном заключении	Данные о стоимости РИД	Данные об оплате пошлины	Комплектность документов	Исходящий номер	Способ отправки	Сведения о корреспонденции
0001	0010	0011	0012	0013	0014	0015	0016

Форма 3. Учетные данные комплектности заявительных документов на РИД вуза

Внутренний регистрационный номер	Дата поступления в ФИПС	Регистрационный номер	Запрос на дополнительные материалы	Ответ с дополнительным материалом	Номер документа	Дата документа	Тип Документа
0001	0100	0101	0102	0103	0104	0105	0106

Форма 4. Учетные данные об НМА и их коммерциализации

Внутренний регистрационный номер	Данные об Акте инвентаризации НМА	Данные о постановке на бухгалтерский учет	Срок полезного использования НМА	Данные о лицензиях	Стоимость коммерциализации НМА	Данные об окончании срока использования	Сведения о поддержании в действии
0001	1000	1001	1002	1003	1004	1005	1006

Рис. 3. Типовые формы учетных данных РИД

В настоящее время известно несколько программных средств, реализующих автоматизируемые функции аналогично представленным. Их основные характеристики приведены в таблице.

ТАБЛИЦА. Программные средства учета РИД

Продукт	Разработчик	Назначение (функции)	Источник
Бизнес-приложения платформы "Мелисса"	ЗНП АО "Отделение ПВЭ и Ф"	Программа «Управление РИД»; Программа «Сбор данных по учету РИД»	http://opvf.ru/
ФГИС «АИС учета РИД»	ФГАНУ ЦИТиС	Федеральная гос. информационная система учета результатов НИОКР военного, специального и двойного назначения, права на которые принадлежат РФ	https://rupto.ru/ru
АИС РНТД	ООО «ДИАВЕР»	АИС ведения результатов научно-технической деятельности по итогам выполнения государственных инвестиционных программ	http://site.diaver.org/ru/

Технические решения в представленных программных средствах реализуют различные механизмы видов и способов управления; способов обработки данных и использования средств обработки данных; использования носителей информации, форм считывания и распознавания данных, а также

форм использования специфических вычислительных моделей; организации связи и способов хранения данных. Однако для применения в вузах в качестве наименее затратных, технологически функциональных и гибких средств автоматизации могут рассматриваться программные средства (программы для ЭВМ) собственной разработки и сопровождения, адаптированных к развернутым в вузах различным автоматизированным системам.

В ходе предварительного исследования был проведен анализ возможных к применению средств разработки требуемой программы:

– MySQL Workbench, инструмент разработки баз данных, который интегрирует функции проектирования, моделирования, создания и эксплуатации баз данных в единой бесшовной взаимодействующей среде;

– Toad for MySQL, средство исполнения запросов, автоматизации управления объектами базы данных и разработки кода SQL, которое содержит утилиты для сравнения, извлечения и поиска объектов, обеспечивает управление проектами, импорт/экспорт данных и администрирование базы данных;

– PostgreSQL, объектно-реляционная СУБД для некоторых UNIX-подобных платформ, различных BSD-систем, Linux, macOS, Microsoft Windows и других.

С применением средств PostgreSQL разрабатываемые оригинальные программные решения позволят обеспечить полноту и достоверность сведений, имеющих юридическую значимость для ведения документооборота коммерциализируемых НМА.

Макет программы для ЭВМ при незначительной доработке может быть доведен до уровня промышленного изделия [3].

Эффект внедрения автоматизированных процедур жизненного цикла РИД вуза достигается посредством реализации процедур, установленных в ГОСТ Р 56823-2015 (Интеллектуальная собственность. Служебные результаты интеллектуальной деятельности), которые обеспечат:

– снижение рисков коммерциализации РИД, за счет полноты представленных сведений и их анализа в ходе первичной регистрации РИД;

– сокращение непроизводительных затрат при регистрации РИД в Роспатенте за счет своевременного формирования комплектности документов и мониторинга их формирования;

– поддержание в актуальном состоянии сведений при сопровождении и получении охранных документов на ОИС за счет формализации атрибутов, подлежащих мониторингу и контролю;

– получение объективных и своевременных данных о движении РИД (ОИС, НМА) в ходе их коммерциализации.

Список используемых источников

1. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб. : ГУАП, 2016. 325 с.

2. Полпудникова Н. В., Шестаков А. В. Предложения об автоматизированном ведении подлинников конструкторской документации предприятия связи на основе технологии распределенных реестров // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2018. Т. 2. С. 535–540.

3. Глыбин П. А., Плетнев Я. А., Шестаков А. В. Автоматизация мониторинга результатов интеллектуальной деятельности // Сб. статей V Международной научно-практической конференции «Инновационное развитие потенциала науки и современного образования»: в 2 ч. Пенза : «Наука и Просвещение» (ИП Гуляев Г. Ю.), 2019. С. 70–72.

УДК 004.056.5
ГРНТИ 49.33.29

АДАПТАЦИЯ МЕТОДОВ ЗАЩИТЫ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ

С. А. Горбань, А. Н. Кривцов, Е. Р. Никонов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

В статье рассматриваются методы защиты технологии блокчейн и их адаптация для распределенного сервиса обмена сообщениями. Приводятся примеры такой реализации для прототипа разработанного сервиса по технологии блокчейн.

блокчейн, защита информации, безопасность, распределенный сервис, ключ, сообщение.

Методы работы с данными, используемые в технологии блокчейн, известны давно, однако эта технология начала активно развиваться только в 2008 году на основании опыта работы с криптовалютой [1].

Технология блокчейн представляет из себя связь данных (блоков), которые расположены последовательно. Каждый следующий блок связан с предыдущим [2].

Благодаря такой модели построения блокчейн имеет массу преимуществ. Например, информация, хранящаяся в нем, неизменна. Это может стать основой для существования сервисов, где приоритетом является сохранность и неизменяемость пользовательских данных [3]. Одним из таких может стать сервис обмена сообщениями.

Однако методы защиты, которые предлагает блокчейн не могут быть в полной мере реализованы в подобных информационных системах и нуждаются в адаптации.

Главной идеей технологии блокчейн, как было сказано выше, является то, что обрабатываемая ей информация связана, каждый последующий блок данных сочленен с предыдущим. Обычно в системах такая зависимость строится на основе индексов с использование хеширования. Попытка изменения хотя бы одного из блоков данных приводит к изменению его уникального хеш-ключа, ставя в несоответствие все последующие блоки, ссылающиеся на этот измененный блок.

Безопасность технологии блокчейн не ограничивается одними лишь хеш-ключами. На опыте с криптовалютой были созданы дополнительные средства обеспечения безопасности. Мощности современных компьютеров позволяют без лишних проблем пересчитать ключи всех блоков данных в системе. Чтобы избежать этого, технология блокчейн использует механизм, называемый Proof-of-work, замедляющий процесс создания новых блоков данных. В случае с биткоинами это занимает около десяти минут, чтобы создать новый блок в цепочке [4]. Такой механизм практически исключает возможность подделки блоков, ведь чтобы после применения механизма Proof-of-work изменить один блок, нужно пересчитать все последующие блоки через него. Также вместо одного, основного центра управления всей цепочкой, блокчейн может использовать P2P сеть (сеть, основанная на равноправии ее участников) [4]. Когда кто-то присоединяется к сети, он получает полную копию блокчейна. Именно так система может проверять, что все блоки корректны, отталкиваясь от всех пользователей сети, которые создают некую согласованность между собой. Таким образом, совмещая механизм Proof-of-work и P2P сеть, технология блокчейн добивается хороших результатов в области безопасности [4].

Рассмотрим, как эти механизмы могут быть адаптированы к безопасности распределенного сервиса обмена сообщениями.

На стороне клиента сообщение подвергается первичной обработке и отправляется на дальнейшую обработку на сервер в базу данных. Система создает новый блок данных с полученной информацией, уникальным идентификатором, временем создания, собственным уникальным ключом. Используя ключ предыдущего блока, ставит новый блок в зависимость с ним. Также создаваемому блоку данных присваивается идентификатор владельца этих данных. Все ключи создаются посредством хеширования, и их тоже можно назвать уникальными для каждого отдельного создаваемого блока данных. Хеширование происходит путём слияния всех составляющих блока. Получается, что каждый блок данных представляет из себя поля: поле с уникальным идентификатором, поле со временем создания, поле с сообщением, после с идентификатором владельца, поле с собственным ключом,

поле с ключом предыдущего блока. Наличие последнего поля означает, что все блоки связаны между собой (каждый блок связан с предыдущим) и напоминают некое подобие цепи (рис.).

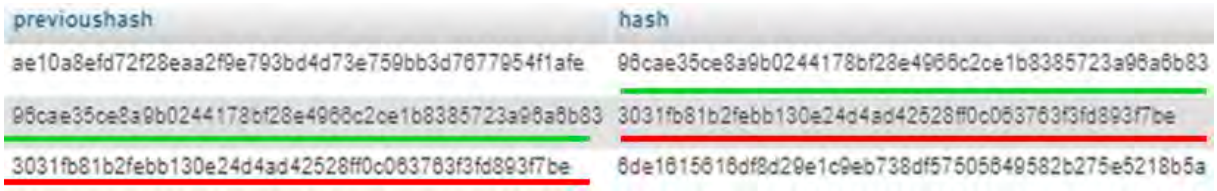


Рис. Хеш-ключи в база данных

Можно увидеть, что механизм Proof-of-work не вписывается в предоставленные условия прямо, ведь сообщения не могут передаваться между двумя пользователями с задержкой в десять минут. Разместить копии блокчейна – копии всех сообщений, между всеми участниками сервиса, пытаясь реализовать некое подобие P2P сети, в полной мере тоже не выйдет, даже исходя из того, что подтверждение каждого нового сообщения потребует подтверждения всех участников системы, а это всё также требует времени. Из всего следует, что методы защиты блокчейна нуждаются в адаптации под систему.

Адаптированные методы защиты могут быть реализованы следующим образом. Как было сказано выше, на стороне клиента выполняет запрос к базе данных на сервер. Осуществляется проверка базы данных на существование каких-либо связанных блоков информации в общем в соответствии с этим запросом. В случае их отсутствия создаётся первоначальный, стартующий блок данных (GenesisBloc – генезис блок), который в дальнейшем передаётся в систему к клиенту с оповещающим сообщением о возможности начала диалога. Таким образом, у каждого участника отдельного диалога (не всех пользователей системы) имеется копия ключа GenesisBlock. Каждый отдельный диалог между пользователями можно хранить в системе в виде отдельной таблицы в базе данных. Таким образом, все участники каждого отдельного диалога будут иметь ключи только от этих диалогов, так называемых «бесед». Также можно реализовать, чтобы вместо ключей у пользователей хранилась копия всей беседы, то есть копия отдельного блокчейна, в которой они участвуют. Разговор в каждой беседе можно разделить на определенные сессии. Чтобы продолжить диалог, нужно активировать сессию. Для активации сессии и продолжения диалога пользователи вводят свои ключи. Ключи передаются на сервер в систему, обрабатываются, сравниваясь с ключом начального блока (GenesisBlock) диалога. После проверки ключей исследуются все остальные блоки. Если вся проверка пройдена, сессия активируется и диалог продолжается, а если не пройдена, то все пользователи диалога оповещаются, что была скомпрометирована

база данных либо один из пользователей. Сессии работают только на продолжении диалогов в беседе, так как при создании нового диалога, как уже было показано ранее, создаётся новый GenesisBlock диалога. Только после создания первоначального блока данных пользователям выдаются ключи для дальнейшего использования, первая сессия активируется автоматически. Адаптированные методы защиты выполняют функции как механизма Proof-of-work, так и P2P сети. Работу с ключами можно реализовать с помощью файлов, куда записан ключ, и которые отправляются на сервер для обработки.

Интерфейс можно реализовать так, чтобы при прохождении через систему безопасности сервис, в том или ином случае, смог оперировать сообщениями-фразами для клиента, такими, например, как: «Ключи валидны. GenesisBlock не поврежден!»; «Данные скомпрометированы! Разрыв цепи в области блоков: (адрес блока), (адрес блока)»; «Данные защищены!»; «Данные скомпрометированы. Несовпадение ключей в области БД, разрыв цепи в области GenesisBlock!»; «Ключ пользователя #1 не валиден! Данные скомпрометированы, разрыв цепи в области GenesisBlock!»; «Ключ пользователя #2 не валиден! Данные скомпрометированы, разрыв цепи в области GenesisBlock!» и т. п. Отталкиваясь от данных фраз, можно понять, какие области безопасности контролирует система.

Для реализации описанного подхода применения предлагаемых адаптивных методов защиты был разработан прототип системы – сервиса обмена сообщениями на основе блокчейна. Условно, данный сервис разделен на клиентскую и серверную части. Серверная часть реализована с использованием сервера Apache и базой данных MySQL. При этом, для реализации «движка общения» использовался язык программирования PHP. Для реализации клиентской части использовался язык программирования JavaScript.

Результаты проведенных экспериментов подтвердили состоятельность адаптации методов обеспечения безопасности технологии блокчейн и возможность использования, как предлагаемых методов, так и самой технологии при разработке систем распределенного сервиса обмена сообщениями.

Список используемых источников

1. Артемьев К. И. Блокчейн: возникновение, особенности использования и регулирования [Электронный ресурс] // Отечественная юриспруденция. 2018. № 4. С. 29. URL: https://cyberleninka.ru/article/n/blokcheyn-vozniknovenie-osobennosti-ispolzovaniya-i-regulirovaniya (дата обращения: 20.02.2020).

2. Федотова В. В., Емельянов Б. Г., Типнер Л. М. Понятие блокчейн и возможности его использования [Электронный ресурс] // European science. 2018. № 1. С. 33. URL: https://cyberleninka.ru/article/n/ponyatie-blokcheyn-i-vozmozhnosti-ego-ispolzovaniya (дата обращения: 20.02.2020).

3. Арефьева А. С., Гогохия Г. Г. Перспективы внедрения технологии блокчейн. [Электронный ресурс] // Молодой ученый: электрон. журн. 2017. Вып. 15. URL: https://moluch.ru/archive/149/42071/ (дата обращения: 08.11.2019).

4. Тапскотт Дон, Тапскотт Алекс. Технология блокчейн: то, что движет финансовой революцией сегодня [пер. с англ. К. Шашковой, Е. Ряхиной]. М.: Эксмо, 2017. 450 с.

УДК 004.415.2
ГРНТИ 50.41.25

КОНЦЕПЦИЯ ПРИЛОЖЕНИЯ ДЛЯ АВТОМАТИЗАЦИИ АДМИНИСТРАТИВНЫХ ЗАДАЧ В АГЕНТСТВЕ НЕДВИЖИМОСТИ

Г. А. Гордиевич, В. А. Тарасов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается концепция кроссплатформенного приложения в виде чат-бота в Telegram, написанного на Google Script – скриптовом языке, основанном на Java Script, для комфортной интеграции приложений с сервисами Google. Описываются основные этапы создания, обосновываются выбранные технологические решения.

Google App Script, JavaScipt, Telegram, чат-боты.

На сегодняшний день существует несколько систем для автоматизации административных процессов агентств недвижимости. Самые крупные из них – это Metris.pro (рис. 1) и Нмаркет.ПРО (рис. 2, см. ниже).

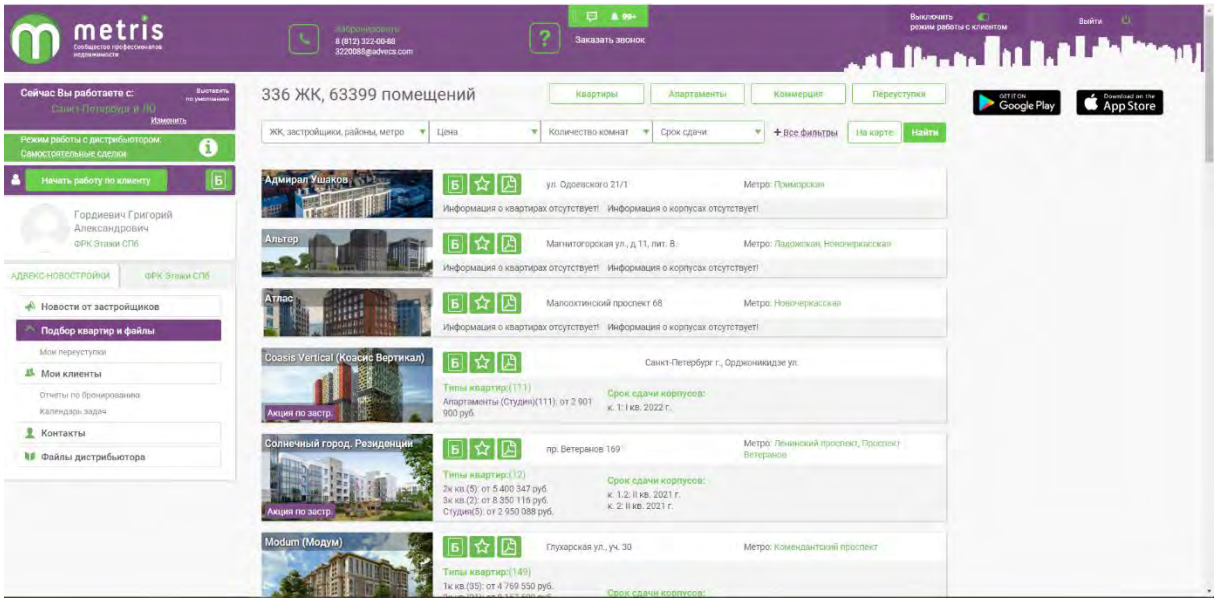


Рис. 1. Стартовая страница Metris.pro

Одни из самых главных недостатков данных систем – это скорость работы, актуальность обновления базы данных по рынку новостроек города Санкт-Петербурга, а также отсутствие полноценных мобильных версий приложений, что в наше время затрудняет работу агентства.

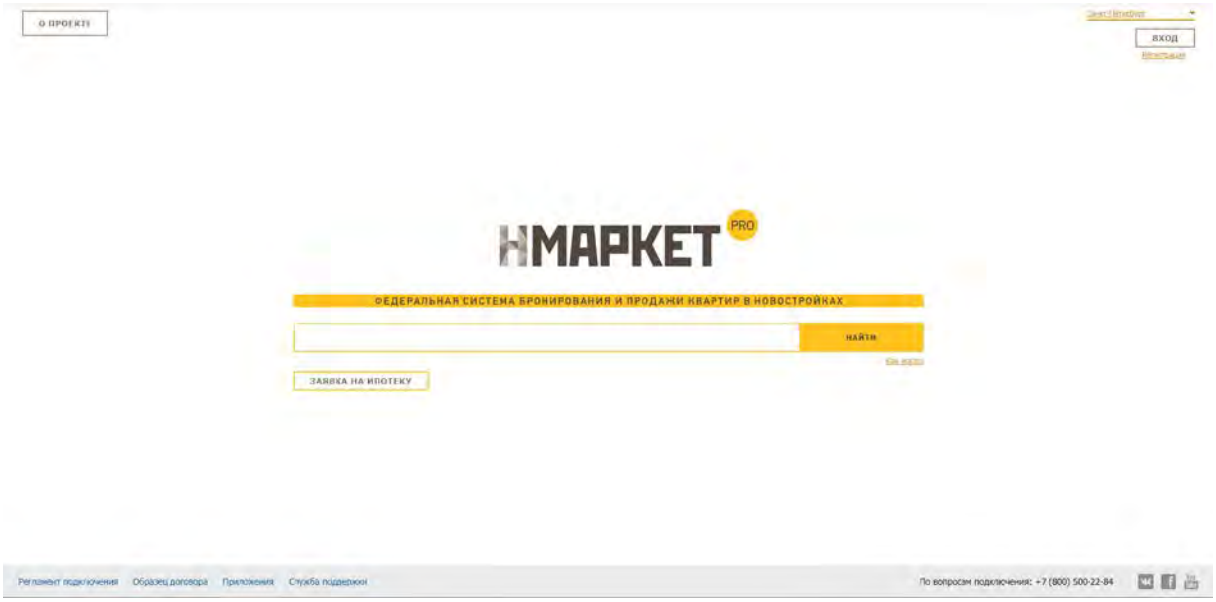


Рис. 2. Стартовая страница Нмаркет.ПРО

Для крупного агентства, которое обрабатывает сотни запросов, очень важно, чтобы сотрудники компании имели постоянный доступ к самой актуальной базе новостроек Санкт-Петербурга, могли получить необходимую информацию с любого удобного для них устройства. В связи с этим выработаны основные критерии нового приложения [1]:

– высокая скорость работы;
– актуальность информационной базы;
– возможности пользоваться как на ПК, так и на смартфонах/планшетах;
– простой и понятный UI/UX-дизайн;
– единый дизайн для любого типа устройства.

Одна из самых важных задач – это обеспечение скорости работы приложения, так как планируется, что на старте будет подключено около 300, а в дальнейшем – более 2 500 пользователей.

Второй вопрос, который также требуется решить – это кроссплатформенность. В настоящее время ни одна компания, оказывающая какие-либо услуги, не может полноценно функционировать без хорошего мобильного приложения, особенно это касается риэлторских услуг.

Так как разработка полноценного кроссплатформенного приложения требует больших затрат и поддержки в целом, выбрано решение, которое сможет в рамках небольшого бюджета решить задачу разработки чат-бота

в Telegram. Основная задача, которая стоит перед ботом – это выдача необходимой информации сотруднику по рынку новостроек Санкт-Петербурга и формирование необходимых запросов.

Платформой для принятия запросов пользователей решено выбрать Telegram. Telegram – кроссплатформенный мессенджер, позволяющий обмениваться сообщениями и медиафайлами многих форматов. Используется проприетарная серверная часть с закрытым кодом, работающая на мощностях нескольких компаний США и Германии, и несколько клиентских с открытым исходным кодом, в том числе, под лицензией GNU GPL. Помимо стандартного обмена сообщениями в диалогах и группах, в мессенджере можно хранить неограниченное количество файлов, вести каналы (микроблоги), создавать и использовать ботов.

Прежде чем начинать разработку, бота необходимо зарегистрировать и получить его уникальный ID, являющийся одновременно и токеном. Для этого в Telegram существует специальный бот – @BotFather. Если написать ему «/start», то выведется список всех его команд. Первая и главная – «/newbot» – после отправки бот просит придумать имя новому боту. Единственное ограничение на имя – оно должно оканчиваться на «bot». В случае успеха BotFather возвращает токен бота и ссылку для быстрого добавления бота в контакты [2]. Для начала работы этого достаточно.

В качестве заготовки создается функция авторизации и базовые кнопки-команды. Авторизация необходима для того, чтобы ботом не мог воспользоваться человек, который не работает в компании. Если телефон сотрудника отсутствует в списке, который есть у бота, то будет выдаваться ошибка (рис. 3, см. ниже).

Актуальная база данных со списком действующих сотрудников должна выгружаться боту в формате csv.

Так как требуется обработка документов в определенном формате, а Telegram-бот не может обрабатывать документы в исходном формате, то для обработки запросов необходимо использовать специально разработанный для этих случаев – Google App Script.

Apps Script – это скриптовая платформа, разработанная Google для создания легких приложений на платформе G Suite. Google Apps Script изначально разрабатывался Майком Хармом в качестве стороннего проекта, когда он работал разработчиком в Google. Google Apps Script впервые публично представлен в мае 2009 года [3].

Google Script – это скриптовый язык, основан на JavaScript 1.6 (рис. 4, см. ниже). Почти все базовые функции работают, то есть для решения большинства задач можно брать готовые варианты на Java Script [4]. Google Script – инструмент для работы с надстройками для документов, листов и слайдов Google.

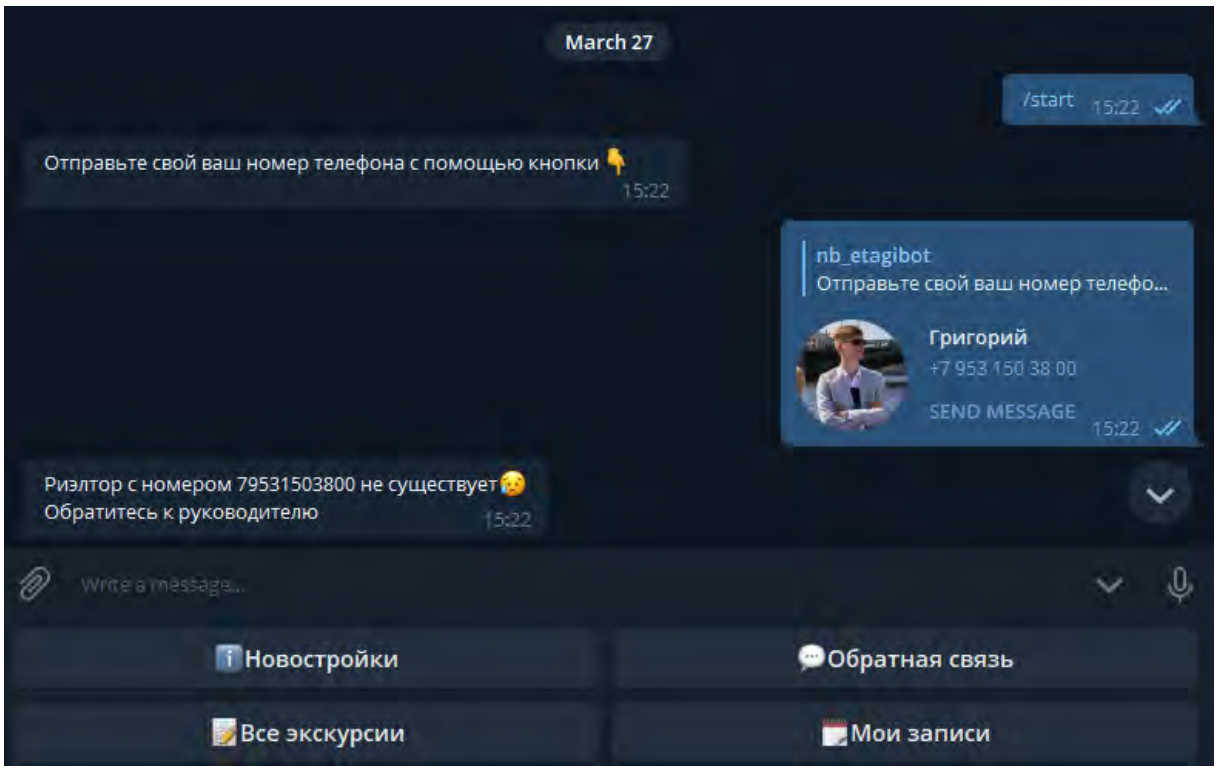


Рис. 3. Регистрация нового бота в Telegram

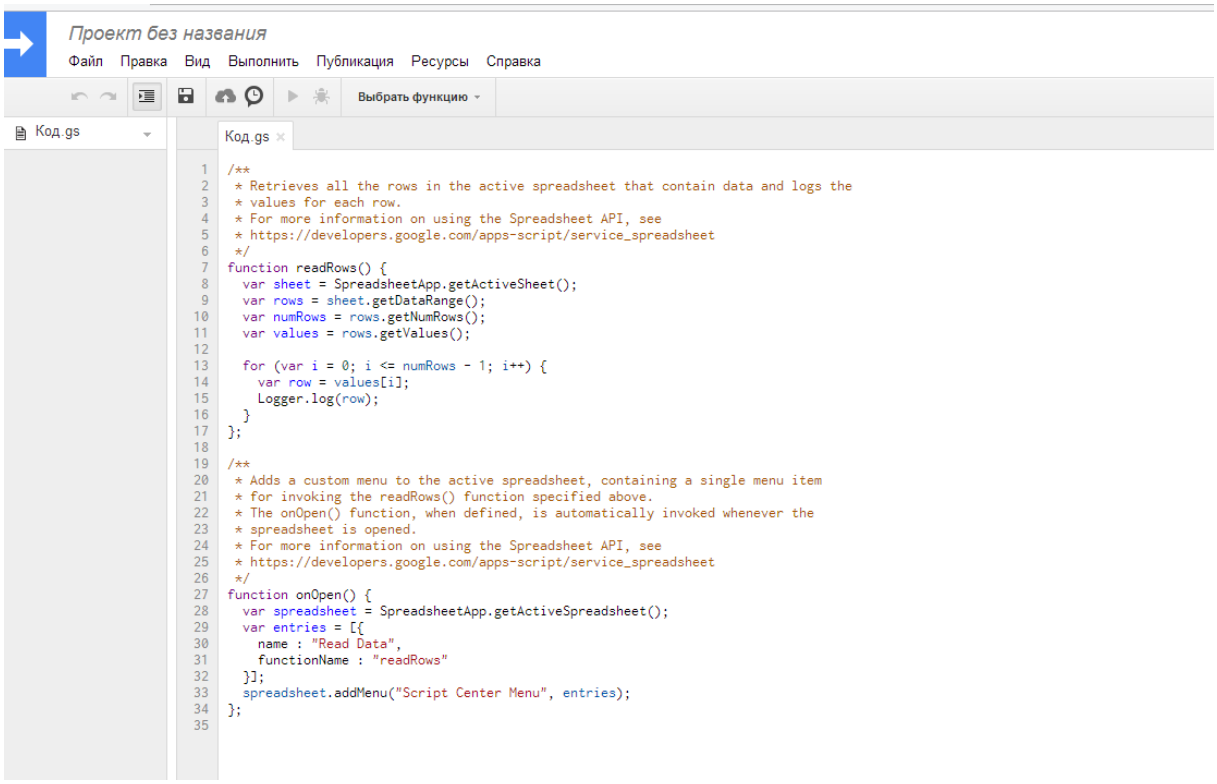


Рис. 4. Пример кода Google Script

Выбор данного языка обусловлен тем, что компания, для которой разрабатывается данная концепция, активно использует в своей работе сервисы

компании Google. Также Google Script не требует покупки никаких дополнительных программ, что при малом бюджете проекта играет немаловажную роль.

Список используемых источников

1. Projectimo. Отличия концепции от устава проекта [Электронный ресурс]. URL: http://projectimo.ru/iniciaciya-proekta/koncepciya-proekta.html (дата обращения: 25.03.2020).

2. Хабр. Инструкция: Как создавать ботов в Telegram [Электронный ресурс]. URL: https://habr.com/ru/post/262247/ (дата обращения: 29.03.2020).

3. NETPEAK.BLOG. Google Apps Script: полезные функции и фишки для SEO (часть первая) [Электронный ресурс]. URL: https://netpeak.net/ru/blog/google-apps-script-poleznyye-funktsii-i-fishki-dlya-seo-chast-pervaya/ (дата обращения: 25.03.2020).

4. Хакер. Пишем скрипты для автоматизации работы с приложениями Google [Электронный ресурс]. URL: https://xakep.ru/2015/01/08/google-apps-script/ (дата обращения: 28.03.2020).

Статья представлена заведующим кафедрой ИУС СПбГУТ, доктором технических наук, профессором Л. К. Птицыной.

УДК 681.3; 654.1; 004.93
ГРНТИ 49.01.21; 50.45.29; 50.51.03

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ ПРОЦЕССАМИ ОБРАБОТКИ ДАННЫХ ДЗЗ ИНФРАСТРУКТУРЫ СВЯЗИ

Е. В. Григорьева, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Анализируются существующие процессы организации сбора и обработки данных дистанционного зондирования Земли (ДЗЗ) на основе типовых системотехнических решений и средств применительно к бизнес-процессам предприятий связи и топологическим объектам инфраструктуры связи. Рассматриваются типовые методики обработки данных ДЗЗ. Исследуется возможность распределенной актуализации пространственных данных о топологических объектов инфраструктуры связи под текущие задачи бизнес-процессов предприятий связи с целью снижении материальных и временных затрат.

линейные объекты связи, автоматизация мониторинга, пространственные данные, дистанционное зондирование Земли, обработка данных.

Основными направлениями исследований автоматизации предприятий связи в условиях реализации программы «Цифровая экономика Российской Федерации» в отрасли «Связь» относятся:

– сбор и обработка данных о характеристиках топологических (линейных и стационарных) объектах предприятия связи и их актуализация;

– внедрение информационных технологий обработки данных дистанционного зондирования Земли (ДЗЗ) о топологических объектах предприятий связи;

– адаптация процедур обработки данных о топологических объектах связи под текущие требования к временным и материальным затратам и условия их сбора.

В соответствии с действующими правовыми и нормативными документами Российской Федерации (например, ФЗ «О связи» № 126-ФЗ в ред. 06.06.2019, Градостроительный Кодекс Российской Федерации № 190-ФЗ в ред.27.12.2019) к сооружениям связи относят объекты инженерной инфраструктуры, в том числе линейно-кабельные сооружения связи, созданные или приспособленные для размещения средств связи, кабелей связи (см. рис. 1), а к линейным объектам связи – линии связи, в том числе линейно-кабельные сооружения, различных классов и категорий, с полосами отвода и охранных зон.

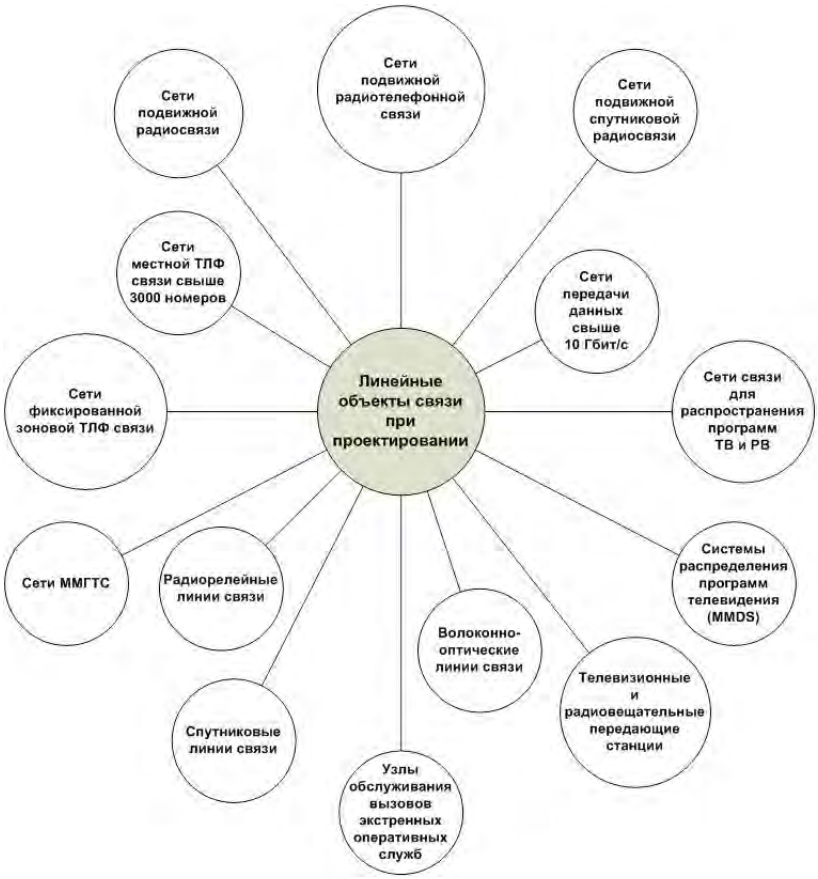


Рис. 1. Совокупность линейных объектов связи [1]

Традиционно используемые системы сбора данных дистанционного зондирования Земли основаны на космических (спутниковых), самолетных (летно-подъемных) и наземных средствах, обобщенные характеристики которых приведены в таблице 1, а оценка уровня их применимости для бизнес-процессов предприятий связи [2] – на рис. 2).

ТАБЛИЦА 1. Характеристики систем сбора данных ДЗЗ

Системы сбора данных ДЗЗ	Мобильность	Опера-тивность	Способ передачи данных	Качество выходных данных	Стоимость
Космические	Орбиталь-ность	Системы привязки	Симплекс, по сеансам	Определено КА	Очень вы-сокая
Самолетные	Средняя	Полетные задания	Дуплекс, непрерывно	Высокое	Средняя
Низколетные	Высокая	Полетные задания	Симплекс, дуплекс, после по-садки	Очень высокое	Низкая
Наземные	Средняя	Высокая	Непрерывно	Высокое	Низкая

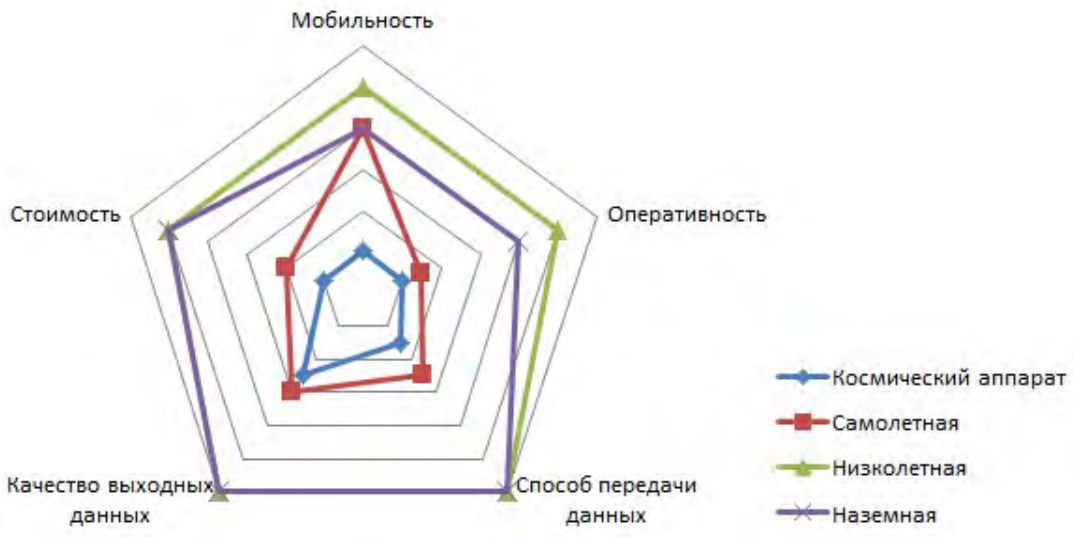


Рис. 2. Оценка уровня применимости систем для бизнес-процессов предприятия связи

Для информационного обеспечения текущих бизнес-процессов предприятий связи целесообразно использовать актуальные пространственные данные, которые могут быть получены по результатам аэрофотосъемки с применением низколетных средств, например, беспилотных летательных аппаратов (БПЛА).

Полевые работы сбора данных ДЗЗ с БПЛА определяются полетным заданием, которое разрабатывается с учетом требований к организации

сбора данных (рис. 3) и технических возможностей БПЛА (например, характеристики комплекса «МАРС-3" представлены в таблице 2).

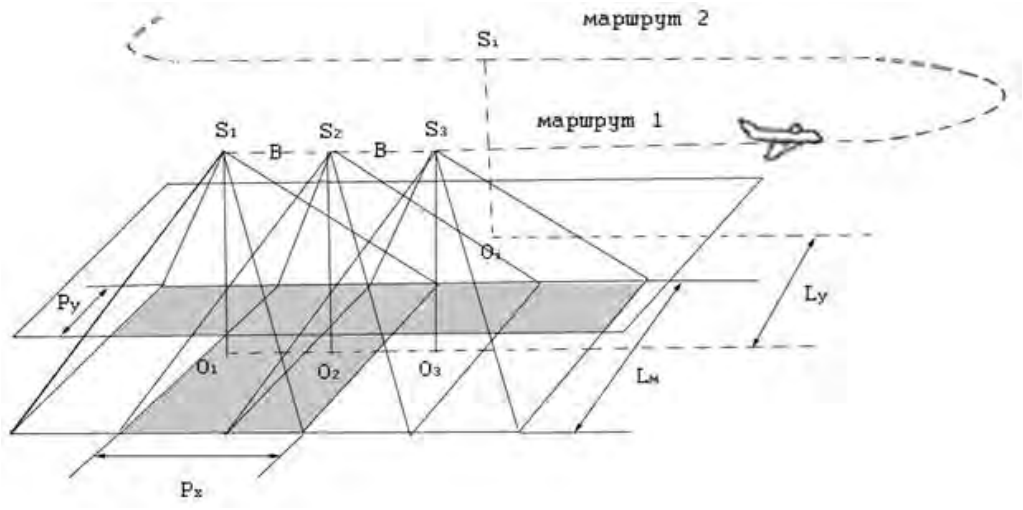


Рис. 3. Полетное здание сбора данных ДЗЗ с БПЛА [3]

ТАБЛИЦА 2. Характеристики комплекса «МАРС-3»

Тип	Летающее крыло
Продолжительность полета, ч	2
Взлетный вес, кг	4,5
Размах крыла, м	2,12
Дальность действия, км	30
Полезная нагрузка, кг	0,5
Крейсерская скорость полета, км/ч	75
Максимальная скорость полета, км/ч	100
Максимальная высота полета, м	1 000
Система взлета	Катапульта
Система посадки	Классическая на фюзеляж

Результаты сбора данных ДЗЗ с БПЛА представлены на рис. 4.

Рис. 5. Аэрофотоснимки ДЗЗ с БПЛА типа «МАРС-3»

Для обработки данных ДЗЗ с БПЛА целесообразно использовать существующее конкурентоспособное программное обеспечение (например, [4, 5, 6]), характеристики которого приведены в таблице 3.

ТАБЛИЦА 3. Характеристики средств обработки данных ДЗЗ

Программа	Разработчик	Функциональные характеристики	Условия применения	Стоимость, тыс. руб.
Agisoft Metashape	Россия	Обработка изображений преобразование в облака точек, полигоны, орто-фотопланы, цифровые модели местности.	Наличие бесплатной 30-дневной версии	От 235,0
ScanEx Image Processor	Россия	Пакетная обработка растровых данных; импорт/экспорт и визуализация данных; коррекция, преобразование; 3D моделирование и др.	Наличие бесплатной 30-дневной версии по запросу	От 45,0
PHOTOMOD UAS	Россия	Обработка и получение фотограмметрических продуктов: ЦМР, 3D-векторы, ортофотопланы.	Наличие бесплатной 30-дневной усеченной версии	От 199,0

При обработке программными средствами всего массива полученных данных ДЗЗ с БПЛА формируется цифровая модель местности с выдачей дополнительных результатов, которые формируют актуальный массив пространственных данных в базе данных предприятия связи (см. рис. 6). Однако для оперативной актуализации данных о состоянии топологических объектов связи он является избыточным и затратным по временным и ресурсным показателям.

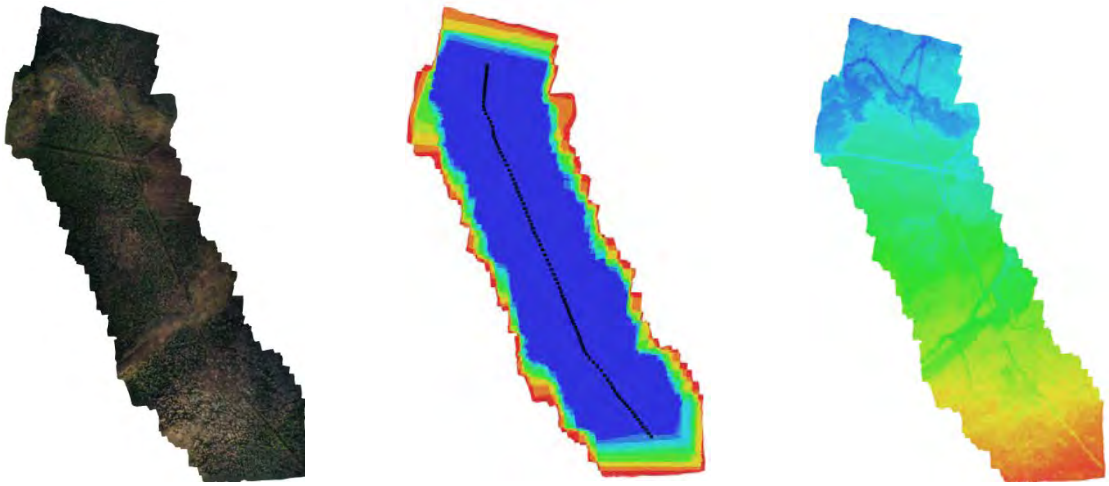


Рис. 6. Результаты обработки ДЗЗ с БПЛА типа «МАРС-3»

Для таких задач целесообразно первоначально применять способ просеивания массива исходных данных при обработке, а на последующих этапах - формировать цифровую модель местности.

Рис. 7. Результат типовой обработки

Рис. 8. Результат обработки с просеиванием

Внедрение предложенного способа обработки ДЗЗ с БПЛА обеспечит:

– упрощение организации сбора, обработки и актуализации данных о характеристиках топологических (линейных и стационарных) объектах предприятия связи;

– снижение финансовых и материальных затрат на применение информационных технологий обработки данных ДЗЗ о топологических объектах предприятий связи, за счет БПЛА;

– снижение временных затрат на обработку и актуализацию данных о топологических объектах связи, за счет адаптации процедур под текущие условия сбора данных.

Список используемых источников

1. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб. : ГУАП, 2016. 325 с.

2. ГОСТ Р 53633.0-2009. Информационные технологии (ИТ). Сеть управления электросвязью. Расширенная схема деятельности организации связи (eTOM). Общая структура бизнес-процессов.

3. Ашихмин А. Расчет параметров аэрофотосъемки беспилотным летательным аппаратом [Электронный ресурс]. URL: https://pandia.ru/text/77/416/94994.php (дата обращения: 17.02.2020).

4. Agisoft Metashape Professional [Электронный ресурс]. URL: https://www.geoscan.aero/ru/software/agisoft/metashape_pro#buy-licenses (дата обращения: 17.02.2020).

5. ScanEx Image Processor, BOX [Электронный ресурс]. URL: https://www.nps.ru/catalog/prikladnoe-po/58078/ (дата обращения: 17.02.2020).

6. ПО Photomod UAS для постобработки GNSS измерений [Электронный ресурс]. URL: https://www.aspector.ru/product/po-photomod-uas-dlya-postobrabotki-gnss-izmereniy/ (дата обращения: 17.02.2020).

УДК 004.94
ГРНТИ 28.17.33

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ ВИРТУАЛЬНОЙ И ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

В. В. Громов, М. В. Серова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С постоянным развитием компьютерного зрения и экспоненциальным ростом вычислительной мощности компьютеров технологии дополненной реальности (Augmented Reality) и виртуальной реальности (Virtual Reality) становятся все более и более заметными. Из-за некоторого совпадения в приложениях и функциях дополненной и виртуальной реальности иногда эти термины путаются или используются неправильно. Эта статья определит AR и VR и объяснит основные различия между ними.

виртуальная реальность, дополненная реальность, гарнитуры, устройства VR, устройства AR.

Благодаря более быстрым и мощным процессорам и компьютерам, более совершенным графическим картам, датчикам и камерам, более быстрым соединениям с Интернетом и инновациям в области разработки программного обеспечения, открылись бесчисленные новые возможности для VR и AR как в частном, так и в промышленном секторах.

VR-гарнитуры полностью захватывают зрение пользователя, чтобы создать впечатление, что он находится в виртуальном пространстве. HTC Vive, Oculus Rift и другие гарнитуры являются полностью непрозрачными,

блокируют внешнюю среду пользователя. Однако, когда гарнитура включается, ЖК-панели или OLED-панели внутри преломляются линзами, чтобы полностью заполнить поле зрения пользователя виртуальным изображением. Это может быть игра, видео на 360 градусов или просто виртуальное пространство.

Большинство гарнитур VR, таких как Rift, Vive, PlayStation VR и Windows Mixed Reality, используют отслеживание движения с шестью степенями свободы (6DOF) благодаря внешним датчикам или камерам (для Rift, Vive и PS VR) или камеры наружу (для WMR). Это означает, что гарнитура не только определяет направление, в котором находится пользователь, но и любое движение, которое он делает в этих направлениях. Это в сочетании с контроллерами движения 6DOF (*6 Degrees of Freedom*) позволяет перемещаться в виртуальном пространстве виртуальными руками. Пространство обычно ограничено несколькими квадратными метрами. Недостатком является то, что пользователь должен быть осторожен, чтобы не споткнуться о любой кабель, который подключает гарнитуру к компьютеру или игровой системе.

Мобильные гарнитуры, такие как Google Daydream View, и автономные VR-гарнитуры, такие как Oculus Go, менее мощные, чем проводные VR-гарнитуры, поскольку они полагаются на обработку на уровне смартфона. Они также обычно предлагают только три степени свободы (3DOF), что означает, что они только отслеживают направление, а не движение в пространстве. У таких гарнитур обычно только один контроллер движения 3DOF (*3 Degrees of Freedom*), который является удаленным или предназначен для работы с более стандартными геймпадами. Возможности пользователя подобны, но не обеспечивают полного погружения в виртуальную реальность.

Как для игр, так и для приложений виртуальная реальность полностью изменяет окружение пользователя, создавая новое виртуальное пространство с заданными параметрами. Физическое местонахождение пользователя не имеет значения. Игры VR дают возможность сидеть в кабине истребителя, приложения – виртуально путешествовать по отдаленным местам.

В то время как виртуальная реальность заменяет видение пользователя, дополненная реальность добавляет в него какие-либо компоненты. Устройства AR, такие как Microsoft HoloLens и различные «умные очки» корпоративного уровня, прозрачны, что позволяет видеть все перед собой, как будто пользователь носит пару солнцезащитных очков. Технология разработана для абсолютно свободного движения при проецировании на любую поверхность. Концепция распространяется на смартфоны с приложениями AR и играми, такими как Pokemon Go, которые используют камеру телефона для отслеживания окружения и наложения дополнительной информации поверх него на экране [1].

AR-дисплеи могут выполнять наложение данных, с указанием времени, а также могут создавать новые голограммы виртуальной реальности с заданными параметрами.

Pokemon Go проецирует покемона на экран телефона поверх того, на что смотрит камера. Тем временем HoloLens и другие умные очки, такие как Magic Leap One, позволяют виртуально размещать плавающие окна приложений и 3D-украшения вокруг пользователя.

Технология дополненной реальности имеет явный недостаток по сравнению с виртуальной реальностью: визуальное погружение. В то время как VR полностью покрывает и заменяет поле зрения пользователя, приложения AR отображаются только на экране смартфона или планшета, и даже HoloLens может проецировать изображения только в ограниченной области зрения пользователя [2].

Базовой AR-гарнитуре, которая совмещает объект пользователя с параметрами объекта исследования, достаточно 3DOF контроллеров. Однако большинству приложений AR требуются дополнительные контроллеры, отслеживающие физическое положение, чтобы программное обеспечение могло поддерживать соответствующие положения для изображений, которые оно проецирует в трехмерном пространстве. Вот почему HoloLens использует стереоскопическую камеру и расширенное распознавание образов, чтобы определить, где находится устройство, и почему более совершенные AR-ориентированные смартфоны, такие как iPhone X, используют несколько камер, расположенных сзади, для отслеживания глубины.

Для приложений дополненная реальность имеет почти безграничные возможности. Программное обеспечение AR для мобильных устройств распознает окружение и предоставляет дополнительную информацию о том, что оно видит, предлагая мгновенный перевод текста или всплывающие обзоры ресторанов.

Для игр дополненная реальность может создавать приключения, используя окружение пользователя. Детективная игра «Fragments» сканирует комнату и создает сцены преступлений, основываясь на ее макете, размещая различные фрагменты вокруг и создавая разные испытания в каждой комнате. «RoboRaid» обнаруживает, где находятся стены, и проецирует голограммы роботов, прорывающихся сквозь них. «Young Conker» ставит препятствия по всей мебели. Во всех этих случаях игры изменяются, чтобы соответствовать пространству.

Виртуальная реальность и дополненная реальность выполняют две совершенно разные функции двумя совершенно разными способами, несмотря на схожие конструкции самих устройств. VR заменяет реальность, перенося пользователя в другое место, в то время как AR добавляет виртуальные компоненты к реальности, проецируя информацию поверх того, что

пользователь уже видит. Это мощные технологии, которые могут полностью изменить то, как мы будем использовать компьютеры в будущем.

Список используемых источников

1. Mangold M. The difference between virtual reality (VR) and augmented reality (AR) [Электронный ресурс]. URL: https://magic-holo.com/en/difference-between-virtual-reality-vr-and-augmented-reality-ar/#Unterschied_VR_AR_ausf%C3%BChrlich_erkl%C3%A4rt

2. Brown A. The difference between virtual reality (VR) and augmented reality (AR) [Электронный ресурс]. URL: https://www.khl.com/international-construction/virtual-and-augmented-reality-/136761.article

УДК 004.27
ГРНТИ 20.23.21

МИКРОКОМПЬЮТЕРЫ И ПЕРСПЕКТИВЫ ИХ РАЗВИТИЯ В СОВРЕМЕННОМ УЧЕБНОМ ПРОЦЕССЕ

В. В. Громов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются основные направления развития микрокомпьютерных систем в учебном процессе. Рассматриваются примеры создания информационных систем в учебном процессе на базе микрокомпьютерных систем Raspberry PI. Рассматривается вопрос обучения навыкам администрирования сложных информационных систем на примере использования серверных платформ Raspberry PI и SUSE Linux Enterprise Server.

Рассматривается возможность применения в учебном процессе современных академических программ по использованию современных операционных систем с возможностью построения макетов имитирующих сложные промышленные системы.

микрокомпьютеры, информационные системы.

Моё знакомство с микрокомпьютерами началось в 2016 году, когда мне был подарен первый Raspberry PI, данный компьютер был оснащен процессором Broadcom BCM2835, 700MHz single core ARM1176JZF-S CPU, и имел 1024 MB оперативной памяти, работающий на чистоте 400 МГц. Данный компьютер использовался мною в цикле лекций по программе «Информатика» для ознакомления студентов с возможностью операционной системы Linux и применения данных компьютеров в режиме промышленной эксплуатации (см. рис.).

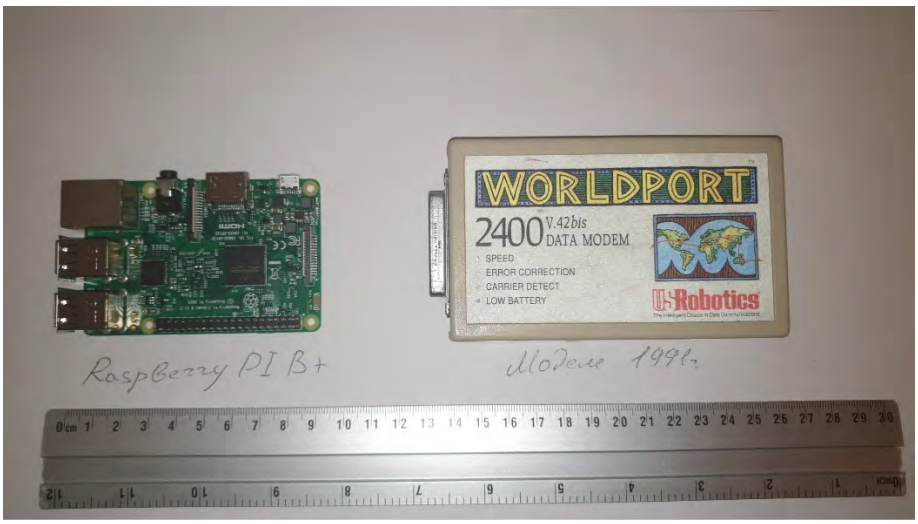


Рис. Микрокомпьютер Raspberry PI и модем 1989 года выпуска

На рис. наглядно продемонстрирован современный микрокомпьютер и модем 1989 года выпуска. Данная фотография демонстрирует преимущества современных технологий и позволяет с уверенностью сказать, что применение микрокомпьютеров может значительно снизить затраты на электропитание информационных систем, а также улучшить процесс обучения современных студентов.

Следует отметить, что данные микрокомпьютеры были созданы для обучения школьников и студентов программированию. В таблице показаны основные параметры современных микрокомпьютеров Raspberry PI.

ТАБЛИЦА. Динамика развития микрокомпьютеров Raspberry PI

Дата выхода	Микроархитектура	Частота	Ядер	ОЗУ	USB	Ethernet	Цена
2012	ARM1176JZ-F	700 МГц	1	512 МБ	2 порта	есть	$35
2014	ARM1176JZ-F	700 МГц	1	512 МБ	4 порта	есть	$25
2015	ARM Cortex-A7	900 МГц	4	1 ГБ	4 порта	есть	$35
2016	Cortex-A53 (ARM v8)	1,2 ГГц	4	1 ГБ	4 порта	есть	$35
2018	Cortex-A53 (ARM v8)	1,4 ГГц	4	1 ГБ	4 порта	Gigabit	$35
2019	Cortex-A72 (ARM v8)	1,5 ГГц	4	2,4 ГБ	4 порта	Gigabit	$36

Приведенные параметры наглядно показывают, что не все компьютеры могут быть задействованы в современном учебном процессе. Большинство студентов привыкли работать в операционной системе, имеющей графический интерфейс, используя современные языки объектно-ориентированные программирования.

Изначально, Raspberry PI, был создан для обучения таким языкам программирования как Phyton, C, Assembler. Основной задачей при создании

данного микрокомпьютера была минимальная стоимость изделия, которая должна была быть в пределах от 25$ до 35$. К чести Raspberry Pi Foundation, они справились с данной задачей, а последующее развитие технологий позволило значительно улучшить свойства и возможности данного микрокомпьютера [2].

В нашей стране мало внимания уделяется данным типам компьютеров, основные компьютеры – семейство CISC компьютеров, оснащенных такими операционными системами как Windows или MacOS X.

Указанные компьютеры позволяют работать в (усеченной), специально модернизированной корпорацией Microsoft операционной системе Windows 10, а также в операционных системах семейства Linux. Применение операционной системы Linux на данном типе микрокомпьютеров позволяет значительно расширить возможности использования данного типа компьютеров в учебном процессе.

Формально, возможно создать модель промышленного сервера на базе ОС Linux использующего такие сервисы как:

1. Сетевые службы (сервисы).
   1.1. SAMBA – пакет программ для взаимодействия Linux и Windows сетевых служб.
   1.2. NFS – сетевая файловая система.
   1.3. FTP- file transfer protocol.
   1.4. SMTP/POP3/IMAP – протоколы почтовых систем
   1.5. TCP/IP – сетевые протоколы
   1.6. WEB – серверы Apache, NGINX.
2. Языки программирования – любые языки программирования, которые поддерживает операционная система, установленная на Raspberry Pi, такие как: C/C++, Pascal, Phyton, Assembler, Basic, Fortran, REXX и др.
3. Возможность работы с базами данных использующих язык SQL, noSQL и др.
4. Возможность виртуализации данных.
5. Создание кластерных систем.

Перечисленные возможности позволяют сделать вывод, что данные микрокомпьютеры позволяют значительно сократить расходы на оборудование и эксплуатацию обучающих систем.

В 2018 году, мною был создан на базе микрокомпьютера Raspberry Pi сервер баз данных использующий СУБД PostgreSQL и WEB – серверы Apache и Joomla CMS система для представления данных. Конечно, данный сервер уступает по своим возможностям серверу, оснащенному процессором Intel семейства Athom, Celeron, Xeon и др., но детально возможно изучить возможности создания серверных систем любой сложности.

В основе указанной системы была использована операционная система SUSE Linux Enterprise Server ver.12 SP5. Данная операционная система позволяет установить на данный тип компьютеров любые указанные выше сервисы и языки программирования. Она отличается хорошей устойчивостью и быстродействием для ARM процессоров.

В 2019 году Академическая программа SUSE позволила получить бесплатный доступ доступ к обучению, знаниям и инструментам SUSE с открытым исходным кодом для школ, колледжей, университетов, академических больниц, некоммерческих музеев, библиотек и многого другого [1].

Участвующие участники пользуются рядом преимуществ:

•Обучение - материалы для сертифицированных Linux курсов, как для тренеров, так и для студентов [1].

•Специальный учебный план – кампус-использование этих материалов для обучения студентов преподавателями [1].

•Возможность бесплатного использования продуктов SUSE для образовательных или лабораторных целей [1].

•Льготная программу закупок для покупки продуктов SUSE на нужном уровне поддержки, включая специальные продукты и условия, доступные только по цене для учебных заведений.

•Ресурсы разработки – доступ к инструментам и продуктам для использования в лаборатории, при разработке программного обеспечения или в учебных заведениях.

•Поддержка – доступ к базе знаний, форумам и технической поддержке.

•Корпоративное лицензионное соглашение для образования [1].

В настоящее время я зарегистрировался в данной академической программе, как преподаватель ВУЗа и бесплатно имею доступ к множеству продуктов корпорации Micro Focus для использования их дома и в обучающих целях в Санкт-Петербургском государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. В следующем 2021 г., я постараюсь предоставить развернутый анализ данных по возможности применения операционной системы SUSE Linux Enterprise Server в учебном процессе и её Академической программа SUSE корпорации Micro Focus.

Список используемых источников:

1. Сайт корпорации SUSE (Академическая программа SUSE). URL: https://www.suse.com/academic/ (дата обращения: 29.03.2020).

2. Сайт Raspberry Pi Foundation. URL: https://www.raspberrypi.org (дата обращения: 29.03.2020).

УДК 006.01
ГРНТИ 84.01.01; 84.01.011

ОСНОВНЫЕ ПРОБЛЕМЫ СТАНДАРТИЗАЦИИ В РОССИИ

В. В. Громов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются проблемы введения в действия межгосударственных и национальных стандартов в России, а также возможные варианты внесения изменений в действующие и вновь вводимые стандарты. В данной статье рассматриваются примеры внесения изменений в межгосударственные стандарты, а также анализируется общее состояние системы стандартизации в России.

межгосударственные стандарты, национальные стандарты.

На VIII конференции АПИНО было рассказано о Распоряжением Правительства Российской Федерации от 24 сентября 2012г. №1762-р. регламентирующем переиздание более чем 29 000 стандартов и руководящих документов Росстандарта до 2020 года. Попробуем проанализировать, что изменилось с данного момента по настоящее время?

По нашим оценкам – ничего, а стало значительно хуже.

Рассмотрим подробно, что происходит в Росстандарте:

1. Введены новые нормативные документы регламентирующие деятельность Росстандарта, а именно:

1.1.Приказ от 27 мая 2016 г. № 1730 «Об утверждении порядка свободного доступа к документам, разрабатываемым и применяемым в национальной системе стандартизации».

1.2.Приказ от 1июля 2016 г. № 844 «О совершенствовании системы распространения документов по стандартизации Федерального Агенства по техническому регулированию и метрологии».

2. Согласно п. 5. Приказа № 844 Федеральному бюджетному учреждению «Консультационно-внедренческая фирма в области международной стандартизации и сертификации» (ФБУ «КВФ "Интерстандарт"») (В. А. Русс) представить в Федеральное агентство (Информационно-аналитическое управление) предложения о прекращении эксплуатации автоматизированной информационной системы «Распространение ГОСТ».

Исходя из вышеперечисленных нормативных документов Росстандарт должен обеспечить свободный доступ к документам национальной системы стандартизации, размещенным на официальном сайте Федерального

агентства по техническому регулированию и метрологии в информационно-телекоммуникационной сети «Интернет».

В настоящее время, Росстандарт вывел из эксплуатацию старую автоматизированную систему «Распространение ГОСТ», а в место неё не предоставил ничего, кроме вновь созданной коммерческой системы ФГУП «Стандартинформ». Цены колеблются от 1 000 до 3 000 рублей за единицу издания (стандарт, ТУ, регламент) (рис. 1).

Формально были созданы приказы, которые регламентируют свободный доступ к документам национальной системы стандартизации, но в настоящее время открытого (свободного) доступа к национальным и основополагающим стандартам Российской Федерации нет.

На рис. 1 представлена поисковая система ФГУП «Стандартинформ», которая позволяет сформировать пакет услуг по предоставлению копии национального или основополагающего стандарта.

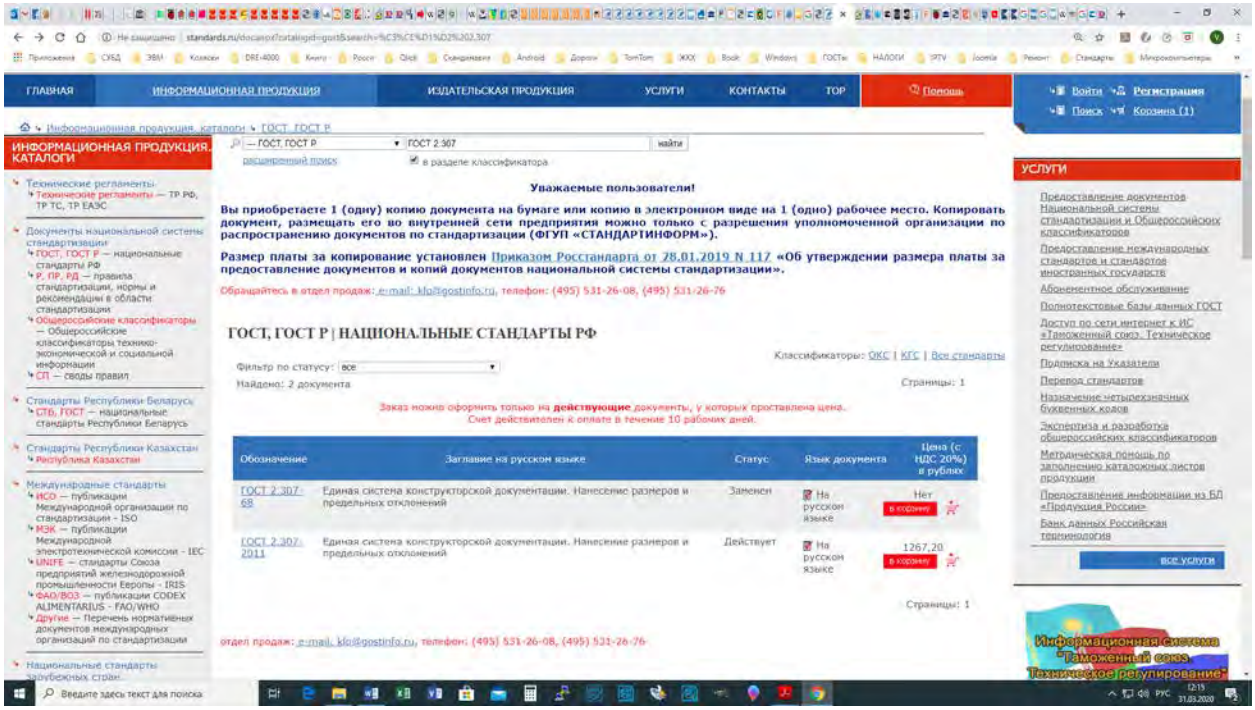


Рис. 1. Поисковая система ФГУП «Стандартинформ»

Как мы видим, стоимость услуг по одному стандарту, достаточна высока, что не позволяет даже профессорско-преподавательскому составу университета проводить закупку необходимой литературы для обучения студентов. Стоимость данных стандартов для юридических лиц не позволяет осуществлять ежегодную подписку по актуальным стандартам.

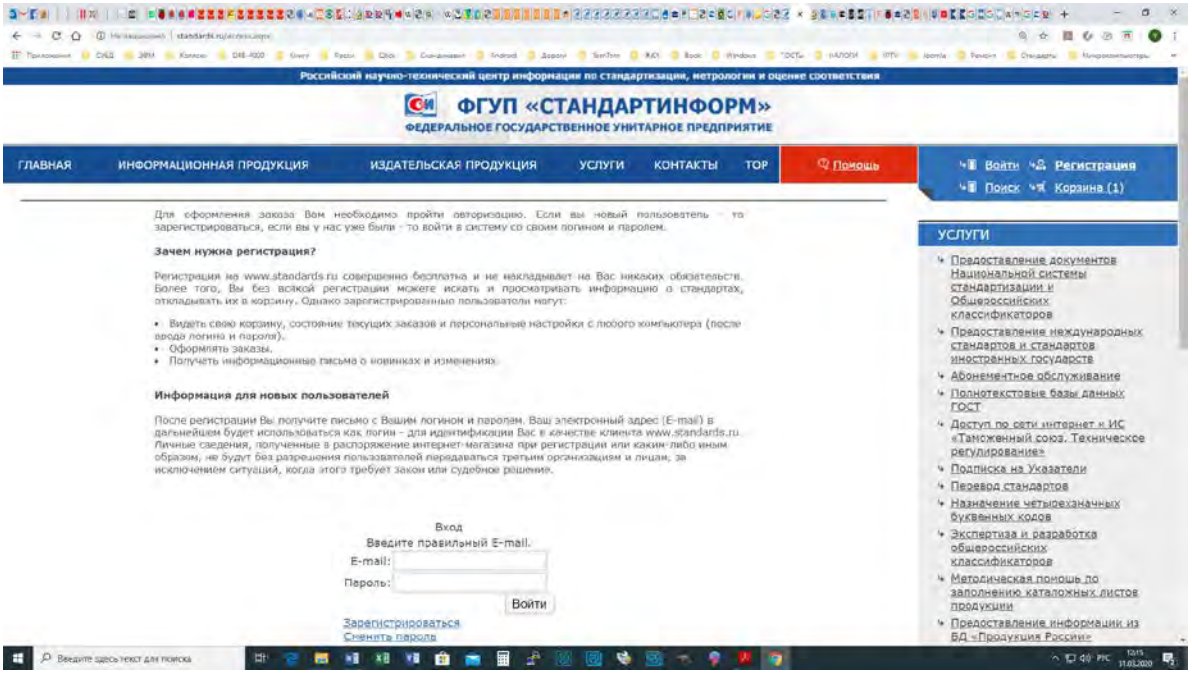


Рис. 2. Окно регистрации

Вместо свободного доступа (рис. 2) предлагается провести регистрацию к национальным и основополагающим стандартам и приобрести копию документа в виде pdf, что противоречит внутренним документам Росстандарта. Мы видим, что создана дополнительная услуга, которая была оценена в некую условную стоимость, для исключения свободного доступа к системе стандартизации Российской Федерации.

Данное ограничение не способствует развитию национальной системы стандартизации, а также не позволяет найти и исправить ошибки в стандартах при их переиздании.

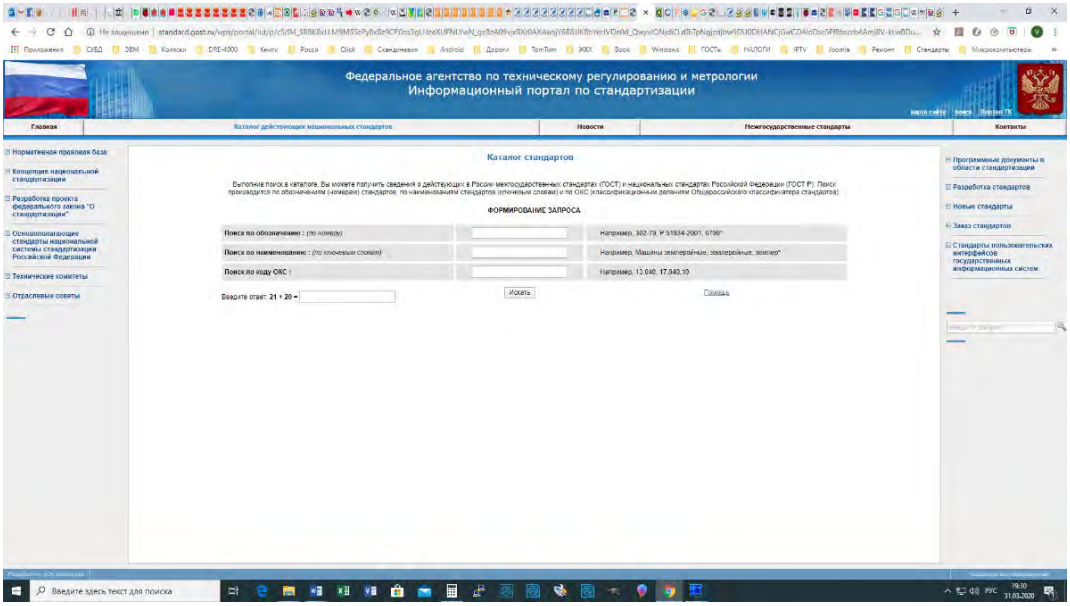


Рис. 3. Автоматизированная система «Распространение ГОСТ»

На рис. 3 (см. выше) представлена автоматизированная система «Распространение ГОСТ», которую разрабатывала «Консультационно-внедренческая фирма в области международной стандартизации и сертификации» (ФБУ «КВФ "Интерстандарт"»).

Данная система поддерживалась до ноября 2019 года, но в последствии большая часть редакционных материалов и фотокопий текстов стандартов и поправок к ним были удалены из базы данных и пользоваться данным ресурсом стало невозможно.

В заключение хотелось бы продемонстрировать, что внутренний ресурс Росстандарта, представленный на рис. 4, не несет никакой информационной нагрузки и не представляет возможность использовать данный ресурс для доступа к основополагающим стандартам.

Вышеизложенные факты позволяют сделать заключение, что система стандартизации претерпела резкие изменения, а вместе с ней и измениться система преподавания дисциплины «Черчение» или «Инженерная и компьютерная графика», а также наша система восприятия стандартов, что в итоге приведет к ухудшению качества образования т. к. свободного доступа к необходимым стандартам у преподавателей нет.

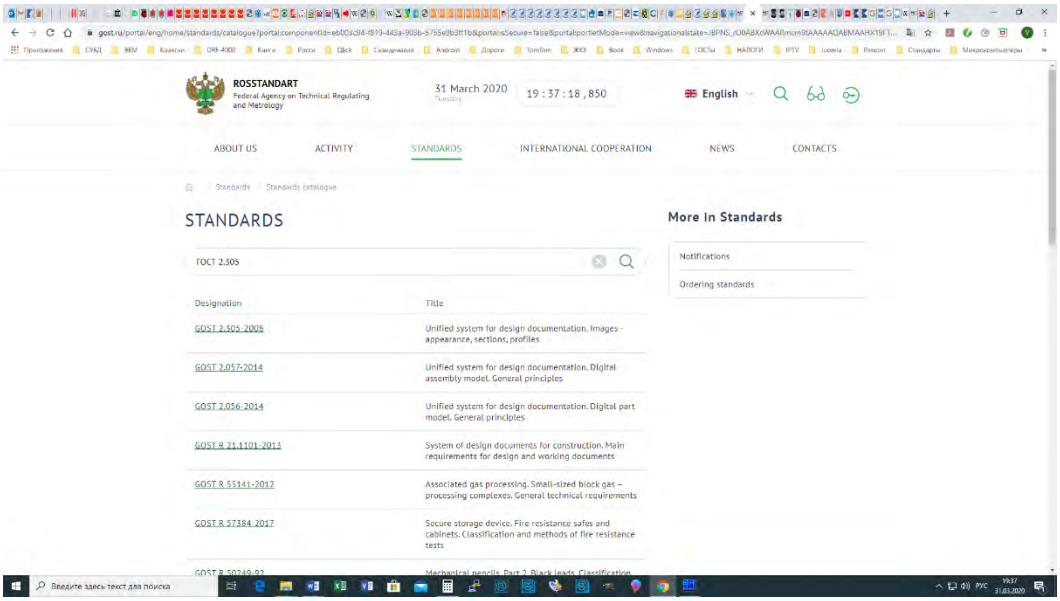


Рис. 4. Внутренний ресурс Росстандарта

Список используемых источников

1. Ежедневное Петербургское сетевое издание "Фонтанка.ру" – общественно-политическое издание. URL: https://www.fontanka.ru/2020/01/30/153/ (дата обращения: 29.03.2020).

2. Ежедневное Петербургское сетевое издание "Фонтанка.ру" – общественно-политическое издание. URL: https://www.fontanka.ru/2020/01/31/153/ (дата обращения: 29.03.2020).

3. ООО «Информационно-рекламное агентство «Карелия.ньюс». URL: https://www.karelia.news/news/2649581/mat-pogibsego-pri-obrusenii-skk-v-sankt-peterburge-rabocego-syn-pogib-na-moih-glazah (дата обращения: 29.03.2020).

4. ИД «Коммерсантъ». URL: https://www.kommersant.ru/doc/4214060 (дата обращения: 29.03.2020).

5. Приказ от 27 мая 2016 г. № 1730 «Об утверждении порядка свободного доступа к документам, разрабатываемым и применяемым в национальной системе стандартизации». URL: http://www.gostinfo.ru/pages/Normrule/directacts/ (дата обращения: 29.03.2020).

6. Приказ от 1 июля 2016 г. №844 «О совершенствовании системы распространения документов по стандартизации Федерального Агенства по техническому регулированию и метрологии». URL: http://www.gostinfo.ru/pages/Normrule/directacts/ (дата обращения: 29.03.2020).

УДК 004.93
ГРНТИ 20.53.19

ИНФОРМАЦИОННАЯ ЭФФЕКТИВНОСТЬ ЦИФРОВЫХ СГЛАЖИВАЮЩИХ ФИЛЬТРОВ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются вопросы оценки информационной эффективности цифровых сглаживающих фильтров. Исследования основаны на анализе изменений энтропии и динамики информационных процессов сглаживания случайных сигналов, а также на понятии колмогоровской сложности информационного объекта и энтропийного потенциала.

информация, интеллектуальный анализ, фильтрация, колмогоровская сложность.

В настоящее время достаточно актуальной является использование информационных оценок в задачах интеллектуального анализа возникновения состояний неопределенности в различного рода системах обработки данных. Причиной возникновения состояний неопределенности при сглаживании случайных сигналов является априорная неопределенность по отношению к характеристикам воздействующих на полезный сигнал помех.

Рассмотрим процесс сглаживания случайных сигналов рекурсивными цифровыми фильтрами [1], которые обеспечивают несмещенное воспроизведение регулярной составляющей входного сигнала и подавление аддитивной стационарной помехи с заданной корреляционной функцией.

Если входной сигнал сглаживающего устройства может принимать n дискретных значений

$$x_i(i = 1, \dots, n)$$

с некоторой вероятностью $P(x)$, то неопределенность состояний x_i выражается энтропией [2]:

$$H_x = -\sum_{k=0}^{n} \mathrm{p}(x_\mathrm{i})\log \mathrm{p}(x_\mathrm{i}).$$

При непрерывном распределении плотности вероятности x степень неопределенности входного сигнала определяется как

$$H_x = -\int_{xmin}^{xmax} \mathrm{p}(x)\log \mathrm{p}(x)dx - \log \varepsilon,$$

где $p(x)$ – плотность вероятности распределения x, а ε – шаг квантования переменной. Первый член последнего выражения

$$h_x = -\int_{xmin}^{xmax} \mathrm{p}(x)\log \mathrm{p}(x)dx$$

представляет собой дифференциальную энтропию, вторая часть выражения определяет значение энтропии, порождаемое шагом квантования сигнала.

В дальнейшем, при оценке количества информации будем использовать только h_x, так как при постоянном шаге квантования его значение не будет влиять на оценку количества информации. Аналогично можно получить выражение для дифференциальной энтропии выходного сигнала y:

$$h_y = -\int_{ymin}^{ymax} p(y)\log p(y)dy.$$

Процесс сглаживания помех и несмещенное воспроизведение полезного сигнала базируется на том, что при определении параметров передаточной функции цифрового фильтра используется априорная информация о характеристиках помех и регулярной составляющей входного и выходного сигналов фильтра. Соотношения между взаимной информацией и условными сложностями при взаимодействии объектов (входной сигнал – цифровой фильтр – выходной сигнал) можно представить в виде следующей схемы [3, 4] (рис.).

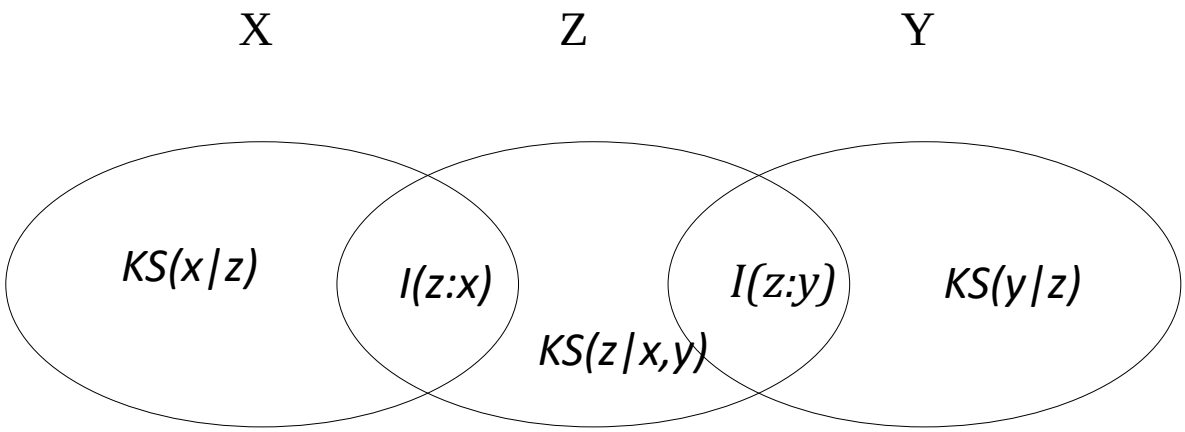


Рис. Общая схема информационного взаимодействия цифрового сглаживающего фильтра (*Z*) с входным (*X*) и выходным (*Y*) сигналами

На рис. область $I(z{:}x)$ представляет количество информации в z о входном сигнале x, которое использовано при реализации и настройке фильтра для обработки этого сигнала. Аналогично определим $I(z{:}y)$ – количество информации в z о выходном сигнале y.

Под $KS(x|z)$ понимается условная простая колмогоровская сложность входного сигнала x при его взаимодействии с цифровым фильтром z. Аналогично определим условную простую колмогоровскую сложность выходного сигнала y – величину $KS(y|z)$.

$KS\ (z\ |x,y)$ – условная колмогоровская сложность цифрового фильтра, определяющего сигнал y при обработке входного сигнала x.

Очевидно, что чем больше априорной информации о параметрах входного сигнала x и подлежащего выделению из помех сигнала y используется при определении параметров цифрового фильтра z, тем эффективнее будет решаться задача сглаживания помехи и выделения полезной составляющей входного сигнала, следовательно тем большие значения $I(z{:}x)$ и $I(z{:}y)$ будут выделены из величины $K(z)$.

Исходя из изложенного, предлагается для оценки эффективности функционирования цифровых сглаживающих фильтров использовать коэффициент информационной эффективности $K_{\text{иэ}}$, значение которого определить следующим соотношением

$$K_{\text{иэ}} = \frac{I(z{:}x)+I(z{:}y)}{KS(z|x,y)}.$$

Сумма $I(z{:}x)+I(z{:}y)$ представляет собой общее количество априорной информации, используемое при определении параметров сглаживающего фильтра. Для определения величины этой суммы используем понятие энтропийного потенциала [5] Δ_e и комплексного энтропийного потенциала L_Δ, причем

$$L_\Delta = \frac{\Delta_\text{e}}{|x_n|} = \frac{K_e\,\sigma}{|x_n|},$$

где σ – среднее квадратичное отклонение для сигнала *x*, K_e – значение энтропийного коэффициента, x_n – величина значения сигнала, на базе которого анализируется его состояние неопределенности.

Значение энтропийного потенциала определяется как половина диапазона равномерного распределения, имеющего такую же энтропию, как и закон распределения наблюдаемого параметра. При этом энтропия случайной величины, распределенная по равномерному закону в интервале $[-\Delta_\text{e}\ ,\ \Delta_\text{e}\ ]$ рассчитывается по формуле:

$$H(x) = \ln(2\Delta_e).$$

Тогда выражение для энтропийного потенциала произвольного закона распределения *x* имеет следующий вид:

$$\Delta_e = \frac{1}{2}e^{H(x)} = \text{К}_e\sigma.$$

Состояние неопределенности для процесса сглаживания случайных сигналов можно охарактеризовать значениями энтропийных потенциалов входного $\Delta_{\text{e}x}$ и выходного $\Delta_{\text{e}y}$ сигналов, а динамику изменения состояния неопределенности – отношением энтропийных потенциалов:

$$\frac{\Delta_{\text{e}x}}{\Delta_{\text{e}y}} = \frac{\frac{1}{2}e^{H(x)}}{\frac{1}{2}e^{H(y)}} = \text{e}^{H(x)-H(\text{y})} = e^{I(x,y)},$$

где *I(x,y)* – количество информации, порожденное процессом сглаживания случайного сигнала *x*.

Далее можно определить

$$I(x,y) = \ln\frac{\Delta_{ex}}{\Delta_{ey}} = ln\frac{K_{ex}\sigma_x}{K_{ey}\sigma_y} = ln\frac{K_{ex}}{K_{ey}} + ln\frac{\sigma_x}{\sigma_y} = I_i + I_p.$$

Под I_i понимается составляющая, величина которой определяется законом распределения вероятностей значений входного и выходного сигналов, а I_p – энергетическая составляющая количества информации [5].

Составляющую I_i при вычислении $K_{\text{иэ}}$ можно исключить, так как эффективность фильтрации оценивается для различных фильтров на примере работы с одинаковыми сигналами.

Таким образом, окончательное выражение для определения информационного коэффициента эффективности фильтра определится как

$$K_{\text{иэ}} = \frac{ln\frac{\sigma_x}{\sigma_y}}{KS(z|x,y)},$$

где условная (относительная) сложность фильтра при наличии информации о характеристиках входного и выходного сигналов может рассматриваться как минимальная длина программы, реализующая алгоритм фильтрации.

Список используемых источников

1. Кузин Л. Т. Расчет и проектирование дискретных систем управления. М. : Машгиз, 1962. 684 с.

2. Николаев В. И. Информационная теория контроля и управления. Л. : Судостроение, 1973. 288 с.

3. Верещагин Н. К., Успенский В. А., Шень А. Колмогоровская сложность и алгоритмическая случайность. М. : МЦНМО, 2013. 576 с.

4. Колмогоров А.Н. Три подхода к определению понятия «Количество информации» // Новое в жизни, науке, технике. Сер. «Математика, кибернетика». 1991. № 1. С. 24–29.

5. Лазарев В. Л., Травина Е. А. Синтез и расчет систем автоматического управления: учеб. Пособие. СПб. : Университет ИТМО, 2018. 34 с.

УДК 004.93
ГРНТИ 28.23.37

РЕАЛИЗАЦИЯ УПРАВЛЯЕМОЙ ПРОЦЕДУРЫ ЛАТЕРАЛЬНОГО ТОРМОЖЕНИЯ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Процедура латерального торможения используется в моделях нейронных сетей, предназначенных для самообучения. Основываясь на правиле «победитель забирает все», функция конкуренции требует больших вычислительных затрат. Предлагается реализация процедуры латерального торможения, существенно упрощающая вычисления и допускающая управление процессом самообучения.

нейронные сети, функция конкуренции, латеральное торможение.

Важной отличительной особенностью нейронных сетей ART (*Adaptive Resonance Theory*) является непрерывное обучение. Сети ART выполняют кластеризацию путем нахождения прототипов и предназначены для решения проблемы стабильности/пластичности, которая является одной из центральных в нейронных сетях. Для ее решения необходимо процесс добавления новой информации в память увязать с процессом анализа ее сходства с уже существующей. Именно это «увязывание» процессов выполняется в сети ART и состоит в том, что осуществляется коррекция запомненной информации с учетом новой.

Подобное непрерывное обучение сети сродни ассоциативной памяти человека, когда каждый входной образец заставляет анализировать целое множество ассоциативных образов. В результате работы ART сети в ее памяти формируются устойчивые наборы образцов, которые представляют ядра кластеров, связанных с определенным «понятием». Тем самым, при подаче произвольного входного вектора сеть отыщет ядро, которое ассоциирует вектора, подобные поданному. Новый образец запоминается, если в этом есть необходимость, для этого должен отсутствовать вектор, однозначно определяющий кластер принадлежности нового образца. Тем самым новые образца запоминаются динамически по мере необходимости, без потери существующих в памяти векторов и без необходимости полного переобучения сети.

Нейронная сеть ART осуществляет кластеризацию входных образцов по категориям, сформированным сетью. Решение о принадлежности входного образца кластеру принимается на основе анализа состояния нейронов распознающего слоя. Если образец близок шаблону черт определенного кластера, то происходит возбуждение одного из нейронов, и образец запоминается в данном кластере. Если отличие образца велико от всех сформированных категорий, то для него формируется новый кластер, который в дальнейшем будет модифицироваться и уточняться другими образами, формируя свой шаблон критических черт. Как следствие, в слое распознавания отводится новый, ранее не задействованный нейрон, для описания новой категории.

Рассмотрим структурную схему нейронной сети ART (рис. 1). Она состоит из двух слоев нейронов – слой распознавания R и слой сравнения C. Эти слои объединены меду собой двумя матрицами синаптических связей W_{ij} и V_{ji}. Связи W_{ij} направлены от слоя C к слою R, а связи V_{ji} – наоборот, от слоя R к слою C. По сути, все обучение сети заключается в формировании значений матрицы синаптических связей W_{ij}, которая по сути представляет из себя адаптивную долгосрочную память LTM (*Long Term Memory*).

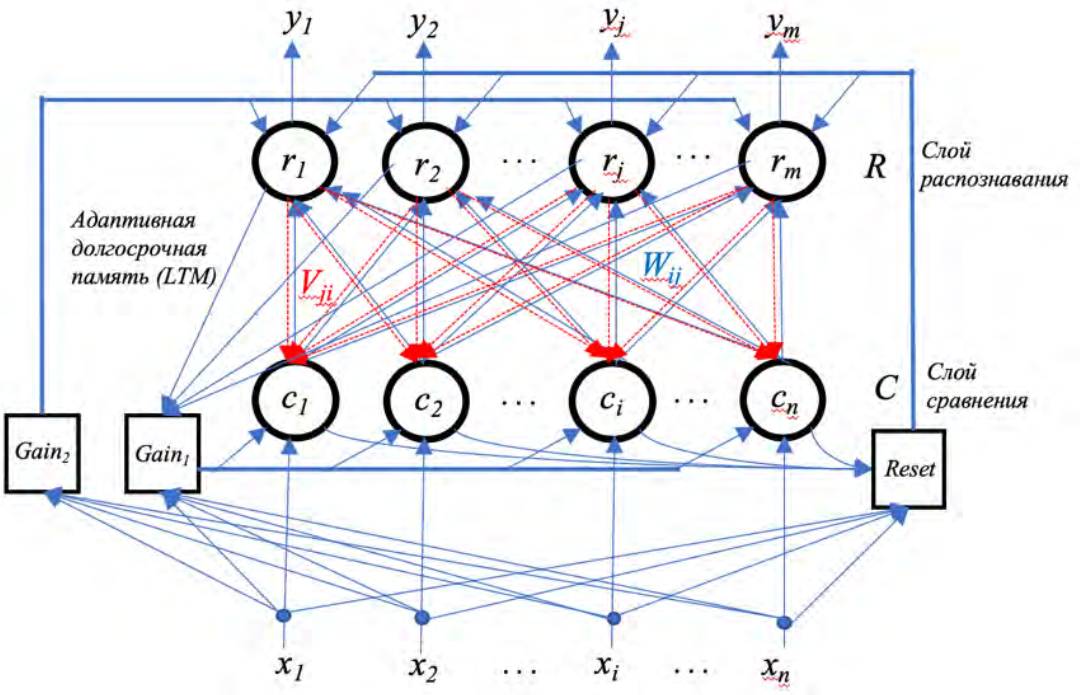


Рис. 1. Структурная схема нейронной сети ART

В отличие от v_{ij}, веса w_{ij} – вещественные, а j-й нейрон слоя распознавания принимает значение в соответствии формулой:

$$r_j = (w_{ij}C)\ AND\ (Gain_2)\ \ AND\ (NOT(Reset_j)),$$

то есть сигнал $Gain_2$ «разрешает» работу слоя распознавания, а сигнал *Reset* позволяет выборочно затормозить любые нейроны в слое.

Нейроны слоя распознавания не содержат нелинейных элементов, но обладают следующей особенностью. Каждый нейрон в слое связан со всеми остальными нейронами этого же слоя обратными тормозящими связями и положительной обратной связью – с самим собой. Такой способ связности называется латеральным торможением. Это приводит к тому, что только один нейрон в слое распознавания может быть активирован. Именно таким образом реализуется алгоритм WTA – «победитель забирает все». Между нейронами существует конкуренция, и нейрон с максимальным выходом «подавляет» все остальные нейроны в слое, выигрывая «состязание». Его выход становится равным единице, а выходы остальных нейронов – нулю.

Эта конкуренция реализуется введением связей с отрицательными весами с выхода каждого нейрона r_j на входы остальных нейронов (рис. 2). Таким образом, чем больший выход имеет нейрон, тем он сильнее тормозит все остальные нейроны в слое. Кроме того, каждый нейрон имеет связь с положительным весом со своего выхода на свой вход, эта обратная связь стремится усилить и поддержать его.

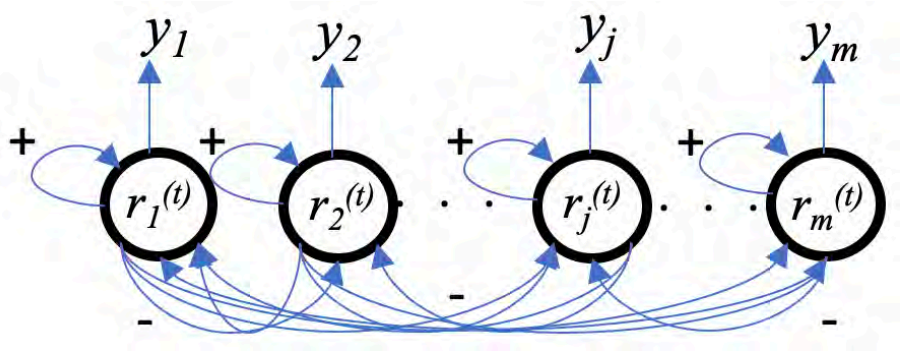


Рис. 2. Слой латерального торможения

Процесс латерального торможения в слое можно описать с помощью диагональной матрицы $L_{m \times m}$ вида:

$$L_{m \times m} = \begin{pmatrix} 1 & \cdots & -\varepsilon \\ \vdots & \ddots & \vdots \\ -\varepsilon & \cdots & 1 \end{pmatrix},$$

где ε – малая случайная величина порядка $1/m$. Вектор $R = (r_1, r_2, \ldots, r_m)^T$ многократно умножается на эту матрицу и при каждой итерации все компоненты вектора, кроме одной, став отрицательными, обнуляются.

Для упрощения описанного процесса предлагается заменить слой латерального торможения структурой, представленной на рис. 3.

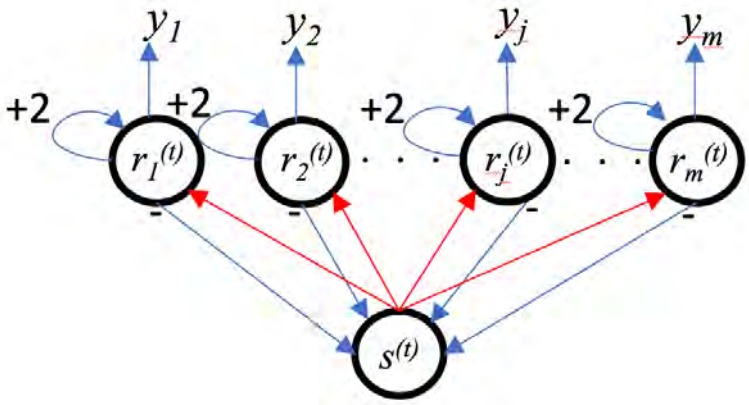


Рис. 3. Схема латерального торможения

Здесь используется дополнительный нейрон, который аккумулирует состояния нейронов слоя. При этом, можно установить произвольные синаптические связи (веса) на входах аккумулирующего нейрона. С учетом коэффициентов ε можно записать:

$$s = \sum_{i=1}^{m} -\varepsilon \times r_i.$$

Состояние аккумулирующего нейрона формируется в виде взвешенной суммы состояний нейронов слоя латерального торможения. Весовой коэффициент выбирается с учетом объема ассоциативной памяти реализуемой нейронной сетью. По сути, аккумулирующий нейрон играет роль амакриновой клетки, получающей сигнал r_i от нейронов слоя латерального торможения и посылающей свое состояние s обратно [2].

Нетрудно заметить, что для компенсации собственного значения состояния r_i, представленного в s, необходимо положительную обратную связь усилить по крайней мере в два раза. На схеме рис. 3 это усиление условно обозначено, как «+2».

Таким образом, предложенная схема позволяет заменить слой латерального торможения одним аккумулирующим нейроном. Число входов данного нейрона совпадает с числом m нейронов слоя и заменяет $m \times (m - 1)$ синаптических связей с отрицательными весами. Итеративное матричное умножение заменяется стандартной активацией одного нейрона.

В заключение следует подчеркнуть, что подобная схема может быть использована везде, где реализуется алгоритм *WTA*, в частности в сетях Кохонена.

Список используемых источников

1. Carpenter G., Grossberg S. A Massively Parallel Architecture for a Self-Organizing Neural Pattern Recognition Machine. Compuer vision, graphics, and image processing 37, 54–115 (1987).

2. Трухина С., Трухин А., Циркин В. Нейрофизиология: физиология сенсорных систем. Учебник для вузов. 2-е изд., испр. и доп. М. : Юрайт, 2020. 459 с.

УДК 004.891.2
ГРНТИ 20.23.17

ТЕХНОЛОГИИ РАЗРАБОТКИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассмотрены сущность, основные понятия, классификация и архитектура интеллектуальных систем поддержки принятия решений (СППР). Проведено исследование методов разработки и проектирования интеллектуальных СППР. Показано,

что будущее интеллектуальных СППР за гибкостью решений, так как ни один из известных подходов (классические модели, машинное обучение, теория игр) не универсален с точки зрения эффективности решения всех типов задач.

интеллектуальные системы поддержки принятия решений, Data Mining, Data collection.

В энциклопедическом словаре [1] дается следующее определение. СППР – это комплекс математических и эвристических методов и моделей, объединенных общей методикой формирования альтернативных решений в организационных системах, определения последствий реализации каждой альтернативы и обоснования выбора наиболее приемлемого решения.

Существует несколько определений *интеллектуальных* систем поддержки принятия решений (ИСППР), которые определяются одним и тем же функционалом. В общем виде, ИСППР – это такая система, которая ассистирует ЛПР в принятии решений, используя инструментарии Data Mining, моделирования и визуализации, обладает дружелюбным интерфейсом, устойчива по качеству, интерактивна и гибка по настройкам.

Цель настоящей работы состоит в исследовании универсальных методов проектирования интеллектуальных систем поддержки принятия решений.

Работа по достижению поставленной цели сводится к решению следующих основных задач:

– исследование и разработка методов автоматизации разработки ИСППР (в том числе, с использованием моделей нейронных сетей);

– исследование и разработка структурных и семантических моделей ИСППР (с использованием языковых и программных средств структуризации информации);

– исследование и разработка методов оценки информационной эффективности ИСППР (с использованием подходов теории информации).

Проектирование интеллектуальных систем поддержки принятия решений требует формализации описания предметной области, что может быть сделано средствами онтологического подхода. При этом необходимо получить модель собственно системы MS (R), в соответствии с принципом последовательного раскрытия неопределенности ранга R.

- $MS(0) = \langle X \rangle$ – нулевой ранг неопределенности системы – множество переменных, существенных для описания системы, то есть совокупность информационных сущностей без информации о причинно-следственных связей между ними.
- $MS(1) = \langle X, G \rangle$ – задает топологию системы. Бинарное множество G задает связи между сущностями.
- $MS(2)$ – структурная модель, которая содержит информацию о типах связей между сущностями (рис. 1).
- $MS(3)$ – полная параметрическая онтологическая модель.

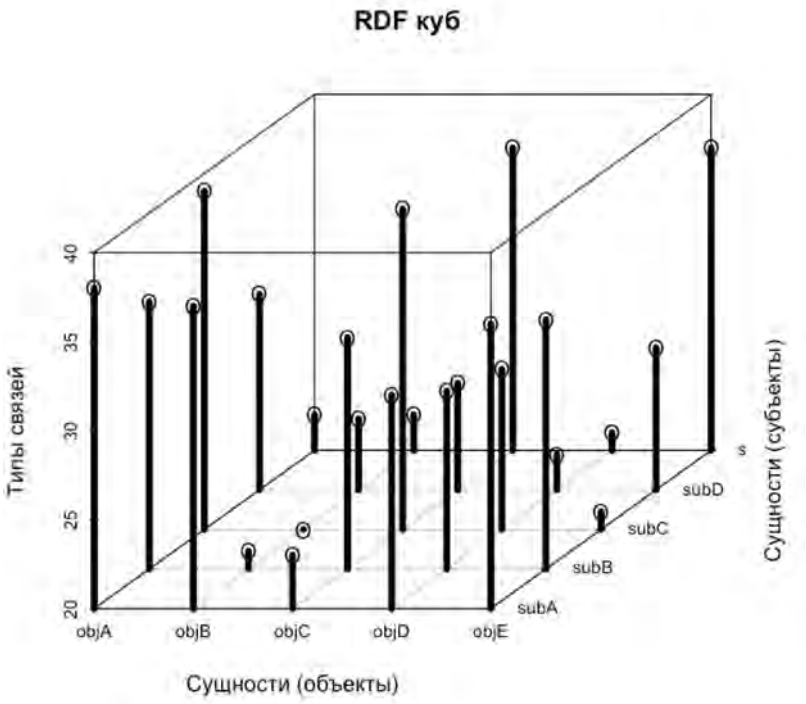


Рис. 1. Структурная модель *MS* (2)

При проектировании реализуется принцип эволюционного развития, при котором сначала формируется топология системы, затем выбираются структуры связей и, наконец, оптимизируются параметры:

$$MS\ (0) \text{ –> } MS\ (1) \text{ –> } MS\ (2) \text{ –> } MS\ (3).$$

Несмотря на многообразие вариантов классификаций, требования и атрибуты ИСППР хорошо ложатся в четыре сегмента: *качество; организация; ограничения; модель*. При этом осуществляются попытки создать некую унифицированную архитектуру ИСППР хотя бы на верхнем уровне. Опыт проектирования показывает, что ИСППР можно разделить на четыре больших слоя [2]:

– пользовательский интерфейс;

– моделирование;

– Data Mining (совокупность методов обнаружения в данных ранее неизвестных, нетривиальных, практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности);

– Data Collection (сбор данных – процесс сбора и измерения информации о целевых переменных в установленной системе, который затем позволяет ответить на соответствующие вопросы и оценить результаты).

Далее в этих слоях можно использовать существующие средства инструментальной поддержки (рис. 2).

Рис. 2. Архитектура ИСППР

В соответствии с предлагаемой концепцией процесс проектирования ИСППР можно разбить на ряд этапов, представленных на рис. 3:

– анализ предметной области;
– сбор данных;
– анализ данных;
– выбор моделей;
– экспертный анализ/интерпретация моделей;
– внедрение моделей;
– оценка ИСППР;
– внедрение ИСППР;
– сбор обратной связи (на каждом этапе).

Таким образом, в работе рассмотрены сущность, основные понятия, классификация и архитектура интеллектуальных систем поддержки принятия решений. Проведено исследование методов разработки и проектирования интеллектуальных СППР. Будущее интеллектуальных СППР за гибкостью решений. Ни один из известных способов (классические модели, машинное обучение, теория игр) не универсален с точки зрения эффективности для решения всех типов задач.

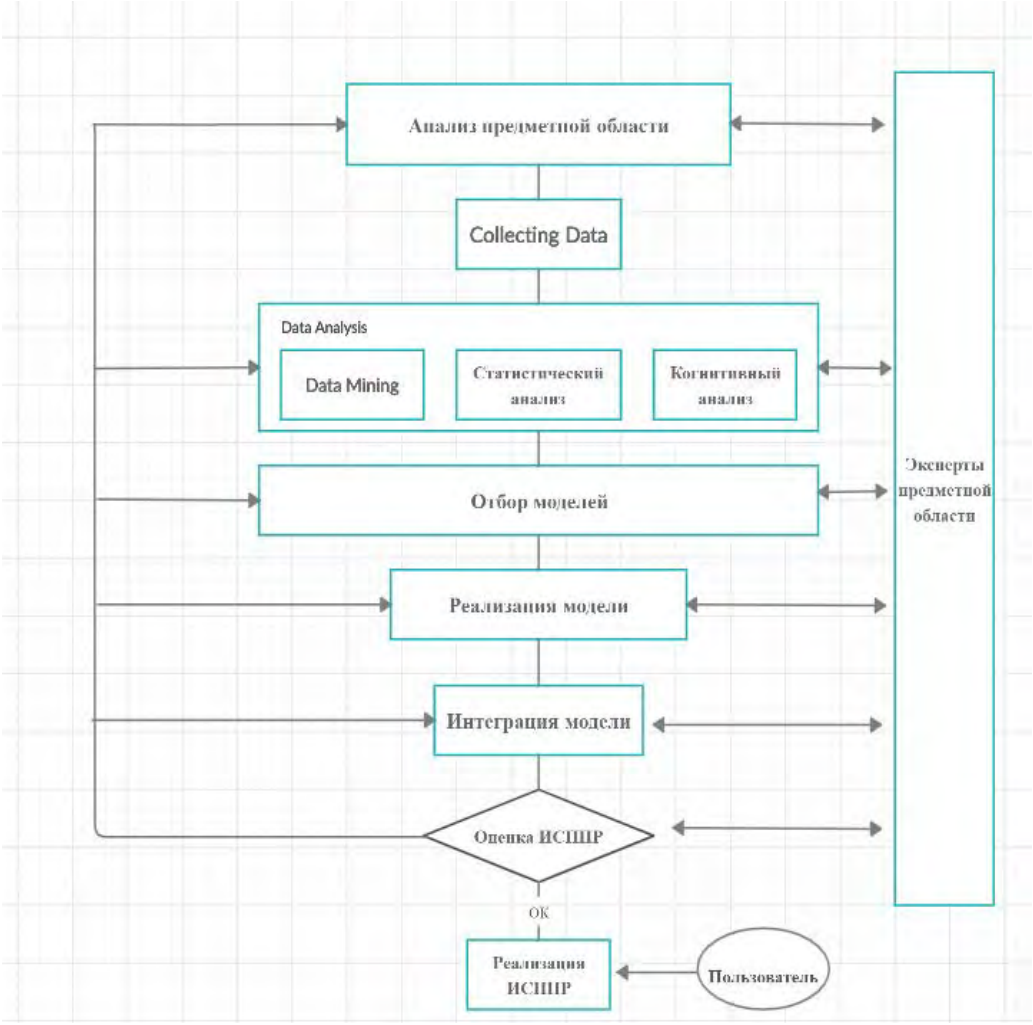


Рис. 3. Этапы разработки ИСППР

В хорошей СППР должны сочетаться различные инструменты, при этом разные модули должны использоваться для разных типов задач и иметь различные интерфейсы вывода для разных категорий пользователей.

Список используемых источников

1. Экономико-математический энциклопедический словарь / Гл. ред. В. И. Данилов-Данильян. М. : Большая Российская энциклопедия: ИНФРА-М, 2003. 688 с. ISBN 5-85270-217-X; ISBN 5-16-000594-3.

2. Интеллектуальные системы поддержки принятия решений – краткий обзор. URL: https://habr.com/ru/company/ods/blog/359188/ (дата обращения: 30.01.2020).

УДК 628.517.2
ГРНТИ 87.55.29

МОНИТОРИНГ АВИАЦИОННОГО ШУМА НА ПРИАЭРОДРОМНОЙ ТЕРРИТОРИИ АЭРОПОРТА ПУЛКОВО

К. В. Гуляева, С. А. Панихидников, Н. В. Сакова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Интенсивное развитие воздушного транспорта увеличивает шумовую нагрузку на территории рядом расположенных городов. В работе рассматривается шумовое загрязнение селитебных территорий, прилегающих к аэропорту Пулково. Оценка шума проводилась в нескольких точках Авиагородка. Представлены данные мониторинга шума, сделан вывод о недопустимых уровнях шума. В работе приведены данные о несовершенстве нормативной базы в области шумового загрязнения.

эквивалентный уровень шума, максимальный уровень шума, авиационный шум.

Среди всех видов физического загрязнения окружающей среды особое место занимает шумовое загрязнение. Повышенный уровень шума отмечается практически во всех крупных городах. Среди всех источников шума на территории городов самый большой вклад в общий уровень вносят все виды транспорта. В Санкт-Петербурге достаточно остро стоит проблема воздействия авиационного шума на отдельные районы в связи с очень близким их расположением от аэропорта Пулково.

В связи с интенсивным развитием воздушного транспорта и увеличением его доступности для населения, люди, живущие на приаэродромный территории и вблизи аэропорта, страдают от шумовой нагрузки. Особенностью авиационного шума является внезапность возникновения, непродолжительность усиления и спада шумового воздействия [1].

Жители домов, расположенных в окрестностях аэропорта, отмечают, что стали нервными, раздражительными. Внезапный шум от пролетающих самолётов нарушает сон: многие не могут долго заснуть или часто просыпаются. Жалобы на ощущение тревоги, страха, на вибрацию дома или посуды предъявляют жители домов, близко расположенных к трассе взлётов и посадок самолётов и к площадкам опробования двигателей. Реакция населения, выявленная опросом, показала, что отношение к одним и тем же уровням авиационного шума различно. Так, днём при уровне шума чуть выше нормы число жалоб составляет 20 %, а ночью при явных превышениях нормы шум беспокоит 80 % населения.

Развитие авиации, увеличение числа полетов приводят к резкому повышению шумовой нагрузки на прилегающие территории. Особую обеспокоенность вызывает тот факт, что по экономическим соображениям большинство вылетов и посадок планируется на вечернее и ночное время, когда люди более чувствительны к повышенному шуму. Увеличение числа полетов также требует постоянного контроля уровня шума на границе санитарно-защитной зоны аэропорта и пересмотра ее при увеличении числа полетов.

Несмотря на то, что постоянно корректируются в сторону ужесточения международные требования к экологическому состоянию приаэродромных территорий, в нашей стране данные требования носят лишь рекомендационный характер. Современная нормативно-методическая база для оценки распространения и влияния практически отсутствует. Система нормирования авиационного шума в РФ не учитывает сложившуюся практику его применения.

Для наглядности ниже приведена таблица 1 сравнение допустимых корректированных уровней авиационного шума по нормативным документам РФ [2, 3, 4].

ТАБЛИЦА 1. Допустимые уровни авиационного шума по нормативным документам РФ

Наименование нормативного документа	*La экв*, дБА		*La max*, дБА	
	День (7:00–23:00)	Ночь (7:00–23:00)	День (7:00–23:00)	Ночь (7:00–23:00)
ГОСТ 22283-2014	55	45	75	65
СН 2.2.4/2.1.8.562-96	55	45	70	60

Объектом исследования данной работы является шумовые загрязнения аэропорта Пулково.

Цель работы: Проведение мониторинга авиационного шума от аэропорта Пулково для получения подтверждения превышения шума, основанного на жалобах и дальнейшем анкетирование жителей Авиагородка (приаэродромной территории). В процессе работы проводились измерения шума от Airbus 320, мониторинг осуществлялся с помощью прибора DT-8851. Составлена карта-схема с точками мониторинга.

Чтобы результаты измерения авиационного шума были максимально объективными, их проводят, делая серию замеров несколько раз в сутки, в контурах проектируемой застройки поблизости аэропорта и маршрутов полета воздушных судов. Включают приборы измерения шума обязательно, как в дневное, так и в ночное время суток, выбирая часы наиболее интенсивного функционирования аэропорта.

Для исследования проводились измерения шума в 7 точках вдоль взлетно-посадочной полосы (ВПП) шумомером «DT-8851» в целях оценки распространения зон влияния авиационного шума. Все выбранные точки находились за пределами санитарно-защитной зоны аэропорта. Мониторинг длился неделю, учитывая все требования по его проведению. По результатам измерений были проведены соответствующие расчеты эквивалентного уровня звука [2].

Расчет проводился по ГОСТ 22283-14. Шум авиационный. Допустимые уровни шума на территории жилой застройки и методы его измерения, использовалась методика № 1 представленная ниже.

$$L_{A_{\text{экв}}} = 10 \lg \left[\frac{1}{T} \sum_{i=0}^{N} \left(\tau_{\text{эф}_i} \cdot 10^{0,1 L_{A_i}} \right) \right], \quad (1)$$

где T – регламентируемый интервал времени, равный 57 600 с для дневного времени (с 7.00 до 23.00 ч) и 28800 с для ночного времени (с 23.00 до 7.00 ч); N – число воздействий за рассматриваемый период.

Точками мониторинга, показанными в рис. [5], были выбраны места скопления людей, рекреационные зоны, учебные заведения, поликлиника, офисное здание, аэровокзал.

Из 7-ми точек превышения наблюдались только в 4-х точках.

Рис. Карта-схема точек мониторинга

Точками превышения уровня шума оказались аэровокзал, офисное здание авиакомпании «Россия», школа № 354 и поликлиника. Рассмотрим результаты мониторинга в точке № 4.

По данным недельного мониторинга *La экв*, дБА за дневное время не превышало 53 дБА, однако, в отдельном измерении было отмечено высокое значение максимального уровня шума *La max*, дБ. У показателей *La экв*, дБА (ночь) и *La max*, дБ (ночь) превышения присутствуют по всем нормативным документам.

ТАБЛИЦА 2. Результаты недельного мониторинга в Авиагородке

	La экв, дБА		*La max*, дБА		Примечания
	День (7:00–23:00)	Ночь (7:00–23:00)	День (7:00–23:00)	Ночь (7:00–23:00)	
1 сутки	46	49	73	73	Превышения по *La экв*, дБА День (7:00–23:00) не выявлено.
	53	56	79	80	
	51	54	80	79	
	47	50	75	75	
2 сутки	44	47	72	70	
	49	52	79	76	
	47	50	73	76	
	46	49	73	74	
3 сутки	45	48	74	71	
	49	52	79	75	
	46	49	74	73	
	46	49	74	72	
4 сутки	45	48	72	73	
	47	50	74	74	
	45	48	73	72	
	45	48	73	71	
5 сутки	45	48	72	72	
	50	53	54	76	
	47	50	75	73	
	46	49	73	73	
6 сутки	46	49	74	75	
	53	56	87	73	
	49	52	75	79	
	47	50	77	73	
7 сутки	45	48	72	72	
	51	54	83	74	
	50	53	74	81	

	La экв, дБА		*La max*, дБА		Примечания
	День (7:00–23:00)	Ночь (7:00–23:00)	День (7:00–23:00)	Ночь (7:00–23:00)	
	46	49	75	72	

Обработка результатов мониторинга проводилась в соответствие с [3].

Среднее значение эквивалентного уровня шума определялось по формуле:

$\bar{L}_m$ вычисляют по формуле:

$$\bar{L}_m = 10lg \sum_{i=0}^{n} 10^{0,1-L_i} - 10lgn, \text{дБ(дБА)}, \quad (2)$$

где L_i – *i*-й из измеренных в данной точке октавных/третьоктавных уровней звукового давления, дБ или уровня звука дБА; i = 1,2,3…n, (n-общее количество измерений в данной точке).

При расчете корректированного значения эквивалентного уровня шума учитывалась поправка на происхождение шума 3 дБА.

Средние корректированные значения эквивалентного шума с поправкой на происхождение и максимальные значения уровня шума представлены в таблице 3.

ТАБЛИЦА 3. Средние корректированные значения эквивалентного шума

La экв, дБА		*La max*, дБА		Примечания
День (7:00–23:00)	Ночь (7:00–23:00)	День (7:00–23:00)	Ночь (7:00–23:00)	
51,8	55,4	87	81	Превышение в ночное время

Проводя мониторинг было выявлено, что одним из влияющих факторов на распространение шумового загрязнения является скорость и направление ветра. Так же такой атмосферный фактор как температура, а именно низкая температура влияют на уровень шума, это наблюдается на мониторинге в ночное время суток.

В связи с тем, что точка, для которой представлены результаты мониторинга, лежит за границами санитарно-защитной зоны аэропорта в ходе данной работы была сформулирована задача создания и исследования санитарно-защитной зоны аэропорта Пулково, а так же выявление наиболее эффективных мероприятий по защите от авиационного шума.

Список используемых источников

1. Феоктистова Т. Г., Феоктистова О. Г. Безопасность жизнедеятельности: пособие по выполнению практических работ «Оценка пригодности территории в окрестностях аэропорта к застройке из условий шума». М. : МГТУ ГА, 2004. 29 с.

2. ГОСТ 22283-2014 «Шум авиационный. Допустимые уровни шума на территории жилой застройки и методы его измерения».

3. ГОСТ 23337-2014 «Шум. Методы измерения шума на селитебной территории и в помещениях жилых и общественных зданий».

4. СН 2.2.4/2.1.8.562-96 «Шум на рабочих местах, в помещениях жилых и общественных зданий и на территории жилой застройки».

5. Гуляева К. В. Карта-схема точек мониторинга. [Электронный ресурс]. URL: https://yandex.ru/maps/2/saint-petersburg/?l=sat&ll= 30.292643%2C59.806005&mode =usermaps&source=constructorLink&um=constructor%3Abc9ece7c66a9b10f52e27b659131 ee81d4 ac71842afcba2db4eab25475200da4&z=13 (дата обращение: 28.11.2019).

УДК 004.05
ГРНТИ 20.53.19

ИССЛЕДОВАНИЕ МЕТОДИКИ РЕДАКТИРОВАНИЯ АУДИОМАТЕРИАЛА В РАДИОВЕЩАНИИ

Е. В. Гунина, А. Я. Моисеева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Получение новых знаний с помощью аудиопередач является общедоступным. Создание аудиоматериала для информирования радиослушателей требует использования определенных методов. При этом существует проблема привлечения внимания аудитории и восприятия получаемой информации. В данной статье рассмотрена методика редактирования аудиозаписей для применения в сфере радиовещания. Результатом исследования были предложены этапы работы над аудиозаписью, которые могут послужить для разработки алгоритма действий, что позволит не только улучшить качество работы, но и ускорить процесс получения результата.

радиовещание, аудиомонтаж, звукорежиссура, звуковая дорожка.

Прослушивание аудиопередач – это один из общедоступных способов получения новых знаний. Создание аудиоматериала для информирования радиослушателей требует использования определенных методов. При этом существует проблема привлечения внимания аудитории и восприятия получаемой информации. В данной статье рассмотрена методика редактирования аудиозаписей для применения в сфере радиовещания.

Большое внимание проблеме актуальности радиовещания уделяет профессор А. Шерель. В частности, он пишет, что «среди всех каналов массовой коммуникации радиовещание обладает самой высокой проникающей способностью» [1]. Также, исследователь В. Егошкина отмечает особенно-

сти радиовещания: «радиостанциям необходимо выдерживать жесткую конкуренцию как со стороны других средств массовой информации, так и внутри радиорынка» [2]. Оба автора предлагают следующие пути решения данной проблемы. А. Шерель считает очевидным вывод о том, что для увеличения качества содержания программы, необходимо разделить работу на части. В то же время, В. Егошкина предлагает решать данную проблему путем детальной проработки контента и структуры радиопрограммы. Таким образом, логично предположить, что разделение труда при создании радиопрограммы является важным фактором для получения качественного результата. Журналист отвечает за качество предоставляемого материала, диктор начитывает информацию, а звукорежиссер монтирует передачу. Следовательно, повышается не только качество, но и количество выходящих передач.

Однако, при подаче программы аудитории, следует учитывать не только качественное наполнение передачи, но и способ восприятия информации слушателем. Физиолог А. Бергер в своем учебнике утверждает, что «человек запоминает 10 % прочитанного, в отличие от 20 % услышанного и 30% увиденного» [3]. Следовательно, возникает проблема удержания внимания аудитории при получении информации только через слуховое восприятие. С психологической точки зрения, в зависимости от интереса слушателя к воспроизводимой информации, А. Шерель выделяет три типа восприятия. Фоновое восприятие подразумевает осознание передачи слушателем как части окружающей обстановки. Сосредоточенное восприятие подразумевает полную концентрацию на получении и запоминании аудиосообщения, и требует значительных психологических усилий от слушателя [1]. Но особое внимание следует уделить селективному восприятию. Это выборочное выделение и осознание фрагментов программы. При этом процесс понимания полученной информации происходит в промежутки между смысловыми блоками [1]. Можно сделать вывод, что селективное восприятие наиболее подходит для усвоения большого количества информации, и при этом не перегружает организм слушателя.

Именно проблема привлечения и удержания внимания слушателя становится главной задачей звукорежиссера передачи. Необходимо совмещать технические решения со знанием эмоционально-психологического настроя слушателя. Специалист по истории радио, профессор МГУ А. Шерель в своем учебнике по радиожурналистике особо подчеркивает, что звук и звуковое общение обладают богатейшими возможностями воздействия на рациональную и эмоциональную сферы человеческого сознания [1]. Ю. Клюев, автор другого учебника для радиожурналистов, также выделяет, что психологическое влияние радио на людей связано с ориентацией его на слуховое, аудиальное восприятие информации [4]. Технические решения,

предлагаемые аудиоинженерами, направлены не только на качество доносимой информации до аудитории, но и на психологию слушателей. Следовательно, сугубо технический процесс монтажа звука неразрывно связан с эмоциональным восприятием субъекта.

В радиовещании слово не является достаточно выразительным средством воздействия на психологию слушателя. Решением является добавление музыкального фона к звучащему тексту. Музыка в этом случае выполняет не только оформительскую задачу, но и подчеркивает проблемно-тематическую направленность программы, формирует ее аудиальный стиль [4]. Правильный подбор звукового фона под тематику передачи повышает заинтересованность слушателя [1]. Учитывая селективность восприятия, новая информация должна подаваться логическими блоками, чтобы аудитория имела возможность осмыслить услышанное [5]. Фрагменты звуковых дорожек должны быть приведены к единым звуковым характеристикам, после чего сведены в цельную звуковую форму [6]. На основе данных утверждений, можно сделать вывод, что на организм слушателя в равной степени оказывает влияние не только информационная наполненность программы, но и ее звуковое оформление.

Работающие в области инженерии звука профессионалы активно решают проблему привлечения и удержания внимания аудитории. В частности, О. Шлыкова и В. Таран предлагают следующий алгоритм аудиоинженерии: подготовка к записи, запись аудиоматериала, премастеринг, сведение аудиоматериала, финальный мастеринг и авторинг [6]. В свою очередь, В. Гринфельд и Я. Никитенко разработали критерии оценки качества аудиоконтента [7]. Данные исследования были проанализированы и пересмотрены с точки зрения наличия у звукорежиссера готовой звуковой дорожки. Также учтены эмоционально-психологические факторы восприятия аудиальной информации, рассмотренные выше. На основе изученных материалов можно разработать четкую модель организации процесса редактирования информационных аудироликов.

Наиболее вероятно первым этапом следует сделать очищение записи от явных посторонних звуков: кашля, чихания, громкого дыхания, окружающего шума.

Следующим этапом можно предположить более детальную чистку материала. Убирается заикание, производится точечная коррекция громкости звука.

Далее возможна коррекция длительности аудио соответственно особенностям восприятия аудиоматериала. Подразумевается увеличение длины пауз между блоками несвязанной информации, а внутри блока длительность перерывов уменьшается.

На четвертом этапе предполагается поиск и наложение подходящего музыкального фона. Фон необходим для удержания внимания слушателя

и заполнения пробелов между словами. Выбор сопровождения зависит от информационного наполнения исходного материала.

Далее логично скорректировать продолжительность выбранного фона согласно длины звуковой дорожки.

Следующим действием вероятно следует произвести корректировку уровня громкости фона. Выставляется общая громкость фона относительно словесной информации. В начале и конце передачи, а также в местах логических пауз, громкость фона увеличивается до уровня исходного материала.

Седьмым этапом предполагается проверка получившегося аудио. Готовый выпуск прослушивается и при необходимости дорабатывается.

Завершающим этапом логично произвести микширование всех дорожек в аудиофайл требуемого формата.

Полученные восемь шагов по обработке аудиоматериала разделяют большой объем работы на небольшие части, что должно увеличить скорость выполнения редактирования. Также данные действия позволят с легкостью разобраться в процессе аудиообработки людям, являющимся новичками в данной области.

Предложенные этапы работы над аудиозаписью могут послужить для разработки алгоритма действий, что позволит не только улучшить качество работы, но и ускорить процесс получения результата.

Список используемых источников

1. Барабаш Д. С., Болотова Л. Д., Гаспарян В. В., Голованов В. Е., Кузнецов Г. В., Кузьмина Е. Г., Левин В. Н., Любосветов Д. И., Смирнов В. В., Тхагушев И. Н., Шерель А. А. Радиожурналистика / под ред. проф. А. А. Шереля. М. : Изд-во московского университета, 2000. 267 с.

2. Егошкина В. А. Формат радиостанций и форматообразующие признаки радиопрограмм [Электронный ресурс] // Коммуникативные исследования. 2017. № 2 (12). С. 61–68. URL: https://cyberleninka.ru/article/n/format-radiostantsiy-i-formatoobrazuyuschie-priznaki-radioprogramm/viewer (дата обращения: 28.11.2019).

3. Бергер А. Видеть – значит верить. Введение в зрительную коммуникацию. 2-е изд.: пер. с англ. М. : Вильямс, 2005. 288 с.

4. Клюев, Ю. В. Радиожурналистика: основы профессии : учеб. пособие. СПб. : Инт «Высш. шк. журн. и мас. коммуникаций» СПбГУ, 2015. 151 с.

5. Головлева Е. Л., Мрочко Л. В., Яковчук Т. Г. Психологические факторы взаимодействия личности с контентом массовой информации [Электронный ресурс] // Экономические и социально-гуманитарные исследования. 2019. № 2 (22). С. 90–96. URL: https://cyberleninka.ru/article/n/psihologicheskie-faktory-vzaimodeystviya-lichnosti-s-kontentom-massovoy-informatsii/viewer (дата обращения: 02.12.2019).

6. Таран В. В., Шлыкова О. В. Аудиомастеринг: динамика технокультуры [Электронный ресурс] // Вестник МГУКИ. 2016. № 3 (71). С. 84–93. URL: https://cyberleninka.ru/article/n/audiomastering-dinamika-tehnokultury/viewer (дата обращения: 15.11.2019).

7. Гринфельд (Соболь) В. А., Никитенко Я. Ю. Авторская программа на радио: разработка универсальных критериев оценки качества аудиоконтента [Электронный ресурс] // Знак: проблемное поле медиаобразования. 2019. № 2 (32). С. 125-133. URL:

https://cyberleninka.ru/article/n/avtorskaya-programma-na-radio-razrabotka-universalnyh-kriteriev-otsenki-kachestva-audiokontenta (дата обращения: 03.12.2019).

УДК 004.4
ГРНТИ 49.34.01

СРАВНИТЕЛЬНЫЙ АНАЛИЗ IAAS (OPENSTACK) И PAAS (OPENSHIFT)

Г. О. Гурабатов, А. Д. Паничев, И. А. Ушаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Облачные сервисы стали набирать все большую популярность, они произвели революцию в области вычислительных систем. Благодаря облачным сервисам появилась возможность реализации проектов любой сложности с минимальными финансовыми затратами на содержание и обслуживание аппаратного обеспечения. Эти технологии дали возможность гибкого использования ресурсов, а именно: более быстрое развертывание приложений с автоматическим реагированием на изменение нагрузки системы, из-за чего пользователям не приходится обращать внимание на нижний уровень стека, а также возможность потреблять только необходимое количество ресурсов, избегая затрат на простаивающую аппаратную мощность.

PaaS, IaaS, Openstack, Openshift, Kubernetes, облачные вычисления, виртуальная инфраструктура.

С каждым годом облачные вычисления предоставляют пользователю все более гибкую систему IT ресурсов [1]. Гибкие облачные сущности могут увеличивать или уменьшать использование ресурсов в зависимости от текущей нагрузки, что помогает уменьшить финансовые растраты на поддержание аппаратной мощности [2].

Рассмотрим наглядный пример. Посещаемость большинства сайтов и нагрузка на аппаратные мощности подвержены, как сезонным, так и дневным колебаниям. Статистику использования сети интернет можно наблюдать с помощью ресурса liveinternet. На рис. 1 приведена статистика нагрузки интернет-трафика в течении нескольких месяцев. На основе этих статистических данных можно сделать вывод о неравномерности нагрузки. Для обеспечения бесперебойной работы интернет-сервисов требуется наличие и содержание физической мощности, соответствующей самой максимальной нагрузке на периоде, следовательно, в периоды меньшей нагрузки большое количество ресурсов не используется. Сложившуюся проблему

нам помогают решить технологии виртуализации [3, 4], обеспечивающие гибкую работу сервисов.

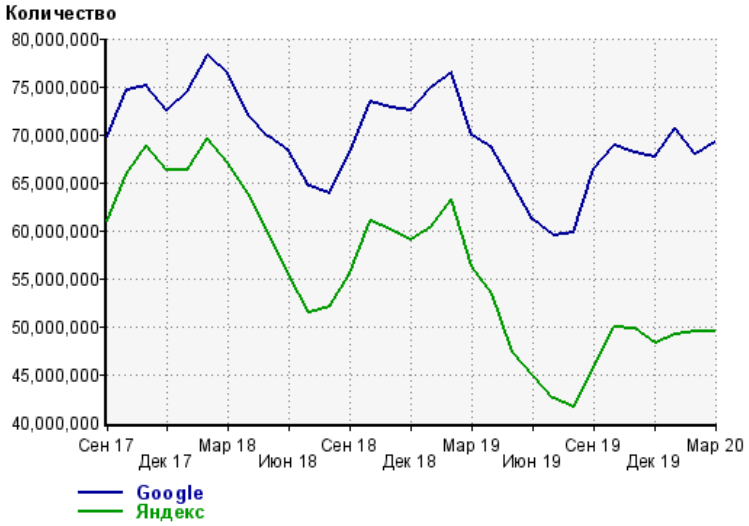


Рис. 1. Статистика посещений поисковой системы за несколько месяцев

На современном рынке появляется все больше моделей предоставления облачных мощностей. В данной статье рассмотрены IaaS *(Infrastructure as a Service)* и PaaS *(Platform as a Service)*, их особенности, возможности и преимущества относительно друг друга.

Инфраструктура как услуга (IaaS) является одним из уровней в модели облачных вычислений. Аппаратная инфраструктура предоставляется и управляется внешним поставщиком. Все существующие локальные ЦОД размещаются облачными провайдерами, включая серверы, хранилище, сетевой уровень и уровень гипервизора. Поставщики также предоставляют множество услуг, таких как мониторинг, автоматическое масштабирование, репликация и т. д.

При аренде виртуальной инфраструктуры у *IaaS*-провайдера клиент получает полные административные права внутри арендованных виртуальных серверов. Все настройки операционных систем этих серверов клиенту приходится выполнять самостоятельно: устанавливать программное обеспечение, конфигурировать брандмауэр и т.д. На рис.2 показано наглядное разделение обязанностей провайдера и клиента.

Рис. 2. Разделение влияния обязанностей и возможностей клиента и провайдера.

Иногда IaaS рассматривается как аппаратное обеспечение или как услуга HaaS (*Hardware as a Service*). Примеры включают Amazon Web Service (AWS), Rackspace, Windows Azure и OpenStack.

OpenStack является лидером в области систем управления облаками с открытым исходным кодом. OpenStack- это набор программных проектов на основе языка программирования python, который управляет доступом к объединенным хранилищам, вычислительным и сетевым ресурсам. Существует растущая система сервисных проектов, которые расширяют функциональность OpenStack, но которые привязаны к базовому набору из шести проектов: Neutron *(Networking),* Nova *(Compute)* Glance *(Image Management),* Swift *(Object Storage),* Cinder *(Block Storage)* и Keystone *(Authorization and Authentication)* [5].

В рамках задач, предусматривающих тестирование и разработку приложений, IaaS является более сложным и избыточным решением. Для того чтобы направить максимум своих усилий на разработку, не уделяя времени на поддержание базовой инфраструктуры, целесообразнее использовать иную модель, а именно PaaS.

Платформа как услуга предоставляет пользователям платформу и среду для разработки, управления и запуска приложений через Интернет. В этой модели разработчики создают приложение, которое будет работать в определенной среде и дополнительно контролировать параметры развертывания и настройки программного обеспечения. PaaS снижает стоимость и сложность развертывания приложений, избавляя от необходимости покупать и управлять базовым оборудованием и программным обеспечением.

В рамках модели PaaS не придется администрировать операционную систему и системное программное обеспечение. Для управления сайтом предоставляется будет предоставлен веб-интерфейс, с помощью которого пользователь сможет наполнить предоставленную платформу своей нагрузкой (скриптами, базами данных и т. д.). С клиента будет снята задача по администрированию сервера: как его аппаратной части, так и программной. На рис. 3 показано наглядное разделение обязанностей провайдера и клиента в PaaS модели.

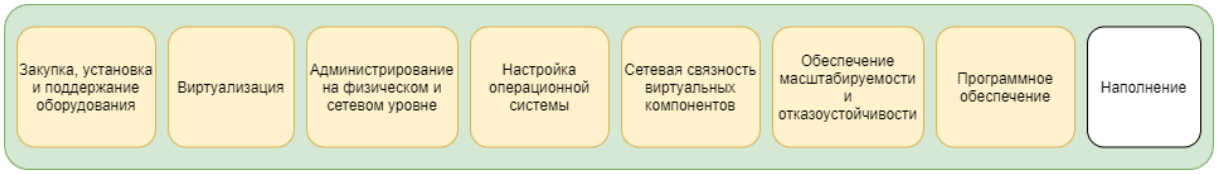


Рис. 3. Разделение влияния обязанностей и возможностей клиента и провайдера

Для начинающих разработчиков и маленьких компаний более разумно использовать готовый функционал таких популярных провайдерских решений, как: Red Hat OpenShift, Cloud Oracle, Google Cloud Services

Большинство из вышеперечисленных решений является абсолютно частным продуктом. Одним из малочисленных представителей PaaS с открытым исходным является продукт Red Hat OpenShift contrainer platform. OpenShift представляет собой платформу для управления контейнерами, поддерживающими оптимизированную работу приложений. Он позволяет создавать, тестировать и развертывать приложения без выделения и обслуживания серверов для каждого приложения. OpenShift запускает приложения в контейнерах Docker. Это гарантирует, что он всегда будет работать одинаково, независимо от среды, в которой он работает. OpenShift построен на основе Kubernetes. Kubernetes обеспечивает функциональность оркестрации, включая такие функции, как отказоустойчивость компонентов, мониторинг, автоматическое пересоздание контейнеров и горизонтальное масштабирование.

При разработке определенного приложения, без большой группы разнонаправленных специалистов и ограниченными финансами логичнее воспользоваться функционалом, который предоставляет PaaS. Таким образом можно направить все усилия на тестирование и быструю реализацию решения, не отвлекаясь на организацию и поддержку нижележащих уровней инфраструктуры. Если приложение будет выполнять сложные математические расчеты или требовать большой графической мощности GPU *(graphics processing unit)*, невозможно в полной мере протестировать и реализовать его функционал в связи с ограничением возможностей процессора внутри контейнера и отсутствием предоставления GPU.

Также невозможно построить многоуровневую сетевую топологию и настроить специфичные политики, ввиду того, что сетевое взаимодействие внутри платформы автоматизировано и настроено частными политиками провайдера. Разработка, требующая корневого доступа к уровню операционной системы, и СУБД так же становиться невозможной, из-за отсутствия прав пользователя на изменение конфигураций нижележащей инфраструктуры. Для реализации данных особенностей продукта следует использовать более полноценную и функциональную модель, такую как IaaS, которая позволит вести разработку любых приложений и сервисов, получить любую необходимую вычислительную мощность, тем самым обеспечивая большой задел на расширение будущих продуктов и их функционала. Но с ростом возможностей, растет и ответственность за работоспособность и отказоустойчивость инфраструктуры, которая ранее лежала на плечах PaaS провайдера.

Как OpenStack, так и *OpenShift* являются проектами с открытым исходным кодом, и оба обеспечивают основы облачных вычислений. Это взаимодополняющие проекты, которые хорошо работают вместе. Openshift в настоящее время не является частью OpenStack и не конкурирует

с ним. Если компания поддерживаете свою собственную систему OpenStack, она может сделать ее еще более полезной, установив Openshift поверх нее [6].

Подводя итоги сравнительного анализа IaaS и PaaS стоит сделать вывод о финансовой стратегии при выборе той или иной инфраструктуры. Именно экономическая выгода определяет развитие облачных инфраструктур и цель работы. Рост компании прямо пропорционален росту приложений и сервисов, что соответственно требует больше аппаратной мощности для поддержания хорошей работы разрабатываемого продукта [7]. Решения провайдеров являются очень удобными на первых этапах развития, но при хорошем потенциале компании, несут значительные экономические убытки. По мере развития компании появляется возможность создать инфраструктуру в частном центре обработки данных, используя решения с открытым исходным кодом и контролировать весь процесс технического взаимодействия.

Список используемых источников

1. Balueva A., Desnitsky V., Ushakov I. Approach to Detection of Denial-Of-Sleep Attacks in Wireless Sensor Networks on the Base of Machine Learning // Intelligent Distributed Computing XIII 2019. PP. 350–355.

2. Савинов Н. В., Токарева К. А., Ушаков И. А., Красов А. В., Сахаров Д. В. Исследование модели сети ЦОД на основе политик Cisco ACI // Защита информации. Инсайд. 2019. № 4 (88). С. 32–43.

3. Сахаров Д. В., Красов А. В., Ушаков И. А., Орлов Г. А. Защищенная модель программно-определяемой сети в среде виртуализации KVM // Электросвязь. 2020. № 3. С. 26–32.

4. Багомедова А. Р., Ушаков И. А., Цветков А. Ю. Разработка методов проверки соответствия серверов виртуализации требованиям безопасности согласно стандарту ГОСТ Р 56938-2016 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. В 4-х томах. СПб. : СПбГУТ, 2018. С. 58–63.

5. Red Hat, "Red Hat OpenStack Platform [Электронный ресурс]. URL: https://www.openstack.org/.

6. Red Hat, "OpenShift Origin" [Электронный ресурс]. URL: https://www.openshift.org/.

7. Котенко И. В., Десницкий В. А., Чечулин А. А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд, 2011, № 3 (39). С. 68–75.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056
ГРНТИ 81.93.29

ИСПОЛЬЗОВАНИЕ ПРОГРАММЫ «TERRIER» ВЕРСИЯ 3.0 ДЛЯ ПОИСКА И ГАРАНТИРОВАННОГО УНИЧТОЖЕНИЯ ИНФОРМАЦИИ НА ДИСКАХ

А. С. Дворников, Н. В. Капчук, С. О. Савченко

Военная академия связи

В ходе работы были рассмотрены принципы записи информации на различные типы носителей, произведен анализ методов гарантированного уничтожения информации с носителей, проведены эксперименты по поиску и гарантированному уничтожению информации с помощью программного обеспечения «Terrier 3.0».

Целью этой работы является анализ носителей информации с помощью программы поиска и гарантированного уничтожения «Terrier 3.0».

носители информации, способы уничтожения информации, информационная безопасность.

Часто, когда нужна повышенная надежность уничтожения данных, к носителям на жестких магнитных дисках применяют механические методы уничтожения, при которых происходит разрушение самого носителя информации. Механические методы уничтожения информации разделены на методы (рис. 1) [5]:

- *механическое воздействие.* Измельчение носителя путем использования устройства измельчения, так называемого шредера;
- *термический.* Нагревание НЖМД до температуры плавления в специальных печах;
- *пиротехнический.* Ещё один гарантированный метод уничтожения информации – это разрушение носителя взрывом;
- *химический.* Применяя химический способ, происходит разрушение рабочего слоя носителя;
- *радиационный.* Разрушение носителя ионизирующими излучениями.

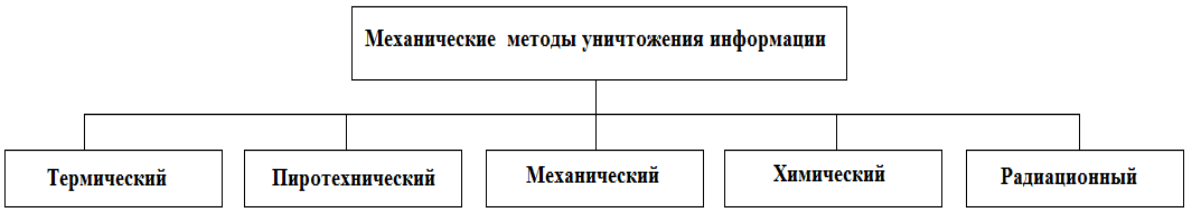


Рис. 1. Механические методы уничтожения информации

Одни из этих методов экологически небезопасны, другие из них могут обеспечивать очень высокую надежность уничтожения данных, но требуют специального дорогостоящего оборудования, которым обладают лишь единичные пользователи.

Экспериментальная часть

В данном разделе проводится уничтожение информации с различных типов носителей с помощью функций операционной системы Windows.

После уничтожения проводится анализ данных, содержащихся на носителях. Для исследования были выбраны носители разных типов и способов записи:

1) оптический диск: DVD-RW HL-DT-ST_BD-RE_BT20N;
2) накопитель на жестких магнитных дисках: WDC WD3200AAKX-001CA0.

Используемые средства для уничтожения и анализа данных на носителях. Программа для поиска данных на носителях информации

Для поиска и анализа, содержащихся на носителях данных, использовали поиск, по ключевым словам, которые встроен в функционал программы поиска и гарантированного уничтожения информации на дисках «Terrier 3.0» (рис. 2). Программное обеспечение «Terrier 3.0» представляет собой сертифицированное ФСТЭК средство контроля защищенности информационных ресурсов от несанкционированного использования. Данное программное решение используется для поиска и уничтожения данных на внешних носителях информации.

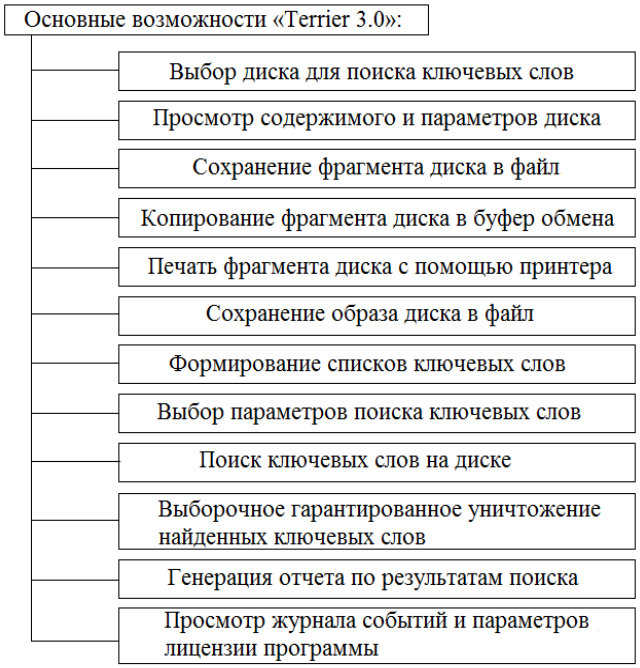


Рис. 2. Основные возможности Terrier 3.0

Уничтожение и анализ данных с оптических носителей информации

В качестве объекта для эксперимента был выбран диск с возможностью многократной перезаписи DVD-RW HL-DT-ST_BD-RE_BT20N, емкость

диска 4.38 Гб. На диске, который использован для эксперимента, была записана информация. CD/DVD-RW диски поддерживают возможность многократной перезаписи и стирания с них информации. Для стирания данных, нужно вставить диск в устройство «Дисковод» и открыть «Мой компьютер», через небольшой промежуток времени дисковод считает диск, и он будет доступен для использования. Далее в проводнике, в доступных операциях над диском необходимо выбрать «Стереть этот диск». После этого запустится инструмент «Запись на диск». Следуя инструкциям «Мастера записи на диск» стирание информации с диска, после небольшого ожидания, успешно завершено. После стирания информации с диска был проведен анализ диска с помощью программного обеспечения «Terrier 3.0» (рис. 3).

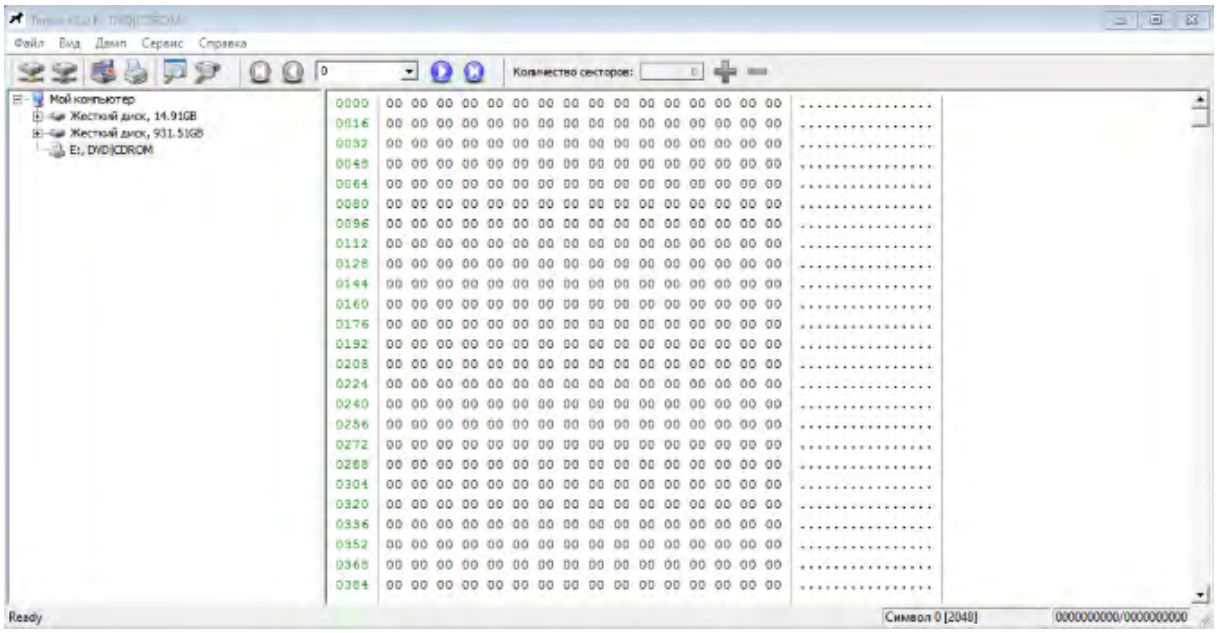


Рис. 3. Результат анализа оптического носителя программой «Terrier 3.0»

Данный анализ показал, что вся информация с оптического носителя полностью удалена и восстановление невозможно.

Уничтожение и восстановление данных с носителей на основе микросхем с энергонезависимой памятью

Для эксперимента был использован НЖМД модели WDC WD3200AAKX-001CA0 с емкостью 219 Гб с записанной на него информацией (рис. 4).

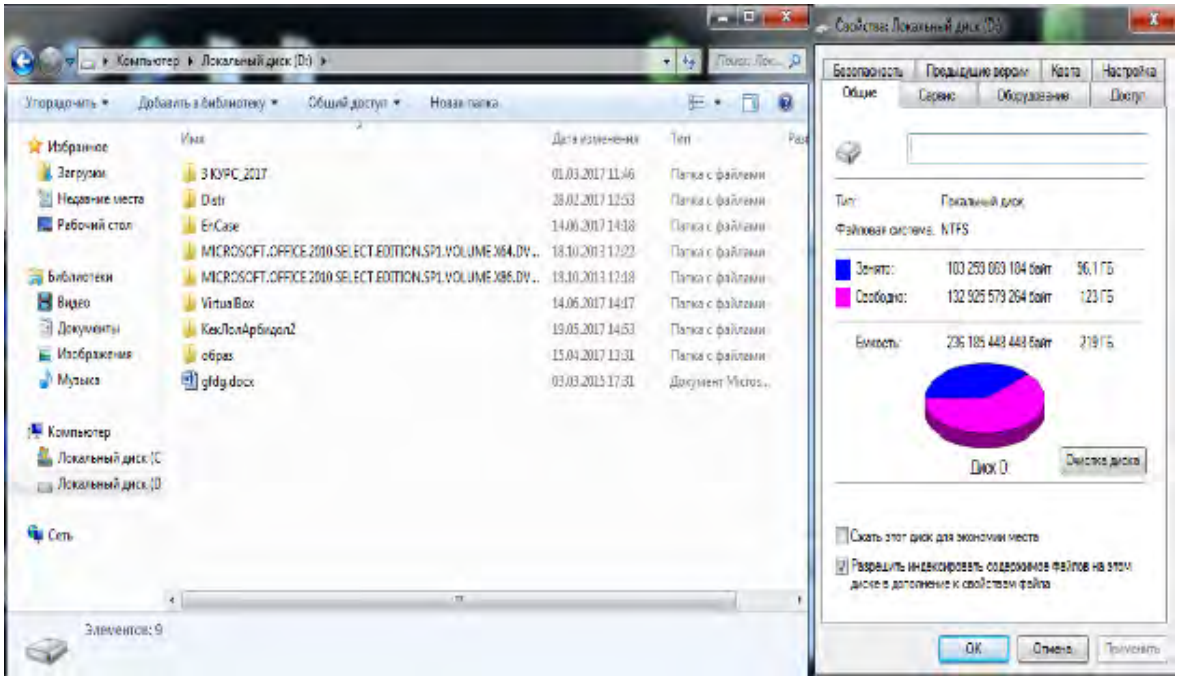


Рис. 4. Данные и свойства носителя на жестких магнитных дисках

Проведем поиск по ключевому слову с помощью программы поиска и гарантированного уничтожения информации «Terrier 3.0». По результатам поиска видим, что ключевое слово «информация» найдено во многих секторах диска. В первой части эксперимента используем быстрое форматирование. После быстрого форматирования, в свойствах накопителя было видно, что все данные были стерты, и он не содержит никакой информации. Однако, после поиска по ключевому слову с помощью программного обеспечения «Terrier 3.0», видно, что диск содержит информацию, т. к. при быстром форматировании пространство на диске помечается как неиспользуемое, без фактического удаления информации (рис. 5).

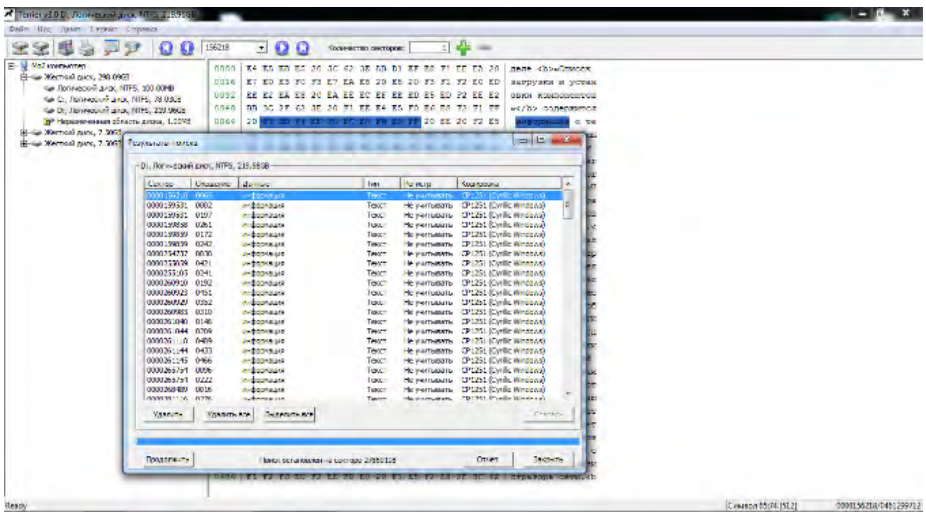


Рис. 5. Результат поиска по ключевому слову программным обеспечением «Terrier 3.0» после быстрого форматирования

Во второй части эксперимента будем использовать полное форматирование. После полного форматирования, в свойствах накопителя так же было видно, что он пустой и не содержит никакой информации (рис. 6).

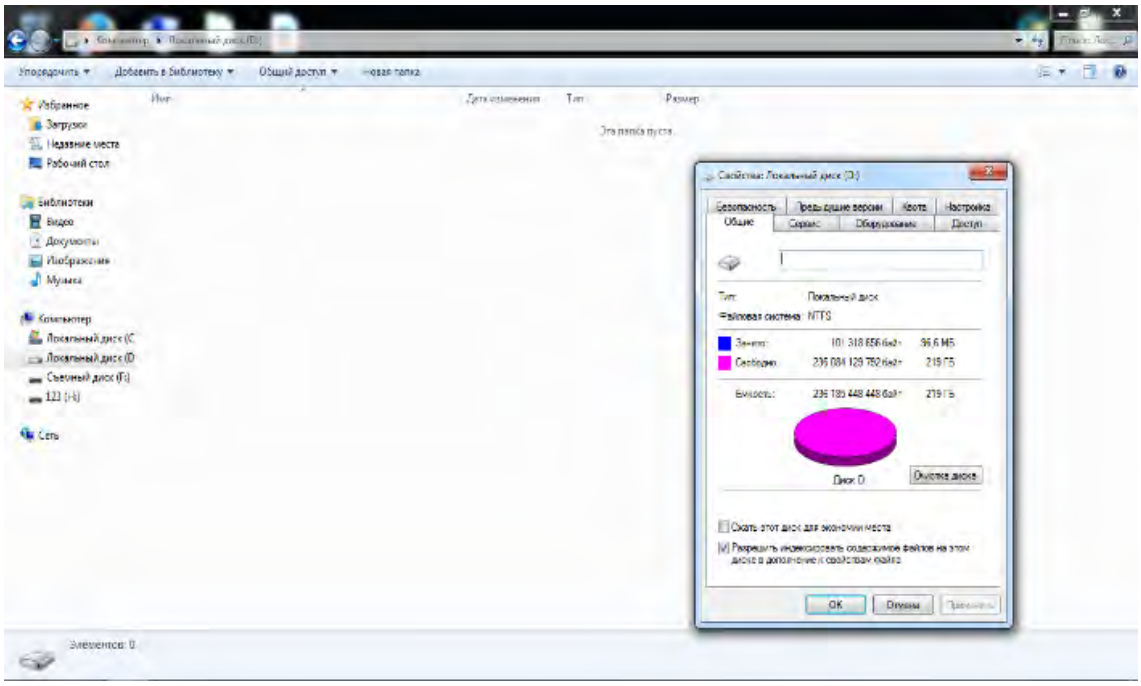


Рис. 6. Данные и свойства накопителя после полного форматирования

Проведя анализ диска с помощью программного обеспечения «Terrier 3.0», видим, что диск пустой и не содержит никакой информации (рис. 7).

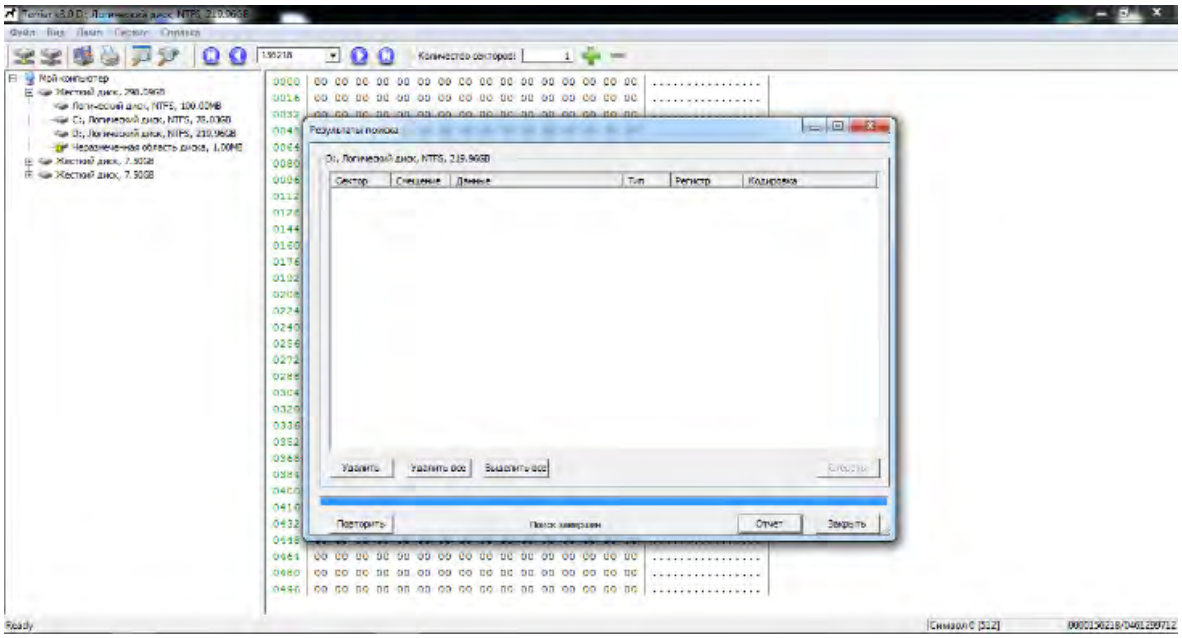


Рис. 7. Результат поиска по ключевому слову программным обеспечением «Terrier 3.0» после полного форматирования

Заключение

В данной работе был проведен обзор носителей и способы записи на них информации, анализ способов гарантированного уничтожения данных с различных типов носителей. Были проведены исследования по поиску и гарантированному уничтожению информации программным обеспечением «Terrier 3.0» с трех типов носителей.

Подводя итог работы, стоит отметить, что для гарантированного уничтожения информации нужно корректно подходить к выбору способов уничтожения информации, ведь существует небольшая вероятность, что информация сохранилась, хоть и не в полном своем объеме. Такое может произойти в связи с тем, что устройства уничтожения информации ещё несовершенны или может зависеть от особенностей сохранения информации на носитель.

Список используемых источников

1. ГОСТ Р. 50739-95 Средства вычислительной техники - Защита от несанкционированного доступа Общие технические требования. Введ. 09.02.95 М. : Госстандарт России, 1995.

2. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. М. : Гостехкомиссия РФ, 1992.

3. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Введ. 30.03.1992. М. : ГТК., 1992.

4. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. М. : Госстандарт РФ, 1996.

5. Коженевский С. Методы гарантированного уничтожения данных на жестких магнитных дисках [Электронный ресурс]. URL: http://www.epos.ua/view.php/about_pubs_archive?subaction=showfull&id=1043964000&archive=&start_from=&ucat=2&

6. Gutmann P. Secure Deletion of Data from Magnetic and Solid-State Memory. Sixth USENIX Security Symposium Proceedings [Электронный ресурс]. URL: https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

7. Schneider B. Applied Cryptography. 2nd ed. John Wiley & Sons, Inc., 1996.

8. Industrial Security Manual for Safeguarding Classified Information. Department of Defense Manual, DoD 5220.22-M, 1987.

УДК 004.056
ГРНТИ 50.41.22

ВЫБОР НАИЛУЧШЕГО ПРЕДСТАВЛЕНИЯ ДАННЫХ В СИСТЕМАХ ХРАНЕНИЯ ДЛЯ ВОЗМОЖНОСТИ ОСУЩЕСТВЛЕНИЯ КОНТРОЛЯ ИХ ЦЕЛОСТНОСТИ

С. А. Диченко, Н. А. Корсун, Б. И. Симорин

Краснодарское высшее военное училище

В основе функционирования современных систем хранения данных информационно-аналитических систем лежит обработка больших массивов данных средствами различных типов и различной архитектуры. Одной из актуальнейших задач при этом является организация хранения данных, обеспечивающая тождественность данных у оператора, отправившего их на хранение и у лица, принимающего решение, при запросе на их использование.

системы хранения данных, информационно-аналитические системы, контроль целостности, многомерное представление данных.

При разработке и создании современных систем хранения данных (СХД) особое внимание уделяется их безопасности, которая в настоящее время достигается построением оригинальных схем, учитывающих структуру многомерного представления в них данных, что является важным при учете уровня аппаратурных и программных затрат, соответствующих наиболее эффективным методам обеспечения целостности.

Для этого в настоящее время ведутся работы по разработке новых способов контроля и восстановления целостности данных [1, 2, 3, 4, 5, 6], в том числе и для облачных хранилищ [7, 8], где эффективность обеспечения целостности зависит от выбор наилучшего представления данных в современных СХД.

Многомерная модель данных, лежащая в основе построения современных СХД, опирается на концепцию многомерных кубов, или гиперкубов (рис. 1). Для декомпозиции многомерного массива информации, хранящейся в СХД, используя известные правила, выполняется его расчленение на сечения (сечения гиперкуба данных), которое заключается в выделении подмножества ячеек гиперкуба при фиксировании значения одного или нескольких измерений. В результате расчленения на сечения получается срез или несколько срезов, каждый из которых содержит информацию, связанную со значением измерения, по которому он был построен.

При фиксировании одного измерения получается сечение гиперкуба данных, содержащее в себе множество ячеек – блоков данных. При этом полученное сечения гиперкуба данных M декомпозируется на M_{ij} блоки данных, где $i = 1, 2, \ldots, n$; $j = 1, 2, \ldots, k$.

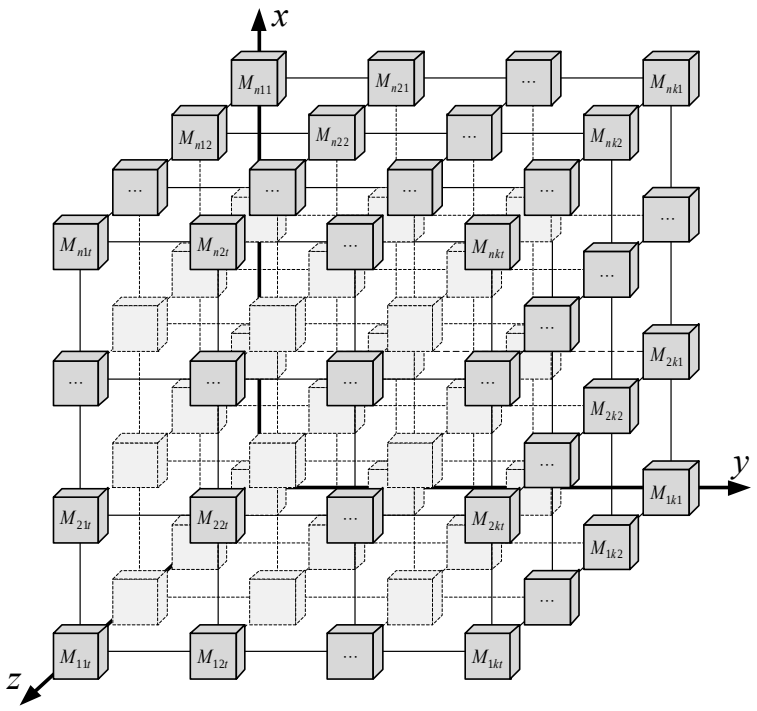


Рис. 1. Принцип организации многомерного куба данных

Такое представление будет соответствовать представлению данных в 2-мерном пространстве (рис. 2а).

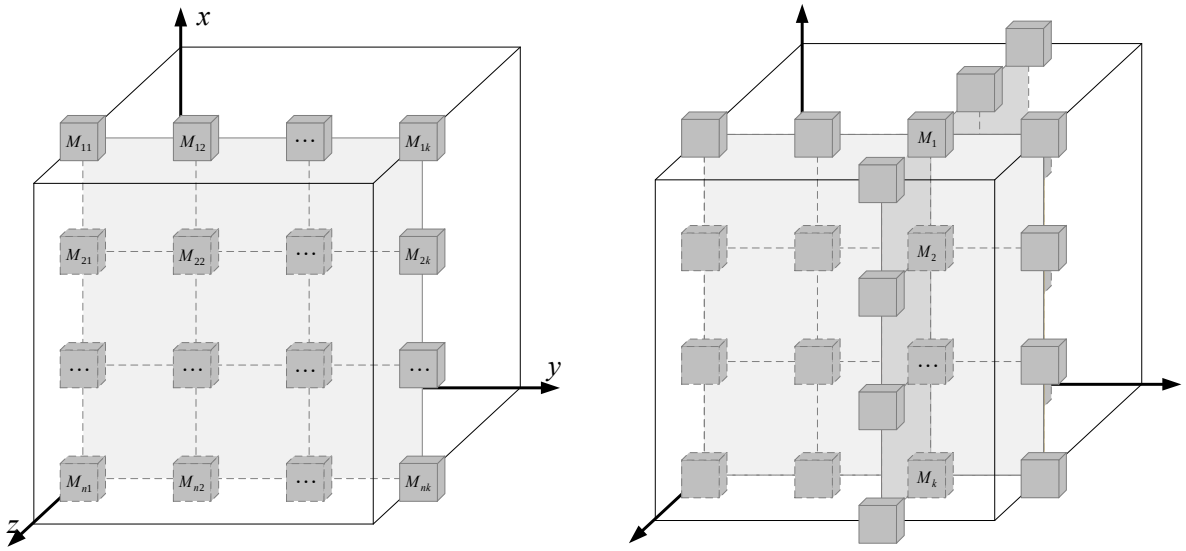


Рис. 2. Представление данных:
а) в 2-мерном пространстве; б) в 1-мерном пространстве

При фиксировании по одному отличному друг от друга измерению на разных срезах получается два пересекающихся в пространстве сечения гиперкуба данных, содержащие в себе множество ячеек – блоков данных. При рассмотрении блоков данных, расположенные на таком пересечении, гиперкуб данных M декомпозируется на M_i блоки данных, где $i = 1, 2, \ldots, k$.

Такое представление будет соответствовать представлению данных в 1-мерном пространстве (рис. 2б).

Нумерация блоков данных на рис. 2а, 2б выполнена независимо от начала системы координат для удобства и стремления приведения формы математического обозначения блоков данных к привычному виду, где нумерация блоков данных − элементов матрицы (рис. 2а) или вектора (рис. 2б) осуществляется слева направо сверху вниз.

Таким образом, информация в СХД является логически целостной. Это уже не просто наборы строковых и числовых значений, которые в случае реляционной модели нужно получать из различных таблиц, а целостные структуры с однозначными связями, что делает преимущества многомерного подхода очевидными.

Список используемых источников

1. Finko O.A., Dichenko S.A. Two-dimensional control and assurance of data integrity in information systems based on residue number system codes and cryptographic hash functions // Proceedings of the 2018 Multidisciplinary Symposium on Computer Science and ICT (Stavropol, Russia, October 15, 2018), 2254, CEUR Workshop Proceedings, 2018. PP. 139–146.

2. Диченко С.А. Концептуальная модель обеспечения целостности информации в современных системах хранения данных // Сборник материалов XIX международной научно-методической конференции: Информатика: проблемы, методология, технологии. Под ред. Д. Н. Борисова. 2019. С. 697–701.

3. Патент на изобретение RU 2680739, 26.02.2019. Способ контроля и обеспечения целостности данных // Самойленко Д. В., Финько О. А. и др. Заявка № 2017141538 от 28.11.2017.

4. Патент на изобретение RU 2696425, 02.08.2019. Способ двумерного контроля и обеспечения целостности данных // Самойленко Д.В., Финько О.А. и др. Заявка № 2018118919 от 22.05.2018.

5. Патент на изобретение RU 2680033, 14.02.2019. Способ обеспечения целостности данных // Самойленко Д.В., Финько О.А. и др. Заявка № 2017117714 от 22.05.2017.

6. Диченко С. А. Контроль и обеспечение целостности информации в системах хранения данных // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 1. С. 49–57.

7. Диченко С. А., Финько О. А. Гибридный крипто-кодовый метод контроля и восстановления целостности данных для защищённых информационно-аналитических систем // Вопросы кибербезопасности. 2019. № 6 (34). С. 17–36.

8. Диченко С. А. Разработка алгоритма контроля и обеспечения целостности данных при их хранении в центрах обработки данных / С. А. Диченко, А. А. Акилов и др. // Сб. науч. ст. VIII Международной молодежной научно-практической конференции с элементами научной школы. Омск: Омский ГТУ, 2018. С. 40–43.

УДК 004.654
ГРНТИ 20.53.17

О ПОВЫШЕНИИ ОПЕРАТИВНОСТИ ОБРАБОТКИ НЕСТРУКТУРИРОВАННЫХ ДАННЫХ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ БЛОКЧЕЙН-ТЕХНОЛОГИИ

М. В. Дульков, И. Н. Фабияновский, И. Б. Саенко

Военная академия связи

Рассматривается проблема оперативной обработки неструктурированных данных в распределенных информационных системах. Обсуждается повышение их оперативной обработки за счет применения блокчейн-технологии. Формулируется постановка задачи на разработку модели и методики на ее основе, предлагаются пути ее решения.

неструктурированные данные, блокчейн-технология, информационный ресурс, распределенная информационная система.

Создание распределенных информационных систем (РИС) и оптимизация размещения информационных ресурсов (ИР) в едином хранилище информации являются весьма актуальной задачей. Это связано с возрастающими потребностями пользователей оперативности предоставлении необходимой информации по запросу и безопасности ее хранения. Для этих целей был проведен анализ предметных областей, специализирующихся на отраслевых решениях с массовыми транзакциями (электронный документооборот, управление технологическими процессами и т. д.). Анализ показал довольно низкую оперативность обработки неструктурированных данных (НД) в РИС. Обычно это связано с постепенным накоплением данных, увеличением количества пользователей, доработкой и расширением функциональных возможностей системы и т. д.

Среди современных РИС, автоматизирующих управленческие процессы, значительное место занимают учетно-отчетные и информационно-справочные системы [1]. Иначе их называют транзакционными или OLTP-системами (от англ. On-Line Transaction Processing) [2]. Они предназначены для ввода данных, структурированного хранения и обработки информации в режиме реального времени и служат для поддержки текущей деятельности различного рода организаций. Задачи OLTP-систем – это быстрый сбор и оптимальное размещение информации в базах данных (БД), обеспечивая при этом полноту, актуальность и согласованность вводимых данных.

Особенностью OLTP-систем является то, что информация, циркулирующая в системе, идет снизу вверх по системе управления и инициирует управленческие воздействия, позволяя выбирать тот или иной способ, имея при этом форму НД. Под термином «неструктурированных данных» будем понимать информацию, которая либо не имеет заранее определенной структуры, либо она не организована в установленном порядке (например, текстовые сообщения, метаданные, аудио, видео, изображения и т. д.), но может храниться в форме структурированных объектов (например, в форме электронных файлов или документов), которые сами по себе имеют структуру. При этом сочетание структурированных и неструктурированных данных также будем называть неструктурированными данными.

Ввиду большого разнообразия существующих OLTP-систем, охватывающих широкий спектр предметных областей, принципы их построения достаточно похожи, а от выбора технологии их построения зависит производительность всей РИС. В результате при построении современных OLTP-систем возникает необходимость решения оптимизационной задачи следующего вида: при заданных требованиях к безопасности информации следует максимизировать производительность системы, измеряемую количеством транзакций, выполняемых в единицу времени, либо минимизировать среднее время обработки одной транзакции [3].

В таблице приведены результаты сравнительного анализа современных технологий, применяемых в OLTP-системах, а именно: блокчейн-технологии и технологии облачных вычислений [4].

ТАБЛИЦА. Сравнительный анализ современных технологий

Технология	Блокчейн	Облачные вычисления
Вариант построения	Децентрализованная система	Централизованная система
Стратегия хранения данных	Дублирование (в каждой локальной БД находится полная копия РБД)	Смешанная (централизованная, локальная, дублирование)
Устойчивость к внешним воздействиям	Высокая (информация поступает на все узлы в системе по всем возможным каналам связи)	Низкая (функционирование системы зависит от пропускной способности канала связи)
Оперативность обработки транзакций	Высокая (обработка транзакций будет происходить на узле, производительность которого будет выше по отношению к другим узлам на текущей момент времени)	Высокая (предоставляется провайдером по запросу в качестве услуги)
Безопасность информации	Высокая (обеспечивается специальным алгоритмом в процессе обработки)	Высокая (предоставляется провайдером по запросу в качестве услуги)
Недостатки	Невысокая интенсивность обновления единого хранилища информации	Эффективность системы обеспечивается провайдером в виде услуги

Исходя из результатов этого анализа, можно сделать вывод, что блокчейн-технология обеспечивает более высокую устойчивость функционирования РИС при ее децентрализации и более высокую оперативность обработки НД при сохранении требуемых показателей безопасности. Достигается это за счет дублирования полной копии распределенной БД в каждой локальной БД.

Рассмотрим общий механизм реализации блокчейн-технологии на примере РИС некоторой коммерческой организации. Пусть руководитель организации имеет автоматизированную информационную систему (АИС), позволяющую отслеживать процесс текущей деятельности, начальник бухгалтерского отдела – систему бухгалтерского учета, начальник кадрового отдела – систему кадрового учета и т.д. Такую совокупность АИС, взаимодействующих между собой с помощью информационно- телекоммуникационной сети (ИТКС), будем называть РИС. Решение руководителя о трудоустройстве в организацию нового сотрудника должно изменить состояние баз данных во всей РИС. Для этого необходимо в каждой АИС вести учет всех изменений своих БД, согласовывать их с другими АИС и предоставлять их по запросу.

На рис. 1 показан процесс создания единого цифрового отпечатка (ЦО). Под ЦО понимается свернутое содержание данных в транзакции до определенного объема посредством специального алгоритма, с помощью которого при необходимости проверяется идентичность содержимого.

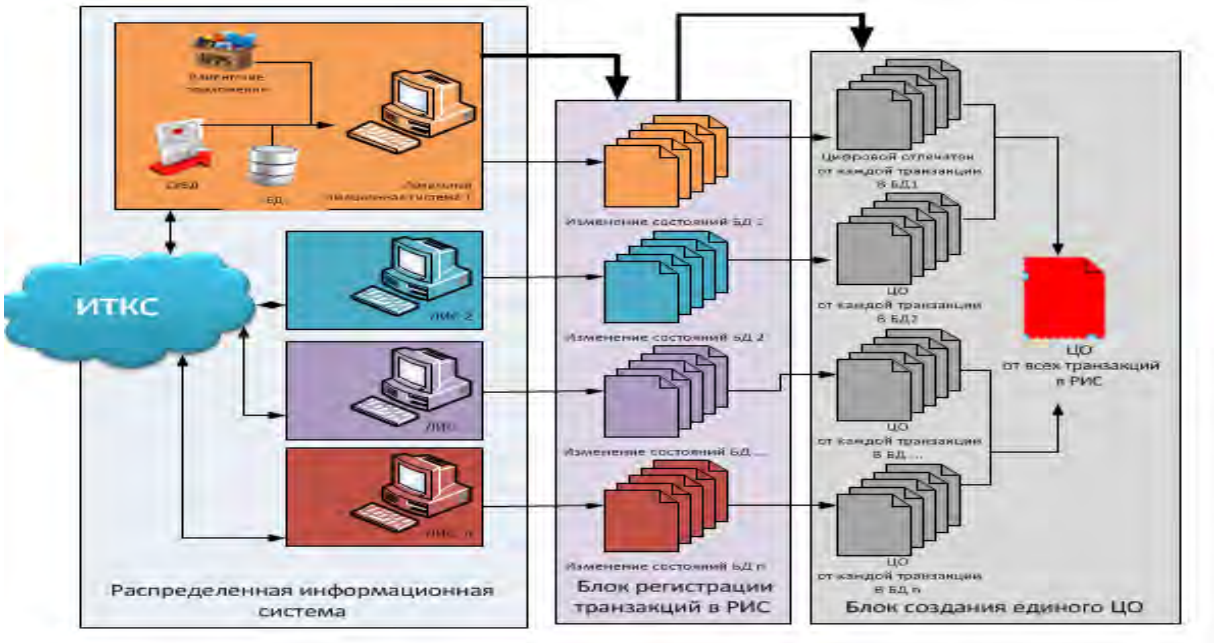


Рис. 1. Процесс создания единого ЦО

Положим, что локальная информационная система 1 (ЛИС1), в которой работает руководитель, играет роль главного узла в РИС, а ЛИС2, …,

ЛИС*n* – подчиненных узлов. Информационное взаимодействие между узлами осуществляется посредством ИТКС. Все узлы учитывают каждое изменение состояния свой БД. Такое действие называется транзакцией. Каждая транзакция в любом узле формирует ЦО, который отправляется на главный узел для создания единого ЦО. Такой механизм позволяет организовать в РИС информационное взаимодействие между узлами.

На рис. 2 показан процесс согласования данных, под которым понимается согласие каждого узла об идентичности своих транзакций в едином ЦО. После того как главный узел сформировал единый ЦО, он его отправляет на каждый узел для проверки правильности вычисленного результата. Это позволяет достичь необходимого согласования между узлами. Результаты вычисления ЦО с каждого узла отправляются на главный узел для принятия решения о добавления блока. Под «блоком» понимается информационная структура, которая отображает совокупность текущих транзакций. При положительном результате вычисления единого ЦО от всех узлов, под которым понимается получение ЦО от более 50 % узлов, главный узел принимает решение на создание блока. В противном случае блок не создается.

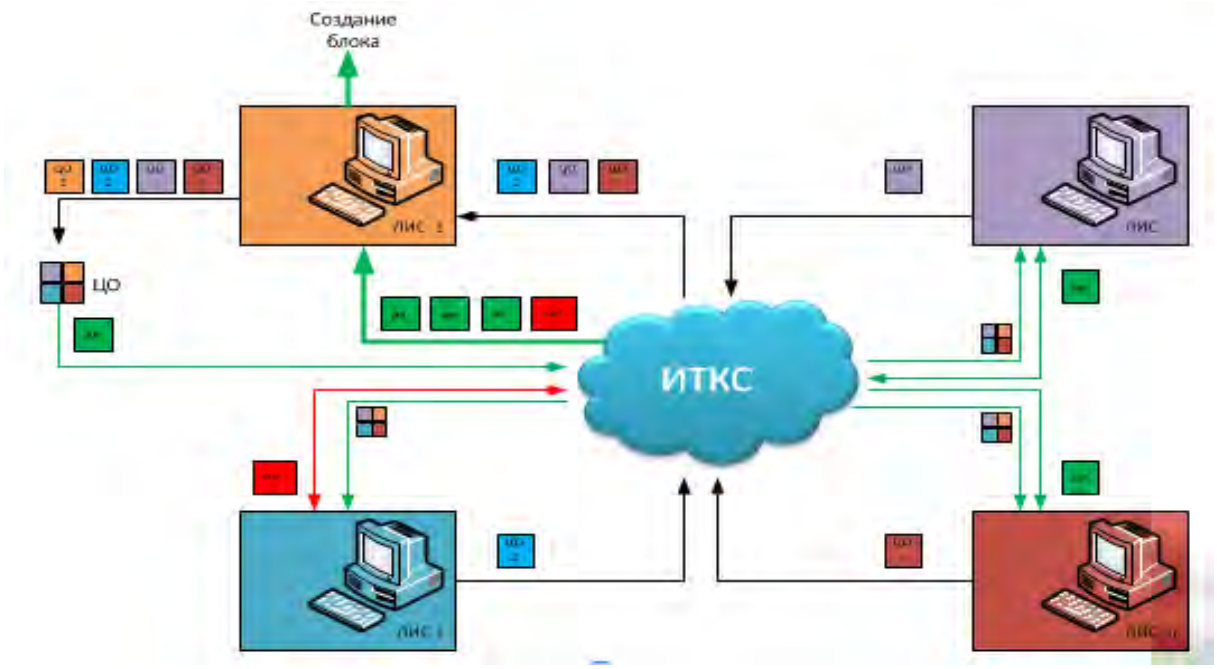


Рис. 2. Процесс создания единого ЦО

На рис. 3 показан процесс добавления блока в цепочку. После того, как главный узел сформировал блок, в сеть отправляется решение о добавление блока к цепочке. Затем каждый узел в сети начинает производить вычисления на добавление блока к цепочке. Для этой цели необходимо вычислить ЦО от цепочки блоков, содержащий единый ЦО от всех текущих транзакций, и ЦО блока, крайнего в цепочке. Узел, на котором результат вычисления в текущей момент времени достигается быстрее остальных, добавляет

блок к цепочке. Затем копия обновленной цепочки блоков рассылается на каждый узел сети. Такой механизм позволяет максимально быстро обновлять РИС с требуемой безопасностью данных.

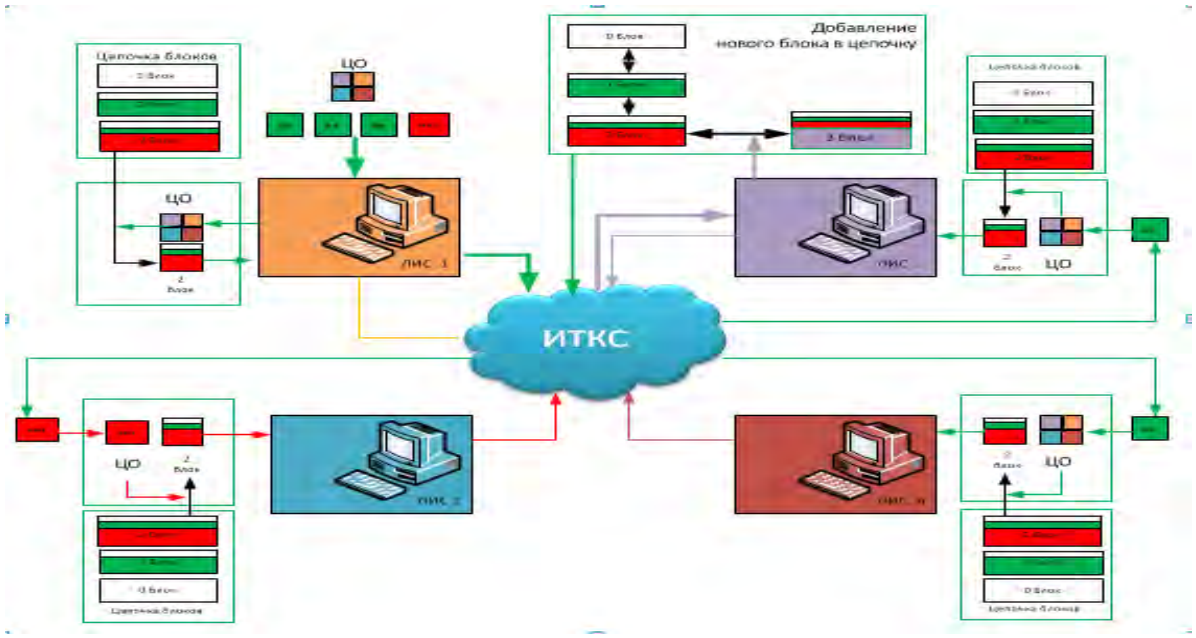


Рис. 3. Добавление нового блока в цепочку

Из рассмотренного примера следует вывод о том, что блокчейн-технология позволяет повысить производительность РИС и согласованность данных за счет ведения оперативного учета всех транзакций, обеспечивая при этом требуемую безопасность данных. Для того чтобы достичь максимальной производительности такой системы, необходимо найти оптимальную длину кодовой последовательности для сжатия данных и период добавления блока к цепочке.

Для решения этой задачи необходимо разработать модель управления информационными ресурсами в РИС, позволяющую оценить оперативность обработки в ней неструктурированных данных, и методику повышения оперативности функционирования РИС на основе использования блокчейн-технологии.

Список используемых источников

1. Когаловский М. Р. Энциклопедия баз данных. М. : Финансы и статистика, 2002. 800 с.

2. Лоховски Ф., Цикритизис Д. Модели данных. М. : Финансы и статистика, 1985. 344 с.

3. Горобец В. В. Анализ подходов к проектированию транзакционных систем // Методы и алгоритмы прикладной математики в технике, медицине и экономике: материалы XI Междунар. науч.-практ. конф., г. Новочеркасск, 28 фев. 2011г. / Юж.-Рос. гос. техн. ун-т (НПИ). Новочеркасск: ЮРГТУ (НПИ), 2011. С. 46–51.

4. Котенко И. В., Саенко И. Б., Полубелова О. В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. 2013. № 2 (25). С. 113–134.

УДК 004.7:004.422.8
ГРНТИ 20.01.07

МОДЕЛЬНО-АНАЛИТИЧЕСКИЙ ИНТЕЛЛЕКТ МУЛЬТИАГЕНТНЫХ СИСТЕМ РАННЕГО ПРЕДУПРЕЖДЕНИЯ

А. В. Дымченко, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Актуализирована интеллектуализация систем раннего предупреждения. Описаны преимущества комплексирования агентов обнаружения внезапных изменений в статистических свойствах контролируемых инвариантов. Определены ключевые принципы комплексирования агентов в целях повышения оперативности обнаружения изменений в статистических свойствах контролируемых инвариантов. Предложены формальные процедуры описания моделей комплексирования агентов обнаружения. Раскрыт процесс формирования модельно-аналитического интеллекта мультиагентных систем раннего предупреждения.

раннее предупреждение, интеллектуальный агент, комплексирование, инвариант, оперативность обнаружения, характеристики, модельно-аналитический интеллект.

В настоящее время остро обострились проблемные вопросы создания и сопровождения интеллектуальных распределённых систем раннего предупреждения о появляющихся событиях, приводящих к негативным или катастрофическим последствиям в национальном или мировом масштабе. Высокая востребованность интеллектуальных распределённых систем раннего предупреждения наблюдается по полному профилю проблем безопасности. В первую очередь, выделяются проблемы борьбы с пандемией и обеспечения жизнедеятельности. Неразрывная связь этих проблем прослеживается с обеспечением информационной безопасности [1, 2], поскольку информационные инфраструктуры становятся жизненно важными техногенными системами для социума.

Благодаря накопленному объёму знаний о методологическом базисе агентных технологий, представляющих одно из приоритетных направлений развития искусственного интеллекта, создаются благоприятные предпосылки для создания и сопровождения интеллектуальных распределённых

систем раннего предупреждения в виде мультиагентных систем. В этом контексте становятся востребованными и знания по использованию агентных технологий для обеспечения информационной безопасности [3, 4, 5]. Помимо того, что архитектура мультиагентных систем базируется на методах теории искусственного интеллекта, появляются новые возможности повышения их интеллектуальности с целью сокращения времени запаздывания по отношению к появляющимся событиям, приводящим к негативным или катастрофическим последствиям. Новые возможности, прежде всего заключаются в реализации функциональности, связанной с принятием оперативных решений относительно обнаружения появляющихся критических событий и управлением оперативностью с помощью модельно-аналитического интеллекта.

В предлагаемом расширении методологических аспектов жизненного цикла мультиагентных систем предусматривается определение формализмов для приобретения знаний о динамических возможностях раннего предупреждения крайне негативных или катастрофических последствий проявляющихся событий во внешней среде.

В функциональную спецификацию мультиагентной системы в целях их использования для предупреждения крайне негативных или катастрофических последствий проявляющихся событий во внешней среде могут вводиться вариативные схемы синхронизации распределенных решений, симплексные и дуплексные режимы работы агентов по формированию и комплексированию частных решений для вынесения интегрального (итогового) решения.

При использовании подобных механизмов в мультиагентной системе раннее предупреждение может основываться на решении задач обнаружения внезапных изменений в статистических свойствах контролируемых инвариантов, распределённых по множеству объединённых в систему агентов. На подсистему планирования действий мультиагентной системы раннего предупреждения, обеспечивающей функциональность искусственного интеллекта, может возлагаться формирование планов по определению состава инвариантов и решающих правил для принятия, как частных, так и интегральных решений. Опорную информационную основу о приемлемости формируемых сочетаний инвариантов и решающих правил может создавать модельно-аналитический интеллект мультиагентной системы, обеспечивающий определение, оценивание динамических характеристик процесса раннего предупреждения и управление сопутствующим качеством.

Представляемый подход к определению модельно-аналитического интеллекта мультиагентных систем раннего предупреждения базируется на выполнении формальных процедур описания моделей комплексирования агентов обнаружения внезапных изменений в статистических свойствах

контролируемых инвариантов, распределённых по множеству объединённых в систему агентов.

При раннем предупреждении обнаружение внезапных изменений в статистических свойствах контролируемых инвариантов осуществляется параллельно работающими агентами, синхронизация которых описывается с помощью булевой функции «$\vee$». При этом каждое решающее правило, закреплённое за отдельным агентом, описывается в классе конечных цепей Маркова стохастической матрицей переходов в конечном пространстве состояний $\mathbf{P}^{(i)}$, $i = 1, 2, ..., I$.

В представляемой ситуации $f_{p,\vee}(k_{p,\vee})$ плотность распределения вероятностей времени раннего предупреждения определяется следующим соотношением, полученным с помощью метода свёртки

$$f_{p,\vee}(k_{p,\vee}) = (1 - P_{1,(N_1+1)}^{(1,k_{p,\vee}-1)})(1 - P_{1,(N_2+1)}^{(2,k_{p,\vee}-1)})...(1 - P_{1,(N_i+1)}^{(i,k_{p,\vee}-1)})...(1 - P_{1,(N_I+1)}^{(I,k_{p,\vee}-1)}) -$$
$$- (1 - P_{1,(N_1+1)}^{(1,k_{p,\vee})})(1 - P_{1,(N_2+1)}^{(2,k_{p,\vee})})...(1 - P_{1,(N_i+1)}^{(i,k_{p,\vee})})...(1 - P_{1,(N_I+1)}^{(I,k_{p,\vee}-1)}),$$

$$i = 1, 2, ..., I, \; k_{p,\vee} = 1, 2, ..., K_{p,\vee},$$

где $P_{1,(N_i+1)}^{(i,k_{p,\vee})} - (1,(N_i+1))$-й элемент $k_{p,\vee}$ степени матричного описания решающего правила *i*-го агента $\mathbf{P}^{(i)}$; $P_{1,(N_i+1)}^{(i,k_{p,\vee}-1)} - (1,(N_i+1))$-й элемент $(k_{p,\vee}-1)$ степени матричного описания решающего правила *i*-го агента $\mathbf{P}^{(i)}$; I – количество агентов, принимающих решение об обнаружении изменений в статистических свойствах контролируемых инвариантов; $K_{p,\vee}$ – верхняя граница дискретного времени принятия решения об обнаружении изменений в статистических свойствах контролируемых инвариантов в симплексном режиме параллельно функционирующих агентов с функцией синхронизацией их работы, описываемой булевой функцией «$\vee$».

Значение верхней границы $K_{p,\vee}$ находится как наименьшее целое в приводимом неравенстве

$$(1 - \sum_{k_{p,\vee}}^{K_{p,\vee}} (1 - P_{1,(N_1+1)}^{(1,k_{p,\vee}-1)})(1 - P_{1,(N_2+1)}^{(2,k_{p,\vee}-1)})...(1 - P_{1,(N_i+1)}^{(i,k_{p,\vee}-1)})...(1 - P_{1,(N_I+1)}^{(I,k_{p,\vee}-1)}) -$$
$$-(1 - P_{1,(N_1+1)}^{(1,k_{p,\vee})})(1 - P_{1,(N_2+1)}^{(2,k_{p,\vee})})...(1 - P_{1,(N_i+1)}^{(i,k_{p,\vee})})...(1 - P_{1,(N_I+1)}^{(I,k_{p,\vee}-1)})) \le \boldsymbol{\delta}_{\vee},$$

где $\boldsymbol{\delta}_{\vee}$ – сколь угодно малая величина.

Оценивание $\mathrm{E}(k_{p,\wedge})$ математического ожидания и $\mathrm{D}(k_{p,\wedge})$ дисперсии времени раннего предупреждения осуществляется по формулам:

$$\mathrm{E}(k_{p,\vee}) = \sum_{k_{p,\vee}=1}^{Kp,\vee} k_{p,\vee} f_{p,\vee}(k_{p,\vee}),$$

$$\mathrm{D}(k_{p,\vee}) = \sum_{k_{p,\vee}=1}^{K_{p,\vee}} (k_{p,\vee} - \mathrm{E}(k_{p,\vee}))^2 f_{p,\vee}(k_{p,\vee}).$$

Приведённые соотношения образуют наукоемкое ядро модельно-аналитического интеллекта мультиагентных систем раннего предупреждения.

Научная новизна предлагаемого подхода к формированию модельно-аналитического интеллекта мультиагентных систем раннего предупреждения заключается в расширении формализаций распределённых систем искусственного интеллекта.

Список используемых источников

1. Птицына Л. К., Паскин Д. М. Анализ рисков срыва временного регламента по обнаружению угроз информационной безопасности // Информационная безопасность регионов России (ИБРР-2019). XI Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23–25 октября 2019 г.: Материалы конференции. СПб. : СПОИСУ, 2019. С 466–468.

2. Птицына Л. К., Паскин Д. М. Определение рисков срыва временного регламента по обнаружению угроз информационной безопасности // Региональная информатика и информационная безопасность: сб. тр. Выпуск 7. СПб. : СПОИСУ, 2019. С. 126–128.

3. Птицын А. В. Методологический базис агентных технологий для обеспечения информационной защищённости // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 1. С. 50–55.

4. Птицына Л. К., Птицын А. В. Обеспечение информационной безопасности на основе методологического базиса агентных технологий // Вестник Брянского государственного технического университета. 2017. № 2 (55). С. 146–154.

5. Птицына Л. К., Дымченко А. В. Моделирование мультиагентных систем принятия решений по обнаружению угроз информационной безопасности // Региональная информатика и информационная безопасность: сб. тр. Выпуск 7. СПб. : СПОИСУ, 2019. С. 115–118.

УДК 519.876.5
ГРНТИ 49.33.35

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ПОВЕДЕНИЯ УЗЛА ИНФОРМАЦИОННОЙ СЕТИ ПРИ АТАКЕ ТИПА DDOS

А. С. Дубонос, Н. В. Евглевская, А. О. Карасенко, О. С. Лаута

Военная академия связи

В данной статье рассматривается один из наиболее серьезных типов намеренного воздействия с целью блокирования/затруднения доступа пользователей к предоставляемым ресурсам, который называется DDoS атакой. Целью работы является проведение имитационного моделирования поведения узла информационной сети при реализации DDoS атаки. Разработанная модель позволяет демонстрировать состояние узла информационной сети при наличии DDoS атаки. Результаты моделирования планируется использовать в обучении искусственной нейронной сети обнаружению DDoS атак для разработки системы защиты информационных сетей.

имитационная модель, ddos атака, информационная сеть, уровень нагрузки.

Развитие технологий в сфере передачи информации ведет к росту числа пользователей сетевым ресурсом. Возрастает тенденция использования большого количества терминалов для организации информационных сетей. Благодаря сложившейся ситуации, взаимодействие пользователей и работа узлов информационных сетей становится эффективнее, что позволяет значительно ускорить процессы решения задач различного рода.

Однако, перечисленные факторы способствуют также появлению разнообразных видов намеренного и ненамеренного негативного воздействия, включающего в себя атаки на сетевые ресурсы, взломы, слежку, разнообразного рода коллизии, нештатные разрывы, конфликты адресов и т. п. [1]. Данные виды воздействия могут негативно повлиять на протекающие технологические процессы. В данной статье рассматривается один из наиболее серьезных типов намеренного воздействия, целью которого является блокирование/затруднение доступа пользователей к предоставляемым информационной сетью ресурсам, называемый DDoS атакой.

Согласно [2], в июле 2019 года была организована 13-дневная атака прикладного уровня против стримминг-сервиса с мощностью до 292 000 запросов в секунду. В августе от действий злоумышленников пострадал один из важных интернет-ресурсов, который протестующие в Гонконге использовали для координации своих действий. По комментариям администрации сайта, он пережил наплыв в 1,5 млрд. запросов за 16 часов, в результате чего

какое-то время на сайт невозможно было зайти, а мобильное приложение работало некорректно. Также в третьем квартале 2019 года нападению подвергся популярный информационный ресурс Wikipedia. Атака началась вечером 6 сентября, в результате чего крупнейшая онлайн-энциклопедия оказалась временно недоступна пользователям в ряде стран Европы, Африки и Ближнего Востока. Wikipedia атакуют достаточно часто, однако это нападение отличалось тем, что, по предварительным данным, достигало мощности более терабита в секунду и продолжалось целых три дня [2].

Несмотря на то, что подобного вида атаки имеют ряд новых и сложных методов реализации, которые могут вызвать много неблагоприятных последствий и содействовать достижению целей злоумышленника, во всех перечисленных случаях за третий квартал 2019 года организация и механизмы произведенных атак основаны на традиционных методиках и алгоритмах ввиду их простоты и эффективности. Основываясь на результатах анализа мировой статистики, отмечен ряд параметров, которые позволяют определять начальные этапы процесса реализации DDoS атаки.

Целью работы является проведение имитационного моделирования поведения узла информационной сети при наличии DDoS атаки. К данным, описывающим поведение узла информационной сети, относится изменение уровня нагрузки оперативной памяти сетевого устройства, уровня нагрузки его центрального процессора, количества запросов (пакетов) в секунду и количества сетевых соединений, установленных устройством. Необоснованно резкое повышение показателей нескольких параметров свидетельствует об аномальном поведении наблюдаемого узла сети [3].

Опираясь на статистические данные работы любого сетевого информационного узла, необходимо учитывать, что повышение нагрузки не всегда является DDoS атакой [4]. Предполагается, что при работе узла сети возможны всплески показателей нагрузки, но их возникновение является асинхронным и краткосрочным по времени, и не является при этом каким-либо вредоносным воздействием на узел и сеть в целом. Сигналом начала DDoS атаки является превышение как минимум двух показателей нагрузки узла информационной сети продолжительностью от 5 секунд.

В качестве метрики определения появления аномалий на узле информационной сети был выбран допустимый порог превышения нагрузки для каждого из параметров. Так, например, для уровня нагрузки центрального процессора устройства выбран порог, равный 80 %, нагрузки оперативной памяти устройства, равный 60 %, количества запросов (пакетов) в секунду, равного 2 000 пакетам в секунду, и количества сетевых соединений, установленных устройством, равный 90 %.

Целью проведения имитационного моделирования является генерация сценария работы узла информационной сети при нормальных условиях

и при появлении DDoS атаки. Для построения модели поведения был выбран высокоуровневый язык программирования Python. В качестве механизма создания показателей выбрана технология генерации случайных чисел. Это обосновывается значительной экономией времени для создания единичного сценария поведения узла информационной сети. Для удобства отображения и отслеживания показателей была использована библиотека Matplotlib. Для работы с моделью разработан простой графический интерфейс с функционалом из нескольких пунктов:

– функция генерации показателей отслеживаемых параметров при нормальном функционировании информационной сети;

– функция генерации показателей отслеживаемых параметров при DDoS атаке;

– функция записи результатов генерации в файлы.

Результаты моделирования представлены на графиках, демонстрирующих изменение значений исследуемых параметров относительно времени. Продолжительность генерации данных при наличии DDoS атаки является случайной.

При моделировании генерировались следующие показатели поведения сетевого устройства в разных условиях: параметр уровня нагрузки центрального процессора, уровня нагрузки оперативной памяти, количества сетевых соединений, установленных устройством сети, и количества запросов (пакетов) в секунду.

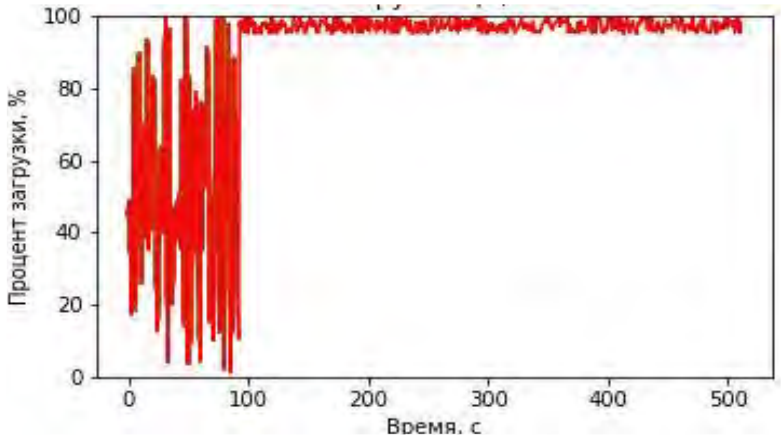


Рис. 1. Уровень нагрузки центрального процессора

В случае нагрузки центрального процессора (рис. 1) наблюдается неоднозначность работы системы. Очевидный резкий рост и дальнейшее поддержание уровня нагрузки выше выбранного предела является признаком проводимой *DDoS* атаки.

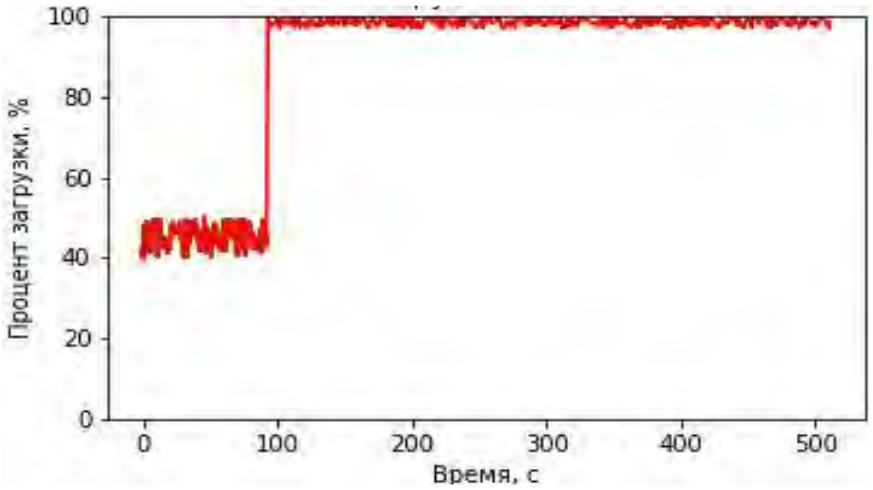


Рис. 2. Уровень нагрузки оперативной памяти

При DDoS атаке узел сети тратит ресурсы памяти для обработки больших объемов поступающего трафика или всевозможного анализа приходящей информации (рис. 2).

При реализации DDoS атаки растет количество возможных соединений с сетевым устройством (рис. 3), которое при этом не успевает их обрабатывать, вследствие чего становится недоступным для подключения к нему реальных пользователей.

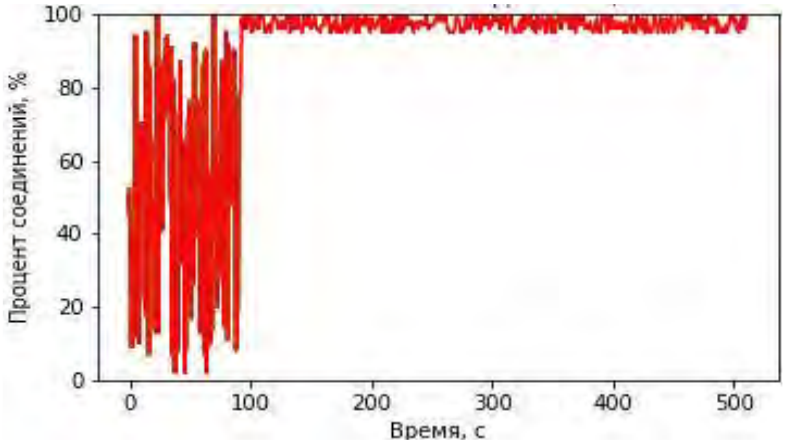


Рис. 3. Количество сетевых соединений

Резкий рост количества запросов (пакетов) в секунду (рис. 4) на 100 секунде нормальной работы информационной сети свидетельствует о появлении DDoS атаки. Количество запросов колеблется в тех пределах, в которых устройство начинает исчерпывать свои вычислительные ресурсы и в результате прекращает работу.

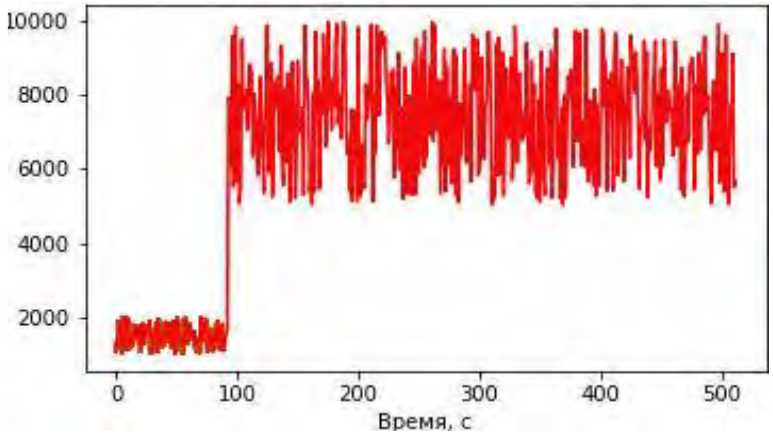


Рис. 4. Количество запросов (пакетов) в секунду

Разработанная модель позволяет продемонстрировать состояние узла информационной сети при реализации DDoS атаки. При этом на графиках изменения показателей каждого из выбранных параметров существует возможность отчетливо увидеть разницу между штатным функционированием информационной сети и аномальными событиями. В данном случае аномальные отклонения особенно ярко выражены на графиках изменения уровня нагрузки оперативной памяти устройства сети (рис. 2) и количества запросов (пакетов) в секунду (рис. 4).

Представленные результаты моделирования планируется использовать в обучении искусственной нейронной сети обнаружению DDoS атак для разработки системы защиты информационных сетей.

Список используемых источников

1. РД 21-02-2006. Типовая инструкция о защите информации в автоматизированных средствах центрального аппарата, территориальных органов и организаций федеральной службы по экологическому, технологическому и атомному надзору. М. : Ростехнадзор, 2006. 43 с.

2. Отчет о проводимых DDoS атаках за квартал 2019 года [Электронный ресурс]. URL: https://securelist.ru/ddos-report-q3-2019/94981/ (дата обращения: 13.02.2020).

3. Зуев В. Н., Ефимов А. Ю. Нейросетевой поведенческий анализ действий пользователя в целях обнаружения вторжений уровня узла // Программные продукты и системы. 2019. Т. 32. № 2. С. 258–262.

4. Бажаев Н. А., Лебедев И. С., Кривцова И. Е. Анализ статистических данных мониторинга сетевой инфраструктуры для выявления аномального поведения локального сегмента системы // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 1. С. 92–99.

УДК 004.048
ГРНТИ 49.33.35

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ МЕТОДА ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Н. В. Евглевская

Военная академия связи

В статье представлены результаты исследования, посвященного выбору архитектуры искусственной нейронной сети, анализу входных и выходных данных, выбору активационной функции, алгоритма обучения искусственной нейронной сети, предназначенной для решения задач обнаружения компьютерных атак. Для обнаружения компьютерных атак, в частности DoS-атак, использовалась технология обнаружения аномального поведения. С целью определения структуры сети, была проведена серия машинных экспериментов, результаты которых представлены в данной работе.

метод обнаружения атак, искусственная нейронная сеть, компьютерная атака, DoS-атака.

Преимуществом использования искусственных нейронных сетей (ИНС) в отличие от других методов обнаружения компьютерных атак является их способность анализировать данные, даже если они являются неполными или искаженными. Нейронные сети имеют возможность учиться на предшествующих событиях, за счет чего достигается высокая эффективность и адаптивность систем обнаружения атак [1].

В данной статье представлены результаты исследования, связанного с выбором структуры ИНС для решения поставленной задачи, анализом входных и выходных данных, выбором активационной функции, алгоритма обучения ИНС.

На сегодняшний день не существует определенной процедуры для выбора архитектуры ИНС (количества слоев и количества нейронов в слоях сети). Чем больше количество нейронов и слоев, тем шире возможности ИНС, тем медленнее она обучается и работает и тем более нелинейной может быть зависимость вход-выход [2].

Количество нейронов и слоев связано:

– со сложностью задачи;
– с количеством данных для обучения;
– с требуемым количеством входов и выходов сети;

– с имеющимися ресурсами: памятью и быстродействием машины, на которой моделируется сеть.

Применимость эмпирических формул для расчета числа слоев и нейронов на практике имеет весьма ограниченную применимость [2, 3].

В связи с этим, для определения структуры ИНС, предназначенной для выявления DoS-атак, была проведена серия машинных экспериментов по тестированию ИНС, результаты которых представлены на рис. 1, 2, 3. Качество тестирования оценивалось такими критериями, как величина минимума максимальной ошибки тестирования при DoS-атаке и средней квадратической ошибки обучения.

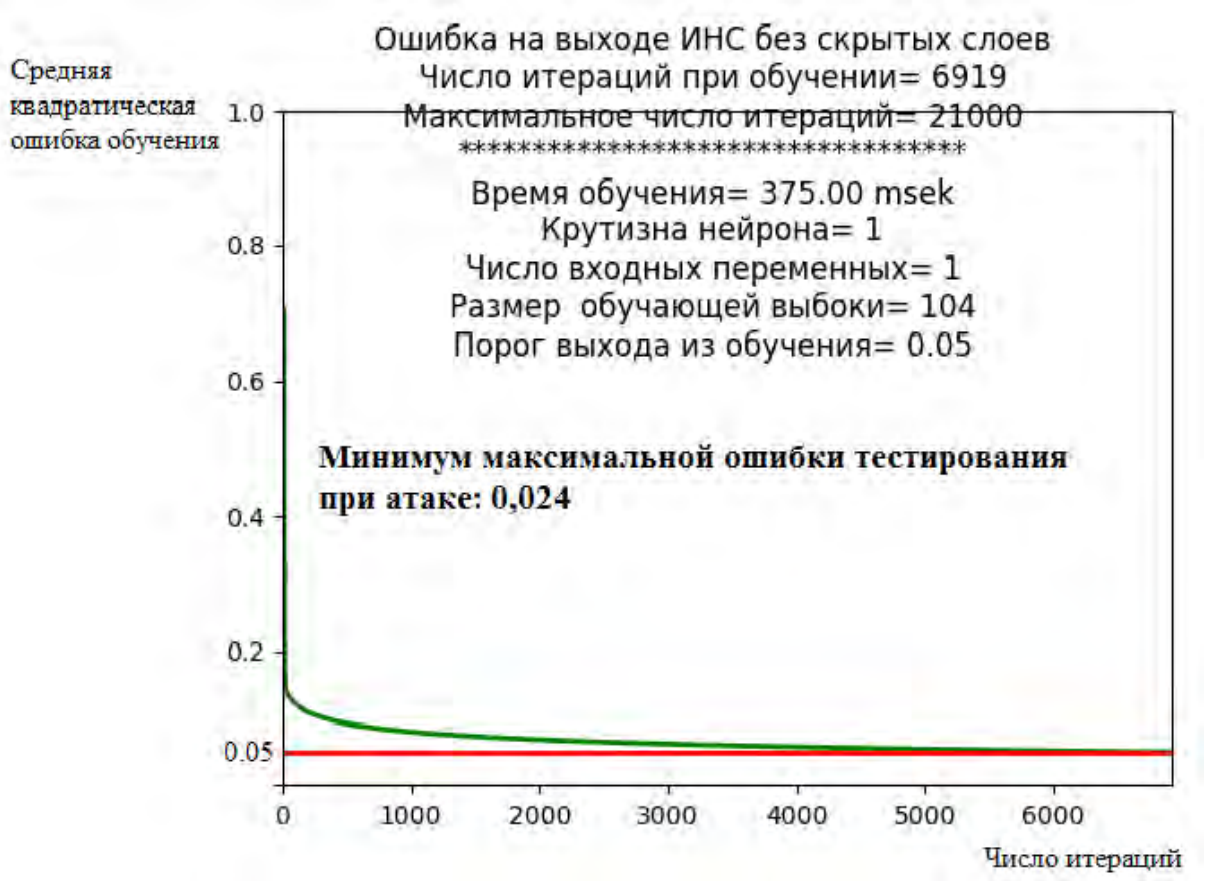


Рис. 1. Результаты тестирования ИНС с одним входным параметром без скрытых слоев

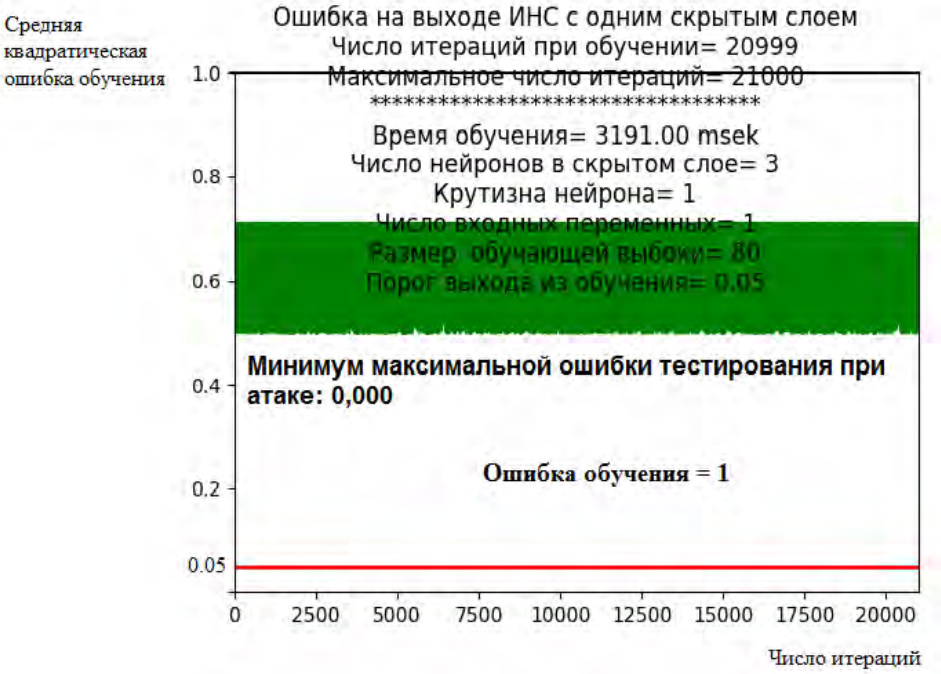


Рис. 2. Результаты тестирования ИНС с одним входным параметром и одним скрытым слоем

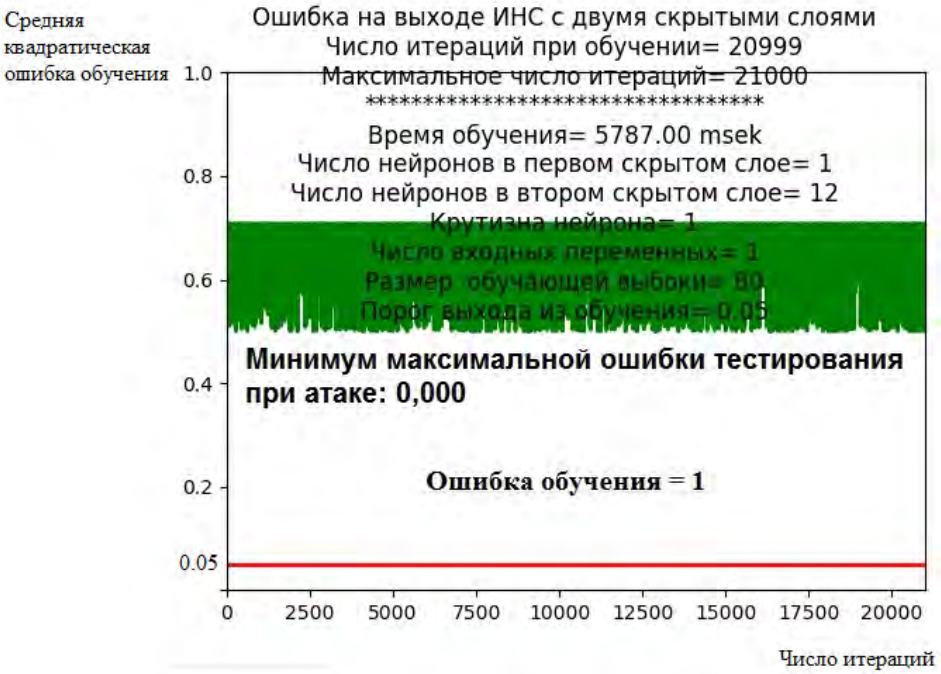


Рис. 3. Результаты тестирования ИНС с одним входным параметром и двумя скрытыми слоями

Из графиков, представленных на рис. 1–3, видно, что минимум максимальной ошибки тестирования при атаке равен 0 и средняя квадратическая ошибка обучения достигает заданного значения 0,05 в случае, представленном на рис. 1, что позволяет сделать вывод о том, что для решения задачи

обнаружения DoS-атак целесообразно использовать структуру ИНС без скрытых слоев. Пример такой сетевой структуры представлен на рис. 4.

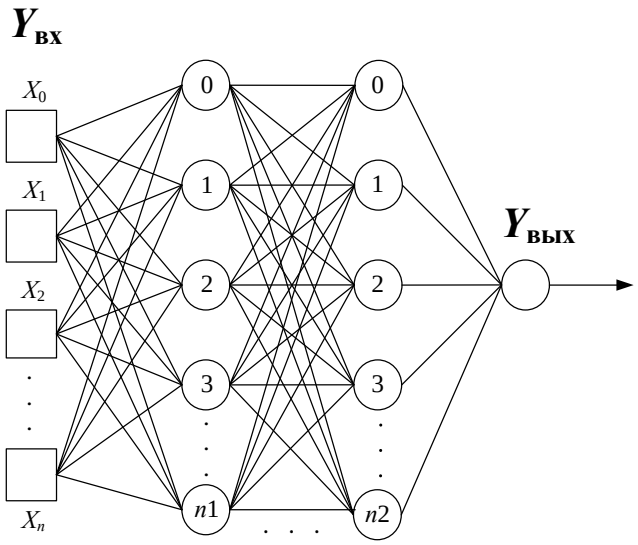


Рис. 4. Выбранная структура ИНС

На рис. 4 обозначено: X_i – входные параметры (i = от 1 до n), X_0 – нейрон смещения ($X_0 = -1$), $Y_{вых}$ – принимает значения 0 или 1.

В качестве метода обучения ИНС выбран градиентный метод обратного распространения ошибки, позволяющий минимизировать среднюю квадратическую ошибку обучения сети [4].

Функцией активации является сигмоидная функция, представленная формулой (1):

$$y = \frac{1}{1+e^{-x}}. \quad (1)$$

На рис. 5 показан график сигмоидной функции.

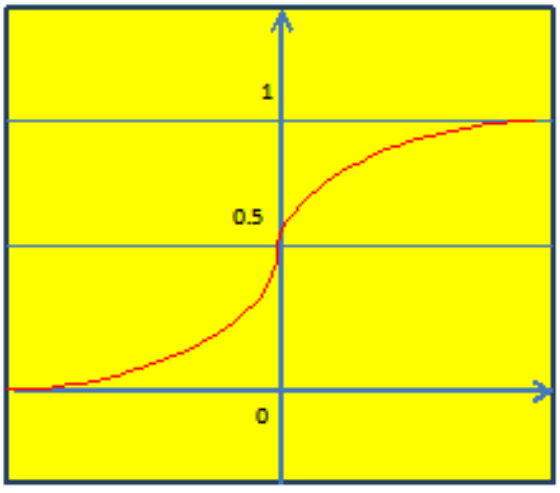


Рис. 5. График сигмоидной функции

Поскольку результат в выходном слое ИНС заранее известен, алгоритмом для обучения нейронной сети является алгоритм обучения «С учителем».

Список используемых источников

1. Евглевская Н. В., Лаута О. С., Михаил И. И. Обнаружение *DoS*/*DDoS*-атак на основе метода искусственных нейронных сетей // Транспорт России: проблемы и перспективы: материалы Международной научно-практической конференции, Санкт-Петербург, 12–13 ноября 2019 г. СПб. : Иптран, 2019. Том 1. С. 421–424.

2. Ясницкий Л. Н. Введение в искусственный интеллект. М. : Академия, 2005. 176 с.

3. Заенцев И. В. Нейронные сети: основные модели: учеб. пособие. Воронеж, 1999. 76 с.

4. Архангельская Е., Кадурин А., Николенко С. Глубокое обучение. Погружение в мир нейронных сетей. СПб. : Питер, 2018. 480 с.

УДК 004.773.5
ГРНТИ 20.15.13

АНАЛИЗ ХАРАКТЕРИСТИК ДОПОЛНИТЕЛЬНЫХ УСЛУГ НА СЕТИ СВЯЗИ МОБИЛЬНОГО ОПЕРАТОРА

В. С. Елагин, Д. А. Ребров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье описывается одна из наиболее популярных дополнительных услуг на сети мобильного оператора. Указаны ее основные особенности, способ построения и основные характеристики, влияющие на работу сервиса в целом. Описаны все элементы сети, которые задействованы в реализации услуги, и цели, которые преследуются при внедрении этих элементов.

Проведен анализ основные характеристик, которые влияют на предоставление сервиса. Описаны способы изменения и улучшения данных характеристик для достижения необходимого качества предоставляемых услуг.

дополнительные услуги, сеть оператора, SIP, UDP.

Каждый владелец мобильного телефона может констатировать, что количество предлагаемых операторами сотовой связи дополнительных услуг постоянно увеличивается. Ассортимент дополнительных услуг, или в международной терминологии Value Added Services (VAS), сотовой связи расширяется по мере увеличения пропускной способности сетей.

Сейчас пропускная способность сети на сетях мобильных операторов, позволяет в любой точки страны пользоваться услугами по получению контента и взаимодействия с другими пользователями. Поэтому в нашей повседневной жизни все чаще появляются дополнительные услуги (Номер 8800, короткая нумерация и т. д.). Но все эти услуги требуют отпрядённые настройки и характеристики сети для их успешного функционирования.

Основной и, на мой взгляд, главной дополнительной услугой в наше время является услуга «Мультифон».

Мультифон – услуга, которая позволяет организовать IP-телефонию в офисе и совершать вызовы через интернет. Вы сможете подключить любое оборудование, поддерживающее протокол SIP и начать совершать вызовы через сеть Интернет.

Разумеется, что у данной схемы есть недостатки:

1. Использование протокола SIP сильно зависит от качества интернета.

2. Так как SIP работает с использованием транспортного протокола UDP (негарантированная доставка пакетов), соответственно, при разговоре могут появляться шумы или отсутствовать звук (эффект «кваканья») [1, 2].

Но как уже говорилось ранее, мобильная сеть операторов имеет достаточно хорошее покрытие и высокую полосу пропускания, что минимизирует данные проблемы.

Для проверки данной гипотезы проведем проверку вызовов совершенных с мобильного устройства с использованием услуги «Мультифон».

Пример вызова:

2020-03-27 12:36:00.06 INV 79********* -> 79********* Answered: 51 sec

Информация о процессе установления вызова (на участке сети, отличном от обычного голосового вызова) показана на рис.

Рис. Процесс установления SIP соединения.

Выборочно просмотрим заголовки и тело сообщений:

1. 2020-03-27 12:36:00.06
access.mnogomebeli > DM-ML-SBC-TRUNK
INVITE sip:79**********@10.250.245.226:5060 SIP/2.0
Via: SIP/2.0/UDP 10.64.0.5:5060;branch=z9hG4bKD5A141106
Remote-Party-ID: "79**********"
<sip: 79**********@10.64.0.5>;party=calling;screen=no;privacy=off
From: "79**********" <sip: 79**********@10.64.0.5>;tag=33EE4510-C38
To: <sip: 79**********@10.250.245.226>
Date: Fri, 27 Mar 2020 09:36:00 GMT
Call-ID: 33C728C5-6F4511EA-A8469C56-97AE4E95@10.64.0.5
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Min-SE: 1800
Cisco-Guid: 0868670129-1866797546-2822806614-2544782997
User-Agent: Cisco-SIPGateway/IOS-15.7.3.M3

Первое сообщение INVITE отправляется со стороны пользователя на сервер Мультифон. По нему мы можем понять, какой абонент и кому совершает вызов. Далее следует сообщение SDP протокола, которой используется для передачи RTP информации [2, 8].

Content-Type: application/sdp
v=0
o=CiscoSystemsSIP-GW-UserAgent 1906 4710 IN IP4 10.64.0.5
s=SIP Call
c=IN IP4 10.64.0.5
t=0 0
m=audio 29586 RTP/AVP 8 101 19
c=IN IP4 10.64.0.5
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:19 CN/8000
a=ptime:20

Сообщение ACK отправляется пользователем непосредственно перед передачей речи. Это конечное сообщение при установлении соединения по протоколу SIP.

25. 2020-03-27 12:36:0.450
access.mnogomebeli > DM-ML-SBC-TRUNK

ACK sip:10.250.245.226:5060;yop=00.00.8B294863.0000.7031;transport=udp SIP/2.0
Via: SIP/2.0/UDP 10.64.0.5:5060;branch=z9hG4bKD5A35703
From: "79*********" <sip: 79*********@10.64.0.5>;tag=33EE4510-C38
To: <sip: 79*********@10.250.245.226>;tag=4ZCUZCbXDU04_165

Получается, что установление соединения при вызове через сеть передачи данных будет дольше на 451 мс в сравнении с обычным телефонным вызовом.

Тогда возникает вопрос, какого качества при этом будет речь и сеанс связи в целом.

Для этого проверим показатели RTP трафика в момент непосредственно разговора [5, 7] (табл. 1, 2).

ТАБЛИЦА 1. Исходящие показатели

"trunk": "user"	Направление вызова, в этом случае от пользователя
"direction": "ingress"	Название программной процедуры
"from": "79*********"	Телефонный номер стороны А
"to": "79*********"	Телефонный номер стороны В
"start": "Fri Mar 27 2020 12:36:06 GMT+0300 (MSK)"	Время начала сеанса связи
"reordered_packets": 0	Количество повторно отправленных пакетов
"lost_packets": 0	Количество потерянных пакетов
"in_jitter": 23	Среднее изменение задержек отправленных пакетов
"out_jitter": 15	Среднее изменение задержек полученных пакетов

Соответственно, по показателю "lost_packets" = 0, видим, что на исходящей стороне не зафиксировано ни одного потерянного пакета [3, 9].

ТАБЛИЦА 2. Входящие показатели

"trunk": "053f149be6b444c0b74ad9539fe5dbc9"	Направление вызова, в этом случае к пользователю
"direction": "egress"	Название программной процедуры
"from": "79*********"	Телефонный номер стороны А
"to": "79*********"	Телефонный номер стороны В
"start": "Fri Mar 27 2020 12:36:06 GMT+0300 (MSK)"	Время начала сеанса связи
"reordered_packets": 0	Количество повторно отправленных пакетов
"lost_packets": 0	Количество потерянных пакетов
"in_jitter": 35	Среднее изменение задержек отправленных пакетов
"out_jitter": 15	Среднее изменение задержек полученных пакетов

По указанным данным, можно сделать вывод, что система вносит минимальные значения задержек и их отклонения в систему (на исходящей стороне: "in_jitter": 23 мкс, "out_jitter": 15 мкс и на входящей стороне: "in_jitter": 35 мкс,"out_jitter": 15 мкс).

Также, на входящей стороне значение "lost_packets" тоже равно нулю, что говорит о том, что в процессе обмена речевой информацией проблем в передаче пакетов не возникло, и речевая информация была передана без искажений или повреждений [5, 9].

Вывод

Сети современных мобильных операторов предназначены для развития и активного использования VAS услуг без каких-либо ограничений. Задержки и помехи, которые система вносит в такие взаимодействия, максимально приближены к нулю и позволяют абонентам отказываться от обычной телефонии в пользу VoIP телефонии [7, 10].

Но большее удобство и выгоду данная технология несет корпоративному бизнесу. Для компаний VoIP телефония позволяет добиться таких преимуществ как [6, 8]:

1. Масштабируемость сети – позволяет строить офисную структуру вне зависимости от масштабов бизнеса и по необходимости включать новых сотрудников или удалять старых вне зависимости от территориального расположения.

2. «Независимость от расстояния» – сотрудники компании могут быть территориально разнесены при этом находиться в рамках одной компании и пользоваться услугой на общих условиях (выгодно для контакт центров или крупных компаний)

3. Управление данными – появляется возможность контролировать данные в рамках компании, например, запись разговоров, для дальнейшей оценки качества работы компании.

Соответственно, это основной вектор развития, который сейчас активно внедряется во многих IT компаниях, который позволяет удешевить и упростить работу разнесенных офисов [3, 4].

Список используемых источников

1. Гольдштейн Б. С., Зарубин А. А., Саморезов В. В. Протокол SIP: справочник. СПб. : БХВ-Петербург, 2005. 456 с.

2. Гольдштейн Б. С., Пинчук А. В., Суховицкий А. Л. IP-Телефония. СПб. : БХВ-Петербург, 2001. 336 с. ISBN: 978-5-9775-3341-6.

3. Elagin V. S., Onufrienko A. V. How can an operator make money on OTT services and what does SDN have to do with it? // T-Comm – Telecommunications and Transport. 2017. Vol. 1. PP. 17–21.

4. Antonopoulos A. M. Mastering Bitcoin, O'Reilly Media Inc, 2017. 416 p.

5. Buinevich M. V. Problem issues and trends in is supply in the field of telecommunications // Protection of information. Insider. 2017. Vol. 1 (73). PP. 49–55.

6. Guan, Y. and Ge, X. Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks // in IEEE Transactions on Signal and Information Processing over Networks. March 2018. Vol. 4. No. 1. PP. 48–59.

7. Goldstein A. B., Zarubin A. A., Onufrienko A. V., Elagin V. S. and Belozertsev I. A., Synchronization of delay for OTT services in LTE // 2018 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Minsk, 2018, pp. 1–4, July 04-05, 2018.

8. Goldstein A. B., Sokolov N. A., Elagin V. S., Onufrienko A. V. and Belozertsev I. A. Network Characteristics of Blockchain Technology of on Board Communication // 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 2019, pp. 1–5, March 20–21, 2019.

9. Elagin V. S., Belozertsev I. A., Goldshtein B. S., Onufrienko A. V. and Vladyko A. G. Models of QOE ensuring for OTT services // 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 2019, pp. 1–4, March 20–21, 2019.

10. Makolkina M., Koucheryavy A., Paramonov A. Investigation of Traffic Pattern for the Augmented Reality Applications // Lecture notes in computer science. 2017. Vol. 10372. PP. 233–246.

УДК 681.518.5
ГРНТИ 50.43.19

АЛГОРИТМ КОНТРОЛЯ ДОСТУПНОСТИ ТРЕБУЕМЫХ НАВИГАЦИОННЫХ ХАРАКТЕРИСТИК WAAS НА БАЗЕ ИСПОЛЬЗОВАНИЯ СРЕДСТВ ЛОКАЛЬНЫХ ДИФФЕРЕНЦИАЛЬНЫХ СИСТЕМ

А. В. Ершов, Р. В. Миргородский, М. И. Носов, Б. В. Шурыгин

Военная академия связи

Рассмотрена актуальная проблема контроля доступности требуемых навигационных характеристик GNSS в реальном времени, решение которой требуется для автоматизации движения железнодорожного состава. Проанализированы основные подходы к контролю доступности THX пользователей широкозонной дифференциальной системы WAAS, который используется как прототип. Показано, что использование ШДС может привести к заниженной ожидаемой доступности THX в сравнении с реальной ситуацией. Предлагается вместо сети опорных станций ШДС, использовать локальные дифференциальные системы и прямые измерения локально-зависимых погрешностей измерения дальностей. При этом можно достичь значительного улучшения точности позиционирования. Предложен модернизированный алгоритм определения уровней защиты с использованием данных от ЛДС.

доступность, требуемые навигационные характеристики, дальномерные погрешности, алгоритм, контроль, система, модернизация.

Полномасштабное внедрение ГЛОНАСС на железнодорожном транспорте открывает широкие перспективы для использования всех потенциальных преимуществ координатного метода автоматического регулирования движения. Существует ряд проблем, которые препятствуют внедрению интеллектуальной транспортной системы на базе спутниковой навигации на Российских железных дорогах. К этим проблемам относятся: фактическая непредсказуемость текущей точности позиционирования, ограничения на использование точных геопространственных данных [1].

Необходимым условием обеспечения требуемых навигационных характеристик (ТНХ) на транспорте является использование функциональных дополнений ГЛОНАСС – локальных и широкозонных дифференциальных систем. Средства дифференциальной навигации обеспечивают, как высокую точность позиционирования, так и эффективный контроль доступности ТНХ в реальном масштабе времени [2].

В настоящее время наиболее известным и открытым для независимых исследований типом ШДС является американская дифференциальная система WAAS, которая поддерживает высокие ТНХ пользователей GPS в пределах рабочей зоны, охватывающей территорию США и Канады [3].

Рассмотрен принцип построения алгоритма контроля доступности ТНХ, используемый в аппаратно-программном комплекса ШДС, который далее используется как прототип для решения задач ж/д транспорта.

Максимально допустимые погрешности позиционирования образуют границы «цилиндра безопасности» – области пространства, в пределах которой должен находиться пользователь, чтобы не нарушить ТНХ (рис. 1).

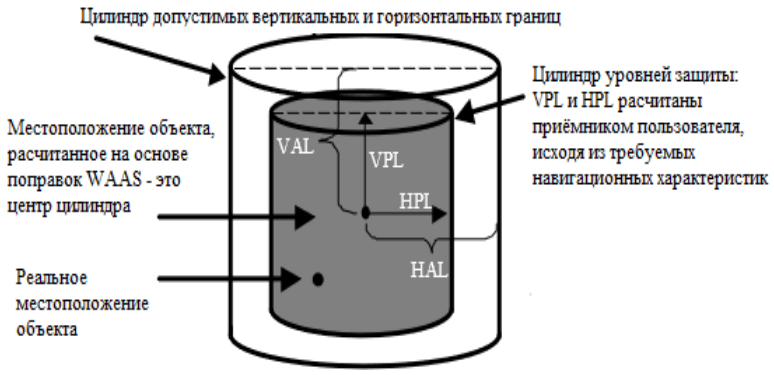


Рис. 1. Концепция «цилиндра безопасности»

Где HPL и VPL – горизонтальный и вертикальный уровень защиты.

Алгоритм оценки доступности ТНХ в плане и по высоте, используемый в WAAS имеет следующий вид [4]:

$$HPL = \begin{cases} K_{HNPA} \times D_{mjr} \\ \text{or} \\ K_{HPA} \times D_{mjr} \end{cases}; \quad VPL = K_{VPA} \times D_V, \tag{1}$$

$$D_{mjr} = \sqrt{\frac{D_X^2 + D_Y^2}{2} + \sqrt{\left(\frac{D_X^2 - D_Y^2}{2}\right)^2 + D_{XY}^2}}, \tag{2}$$

$$D_X^2 = \sum_{i=1}^{N} S_{X,i}^2 \times \sigma_i^2; \quad D_Y^2 = \sum_{i=1}^{N} S_{Y,i}^2 \times \sigma_i^2; \quad D_V^2 = \sum_{i=1}^{N} S_{V,i}^2 \times \sigma_i^2, \tag{3}$$

$$D_{XY} = \sum_{i=1}^{N} S_{X,i} \times S_{Y,i} \times \sigma_i^2, \tag{4}$$

$$\mathbf{S} = \begin{vmatrix} S_{X,1} & S_{X,2} & ..... & S_{X,N} \\ S_{Y,1} & S_{Y,2} & ..... & S_{Y,N} \\ S_{V,1} & S_{V,2} & ..... & S_{V,N} \\ S_{t,1} & S_{t,2} & ..... & S_{t,N} \end{vmatrix} = \left(\mathbf{G}^T \times \mathbf{W} \times \mathbf{G}\right)^{-1} \times \mathbf{G}^T \times \mathbf{W}, \tag{5}$$

где K_{HNPA}, K_{HPA}, K_{VPA} – это коэффициенты доверительной вероятности при оценке погрешности позиционирования разных категорий точности; D_{mjr} – длина проекции главной полуоси проекции эллипса рассеяния погрешности позиционирования на плоскость в локальной системе; D_x, D_y, D_{xy}, D_v – полуоси эллипса рассеивания погрешности позиционирования в направлении на восток, север и по высоте.

S – проекционная матрица для решения навигационной задачи методом наименьших квадратов; $\mathbf{G}_i = [-\cos El_i \times \cos Az_i \; -\cos El_i \times \sin Az_i \; -\sin El_i \times 1]$ – i-й столбец матрицы G; El_i – угол места i-го дальномерного источника (в градусах); Az_i – азимут i-го дальномерного источника (в градусах);

$\mathrm{W}^{-1} = \begin{matrix} w_1 & 0 & \cdots & 0 \\ 0 & w_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & w_i \end{matrix}$ – матрица весовых коэффициентов измерений по спутникам; $w_i = 1/\sigma_i$ – весовой коэффициент, соответствующий i-му спутнику; σ_i – среднеквадратическое отклонение ионосферных дальномерных погрешностей для i-го спутника.

Использование выражений при оценивании текущей доступности ТНХ средствами WAAS необходимо начинать с известного значения СКО дальномерных погрешностей и последовательно рассчитывать параметры.

Входными данными, которые сообщаются через геостационарные спутники WAAS пользователям системы для определения уровней защиты

HPL и VPL, являются компоненты относительной дальномерной погрешности по каждому из видимых спутников GPS (UDRE) и соответствующая вертикальная ионосферная погрешность (GIVE) [5].

Очевидно, что надежность контроля доступности THX WAAS зависит от того, насколько модели компонент дальномерных погрешностей UDRE и GIVE соответствует реальным условиям определения местоположения. Соответственно, точность определения местоположения пользователя особенно уязвима к возмущениям в ионосфере.

Оценка величины GIVE во всей рабочей зоне WAAS по одному и тому же алгоритму может оказаться некорректной и вести к завышенным значениям уровней защиты VPL и HPL и, соответственно, к заниженной ожидаемой доступности THX в сравнении с реальной ситуацией. Эта проблема может быть решена с помощью использования локальных дифференциальных систем (ЛДС) [6].

В связи с отсутствием в широком доступе информации об алгоритмах контроля доступности THX существующих ЛДС, предлагается использовать алгоритм WAAS и провести модернизацию для использования на железнодорожном транспорте по двум направлениям:

а) модернизация собственно алгоритма (оставляем только горизонтальную плоскость и решаем задачу в системе координат «путевая ордината-угол эллипса рассеивания»);

б) модернизация опорного сегмента: вместо сети опорных станций ШДС, декомпозиции и интерполяции «локально-зависимых» компонент дальномерных погрешностей предлагается использовать локальные дифференциальные системы и прямые измерения локально-зависимых погрешностей измерения дальностей.

Для проведения исследований были использованы архивы данных измерений радионавигационных параметров в формате RINEX 2.0 с 30-ти секундным временным разрешением. Каждый файл данных содержал суточные измерения всех видимых спутников GPS на одной из стационарных станций, расположенных в двух областях зоны покрытия WAAS: Аляска и CONUS. Для исследования были выбраны 12 объектов на территории Аляски и 70 объектов на территории CONUS. Карта расположения опорных станций приведена на рис. 2.

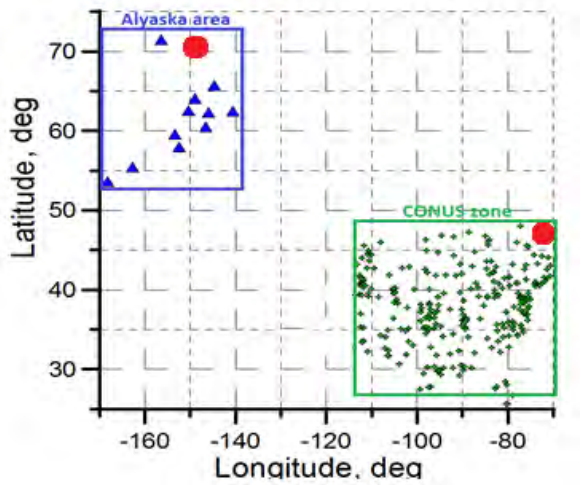


Рис. 2. Карта расположения опорных станций

В программном комплексе MATLAB был разработан алгоритм обработки указанных данных. Для демонстрации работоспособности алгоритма и оценки доступности ТНХ были выбраны 2 станции, которые помечены на рисунке 18 красными точками:

– ALBH (широта: 49.111257; долгота: -68.154798; высота: 27.48);

– HOLM (широта: 70.7363; долгота: -151.76124 высота: 0.43).

Они находятся друг от друга на значительном расстоянии, что позволит наблюдать результат в разных условиях измерений. На рис. 3 представлен пример результата работы алгоритма для станции ALBH.

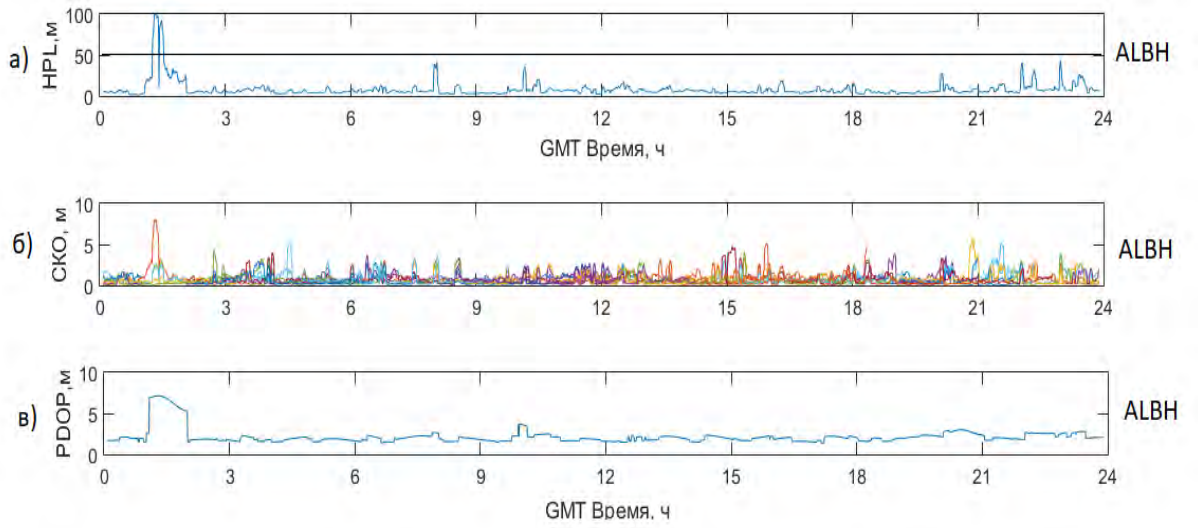


Рис. 3. Исследование уровня защиты для станции ALBH

На рис. 3 показаны:

а) зависимость уровня погрешности позиционирования от времени;

б) среднеквадратичное отклонение ионосферной погрешности;

в) геометрический фактор PDOP.

Можно видеть, что уровень защиты HPL нарушается один раз в период первых 3 часов суток. В это время пользователь должен получать уведомление о том, что погрешность превышает допустимые пределы. Так как входными данными являлись СКО погрешностей, можно проследить взаимосвязь между графиками а и б, по которым видно, что основные всплески и спады уровня защиты, погрешностей и геометрического фактора совпадают по времени. Это говорит о корректной работе разработанного алгоритма.

Аналогичные исследования были проведены для станции HOLM. Результат работы алгоритма изображён на рис. 4 (см. ниже).

На рис. 4 взаимосвязь графиков а и б не такая очевидная. В периоды 0–7 ч, 21–24 ч, наблюдается превышение уровня защиты 6 раз и увеличение значения СКО по большей части видимых спутников. Однако в период с 9 по 21 ч HPL не выходит за допустимые пределы, хотя на графике показан

уровень СКО ионосферной погрешности, превышающий 5 метров. Это вызвано тем, что повышение значения СКО ионосферной погрешности одного или двух спутников в пределах 5 метров по сравнению с данными от остальных спутников не оказывает решающего влияния на точность позиционирования. Значение PDOP в течение 24 часов не превышает 5, однако HPL был превышен 6 раз, что говорит о худшем состоянии ионосферы и условий наблюдения по сравнению со станцией ALBH.

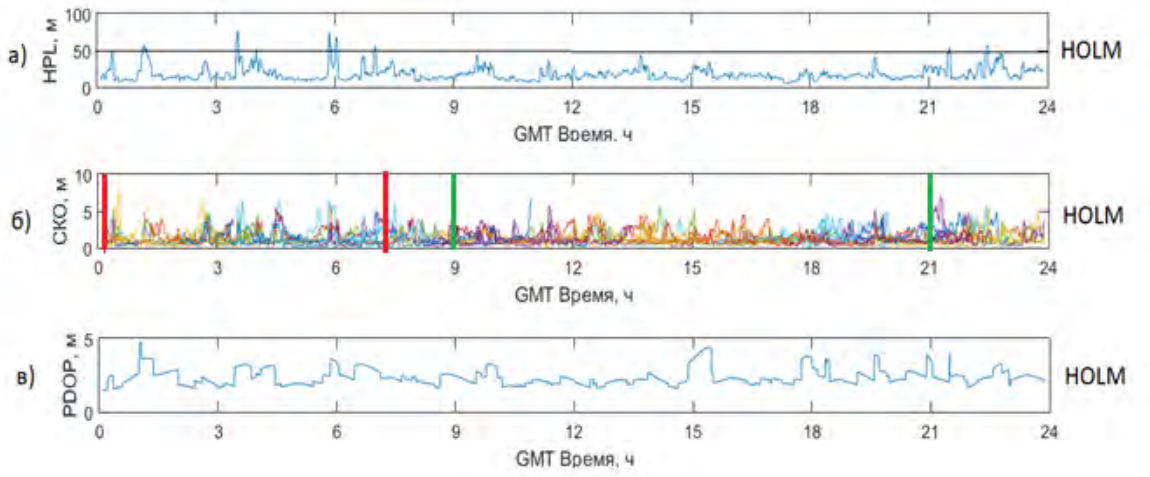


Рис. 4. Исследование уровня защиты для станции HOLM

Заключение

Таким образом, успешно была проведена проверка работоспособности алгоритма при использовании прямых измерений локально-зависимых погрешностей измерения дальностей вместо данных от ШДС. Полученные результаты говорят о возможности использования предложенного алгоритма в составе типового ПАО интеллектуальных транспортных систем. При этом можно достичь значительного улучшения точности позиционирования на основе использования данных от локальных дифференциальных систем, а также обеспечить своевременное предупреждения пользователя о превышении допустимых пределов погрешности позиционирования.

Список используемых источников

1. Тяпкин В. Н., Гарин Е. Н. Методы определения навигационных параметров подвижных средств с использованием спутниковой радионавигационной системы ГЛОНАСС. Изд-во: СФУ, 2012. 260 с.

2. Перов А.И . и Харисова В. Н. ГЛОНАСС: принципы построения и функционирования. М. : Радиотехника, 2005. 688 с.

3. Wide-Area Augmentation System Performance Analysis Report, July 2006. URL: http://www.nstb.tc.faa.gov/REPORTS/waaspan17.pdf.

4. Kneissl F., Stöber C., Prof. Dr.-Ing. Günter Hein Combined Integrity of GPS and Galileo, Inside GNSS, jan/feb 2010.

5. ГОСТ Р 53610-2009 Глобальная навигационная спутниковая система. Форматы передачи корректирующей информации. Технические требования.

6. Корнилов И. Н., Ергашёв Н. В. Создание локальной дифференциальной подсистемы на основе сотовой сети связи // Фундаментальные исследования. 2015. № 7-4. С. 755–759.

УДК 004.431.4
ГРНТИ 20.53.15

СПОСОБЫ ПЕРЕДАЧИ ПАРАМЕТРОВ В ПРОЦЕДУРЕ НА ОПЕРАЦИОННОЙ СИСТЕМЕ ЭЛЬБРУС

А. В. Ершов, К. И. Налимов, М. И. Носов

Военная академия связи

В данной статье рассматривается способы передачи параметров в процедуре на языке низкого уровня ассемблер на операционной системе Эльбрус. Данный вопрос можно использовать как для повышения оптимизации программы или поднятия уровня безопасности.

ключевые параметры, способы передачи, ассемблер, язык низкого уровня, оптимизация, безопасность.

В современном мире, во время написания программ, существуют несколько важных моментов, одни из которых: безопасность и производительность. Чаще всего эти два пункта не удаётся учесть и приходится выбирать что-то одно.

Попробуем рассмотреть каждый из пунктов в момент передачи параметров в процедуре, так как это место является довольно уязвимым для воздействия из вне и проблемным в плане скорости работы.

Для примера была написана простая программа на языке C++ которая производила сложения простых чисел.

```
int main()
{
	DWORD a = 0x100;
	DWORD b = 0x05;
	DWORD c = a + b;

	printf("%04x + %04x = %04x", a, b, c);

	_getch();
}
```

Рис. 1. Сложение простых чисел

Программа прошла деассемблирование после компиляции, и был получен нужный участок кода.

```
0x411849:  c7 45 f8 00 01 00 00          mov dword [ ebp + 0xfffffff8 ], 0x100
0x411850:  c7 45 ec 05 00 00 00          mov dword [ ebp + 0xffffffec ], 0x5
0x411857:  8b 45 f8                      mov eax, dword [ ebp + 0xfffffff8 ]
0x41185a:  03 45 ec                      add eax, dword [ ebp + 0xffffffec ]
0x41185d:  89 45 e0                      mov dword [ ebp + 0xffffffe0 ], eax
0x411860:  8b 45 e0                      mov eax, dword [ ebp + 0xffffffe0 ]
0x411863:  50                            push eax
0x411864:  8b 4d ec                      mov ecx, dword [ ebp + 0xffffffec ]
0x411867:  51                            push ecx
0x411868:  8b 55 f8                      mov edx, dword [ ebp + 0xfffffff8 ]
0x41186b:  52                            push edx
0x41186c:  68 14 7c 41 00          push 0x417c14 ; "%04x + %04x = %04x"
0x411871:  e8 dc fa ff ff                call 0x411a50 <function_411a50>
```

Рис. 2. Участок кода после деассемблирования

Из всех способов передачи параметров в процедуре мы рассмотрим всего 2:

– способ передачи через регистры;
– способ передачи через стек.

Способ передачи через регистры

Данный способ очень простой. Если нам нужно передать несколько параметров, то мы просто записываем их в нужные регистры и используем. Ничего сложного, но есть один большой минус. Это ограниченное количество регистров. Но зато этот способ очень быстрый в плане передачи. В плане безопасности тоже всё просто так, как данные не выходят за предел рабочей области регистров. Больше тут нечего дополнить введу простоты этого способа.

Способ передачи через стек

Для начала определимся с понятиями.

Стек – абстрактный тип данных, представляющий собой список элементов, организованных по принципу LIFO.

Способ организации стека довольно просто.

Перед вызовом процедуры параметры необходимо поместить в стек с помощью команды PUSH. Параметры помещаются в стек, начиная с последнего, так что перед вызовом процедуры на вершине стека оказывается первый параметр.

Assembler	mov dword [ebp + 0xffffff8], 0x100 mov dword [ebp + 0xffffffec], 0x5
C++	DWORD a = 0x100; DWORD b = 0x05;

Рис. 3. Первый этап

Как мы видим, компилятор размещает объявленные переменные в выделенной памяти для программы. Таким образом мы не теряем данные и можем обращаться к ним несколько раз. В обычном случае данные пришлось бы класть в регистр и не позаботившись о новых данных мы могли бы их потерять. Адресация переменных начинается с конца, что упрощает работу с ними.

Assembler	add eax, dword [ebp + 0xffffffec] mov dword [ebp + 0xfffffe0], eax
C++	DWORD c = a + b;

Рис. 4. Второй этап

Дальше данные были суммированы и записаны в память.

Assembler	mov eax, dword [ebp + 0xfffffe0] push eax mov ecx, dword [ebp + 0xffffffec] push ecx mov edx, dword [ebp + 0xffffff8] push edx push 0x417c14 ; "%04x + %04x = %04x" call 0x411a50 <function_411a50>

Рис. 5. Третий этап

И вот тут начинается самое интересное. В функции «printf("%04x + %04x = %04x", a,b,c);» у нас имеется 4 параметра. Все они записываются в стек. Строка "%04x + %04x = %04x" была записана по адресу 0x417c14 ещё на момент компиляции. Далее вызывается сама функция «printf» по адресу 0x411a50. В самом начале процедуры содержимое регистра EBP сохраняется в стеке и в него копируется значение регистра ESP. Это позволяет «запомнить» положение вершины стека и адресовать параметры относительно регистра BP.

Assembler	push ebp mov ebp, esp

Рис. 6. Завершающий этап

После идёт выполнение функции и конец программы.

Что в конечном итоге мы имеем:

– неограниченное число передаваемых параметров функции (процедуре);

– несложная организация памяти, что последним положили, то первым и взяли.

Но не всё так хорошо, как кажется на первый взгляд. У стека есть 2 минуса. Меньшая производительность, по сравнению с записью данных в регистр. Так как запись идёт в выделенную память программы. Второй минус – это безопасность. Стек уязвим к переполнению, что позволяет провести её взлом путём установки эксплойта.

Так же стоит упомянуть о том, что за стеком нужно внимательно следить. Для восстановления состояния стека до его использования подпрограммой, необходимо загрузить в регистр ESP адрес, хранящийся в EBP.

Список используемых источников

1. IndigoBits. URL: http://indigobits.com/assembler/39-sposoby-peredachi-parametrov-v-procedury.html

2. Стековый кадр [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Стековый_кадр

3. Ревич Ю. Практическое программирование микроконтроллеров Atmel AVR на языке ассемблера. 3-е изд. СПб. : БХВ-Петербург, 2014. 368 с. ISBN: 978-5-9775-3311-9.

4. Аблязов Р. З. Программирование на ассемблере на платформе x86-64. М. : ДМК Пресс, 2011. 304 с.

5. Столяров А. Программирование на языке ассемблера NASM для ОС Unix: учебное пособие. 2-е изд. М. : МАКС Пресс, 2011. 188 с.

УДК 004.056.53
ГРНТИ 81.96

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ НА ОСНОВЕ РИСК-ОРИЕНТИРОВАННОЙ МОДЕЛИ АУТЕНТИФИКАЦИИ

А. О. Жаранова, В. В. Капитоненко, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обоснована актуальность использования метода аутентификации на основе рисков. Описано влияние метода аутентификации на основе риск-ориентированного подхода на безопасность веб-приложений. Приведены преимущества использования риск-

ориентированной модели аутентификации веб-приложений в сравнении с распространенными методами защиты данных. Разработана модель аутентификации на основе рисков. Выявлены типовые параметры пользователя, необходимые для реализации защищенной аутентификации. На базе выбранных параметров описан механизм аутентификации веб-приложения на основе рисков. Определены перспективы развития риск-ориентированной модели аутентификации.

безопасность веб-приложений, аутентификация, риск-ориентированная модель аутентификации.

По статистике международного сервиса Positive Technologies, специализирующегося на разработке программного обеспечения в области информационной безопасности, общий уровень защищенности веб-приложений с каждым годом повышается, однако половина веб-приложений имеют уязвимости с высокой степенью риска. На 2019 год статистика такова: несанкционированный доступ к приложениям возможен на 39 % сайтов, 68 % веб-приложений имеют нарушения конфиденциальности данных и в 45 % обнаружены уязвимости в аутентификации. Почти треть таких уязвимостей состоит в неспособности правильно ограничить количество попыток аутентификации, что используется злоумышленниками для несанкционированного доступа к учетным данным и веб-приложениям, изменению или уничтожению данных [1].

Существует множество способов защиты аутентификации, которые увеличивают время взлома учетной записи и дают возможность защитить данные системы [2], по рекомендации NIST (Национальный институт стандартов и технологий) эффективным способом защиты является многофакторная аутентификация [3]. Однако по статистике компании Google менее 10 % пользователей пользуются двухфакторной аутентификации (2*FA*). По словам Гжегожа Милка, инженера-программиста Google, причина заключается в неудобстве применения данного метода для пользователей, так как система запрашивает дополнительные действия для аутентификации [4]. Соответственно, актуальным становится вопрос разработки модели, обеспечивающей безопасность системы без требования дополнительных действий от пользователя.

Risk-Based Authentication (RBA, риск-ориентированная модель аутентификации или аутентификация на основе рисков) – адаптивная мера безопасности для усиления аутентификации на основе паролей. RBA отслеживает дополнительные неявные атрибуты, передаваемые пользователем при вводе пароля (например, информация об устройстве или геолокации), и запрашивает дополнительные факторы аутентификации при определенном уровне риска [5]. Преимуществами данной модели являются лояльность пользователей к системе, не требующей дополнительных действий для аутентификации, и гибкость настройки модели, включающая возможность корректировки атрибутов, способов расчета оценки риска, уровней

риска и применяемых дополнительных методов защиты. Недостатком аутентификации на основе рисков является отсутствие общедоступных источников, описывающих модель, алгоритмы ее работы и используемые атрибуты.

Подобные принципы обеспечения защиты веб-ресурсов используются в таких крупных компаниях, как Google, Facebook, LinkedIn, Amazon и GOG.com, каждая из которых формирует собственный алгоритм работы системы и индивидуально выбирает атрибуты пользователя (устройства). Их модели представляют собой «черный ящик», однако по результатам исследования [5] выявлены атрибуты для расчета оценки риска.

ТАБЛИЦА 1. Модели *RBA* компаний

Название компании	Используемые атрибуты	Принцип работы аутентификации
GOG.com	IP-адрес	Полагаясь на один атрибут, ищет точное совпадение IP-адреса в базе данных. При несовпадении запрашивает дополнительный фактор аутентификации
Google	IP-адрес, параметры времени, строка User-Agent, разрешение экрана	По переданным атрибутам и извлеченной из IP-адреса геолокации рассчитывает оценку риска и сравнивает ее с историей аутентификации. При низком и среднем уровне предоставляет доступ, но при среднем отправляет пользователю предупреждение безопасности. При высоком уровне запрашивает дополнительный фактор аутентификации и при несовпадении более одного атрибута отправляет критическое предупреждение безопасности
Linkedin		
Amazon	IP-адрес	

В соответствии с описанными принципами разработана модель аутентификации на основе рисков, представленная на рис. 1. Модель сочетает в себе несколько методов обеспечения безопасности, таких как: использование черных списков с подозрительными устройствами, для которых применяются более сложные алгоритмы аутентификации, проверка IP-адреса с открытых списков источников угроз (например, *Abuse.ch*), ведение журнала аутентификации пользователей [2].

Алгоритм работы риск-ориентированной модели аутентификации представляет собой следующую последовательность действий: пользователь передает значения атрибутов, система собирает дополнительную информацию с IP-адреса и обращается к базе данных с историей аутентификаций пользователя. На основании собранной информации рассчитывается оценка риска, по которой формируется решение системы с использованием методов защиты аутентификации и занесением устройства в список подозрительных устройств при получении соответствующей оценки риска. Данный список может влиять на решение системы для включения более сложных алгоритмов аутентификации пользователя.

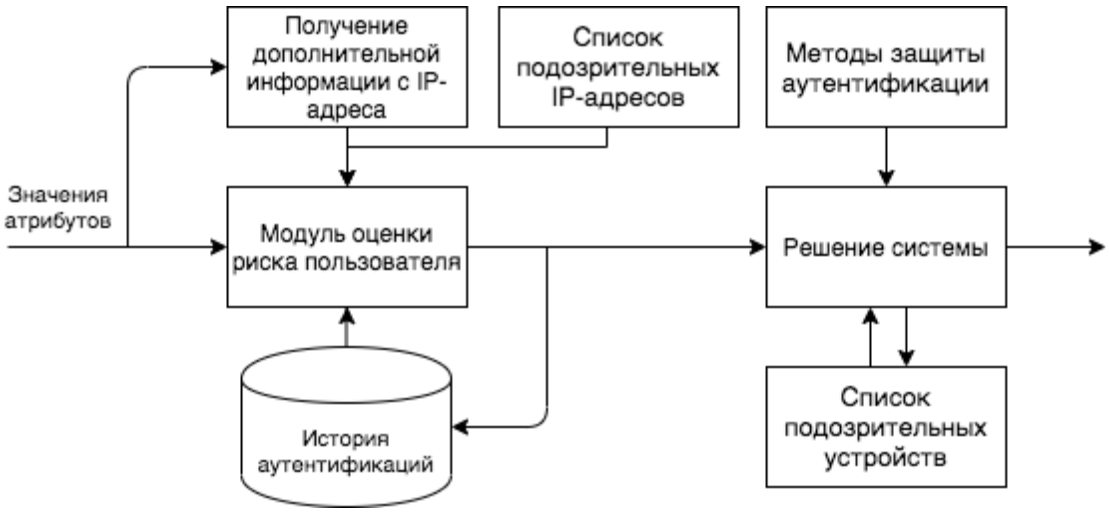


Рис. 1. Риск-ориентированная модель аутентификации

Для разработки механизма работы модели аутентификации на основе рисков определены наиболее влияющие на идентификацию устройства атрибуты [2, 6], представленные в таблице 2. Помимо атрибутов для расчета оценки риска в таблице представлены источники значений атрибутов и примеры этих значений.

ТАБЛИЦА 2. Атрибуты для расчета оценки риска аутентификации

Атрибут для расчета оценки риска	Источник значения атрибута	Пример значения атрибута
IP-адрес	HTTP Заголовок	91.23.23.22
Доступ к cookies	JavaScript	yes
User-Agent	HTTP Заголовок	Mozilla/5.0 (Linux; U; Android 2.3. 1; en-us; MID Build/GINGERBREAD) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1
Кодировка контента	HTTP Заголовок	gzip, deflate, br
Геолокация	JavaScript	(87.5545, 54.4343)
Язык	HTTP Заголовок	en-US,en;q=0.9
Длина и ширина экрана	JavaScript	1920x1200
Платформа системы	JavaScript	Linux x86_64
Часовой пояс	JavaScript	-60 (UTC+1)
Поле http_accept	HTTP Заголовок	accept="image/png, image/jpeg"
Список шрифтов	JavaScript	Arial, Helvetica, Consolas, Roboto…
Количество неудачных попыток входа за сессию	JavaScript	2

Для расчета риска без учета количества неудачных попыток аутентификации используется формула компании IBM:

$$b = \frac{\sum_{i=1} u_i}{J},$$

где u_i – вес атрибута i, неизвестный системе, J – общая сумма весов всех атрибутов, которые обрабатывает система.

Веса атрибутов оценки риска настраиваются индивидуально в зависимости от того, где используется модель. Например, если это система офиса компании, подразумевающего работу с конфиденциальными данными в основном на территории компании, то наибольший вес необходимо назначить атрибуту «геолокация», из-за чего пользователи, находящиеся вне офиса, имеют повышенный уровень риска.

Для расчета оценки риска используется следующая формула:

$$R_h = b + \left(\frac{l_k - b}{\sum_{c=1}^{k} m_c}\right) \cdot h,$$

где h – количество неудачных попыток аутентификации пользователя за сессию, k – текущий уровень риска (при $h=0$ определяется по коэффициенту b, для $h>0$ – по R_{h-1}), l_k – граница уровня риска для текущего уровня риска k, m_k – количество максимальных попыток для текущего уровня риска k.

На рис. 2 представлен алгоритм работы аутентификации на основе рисков в системе.

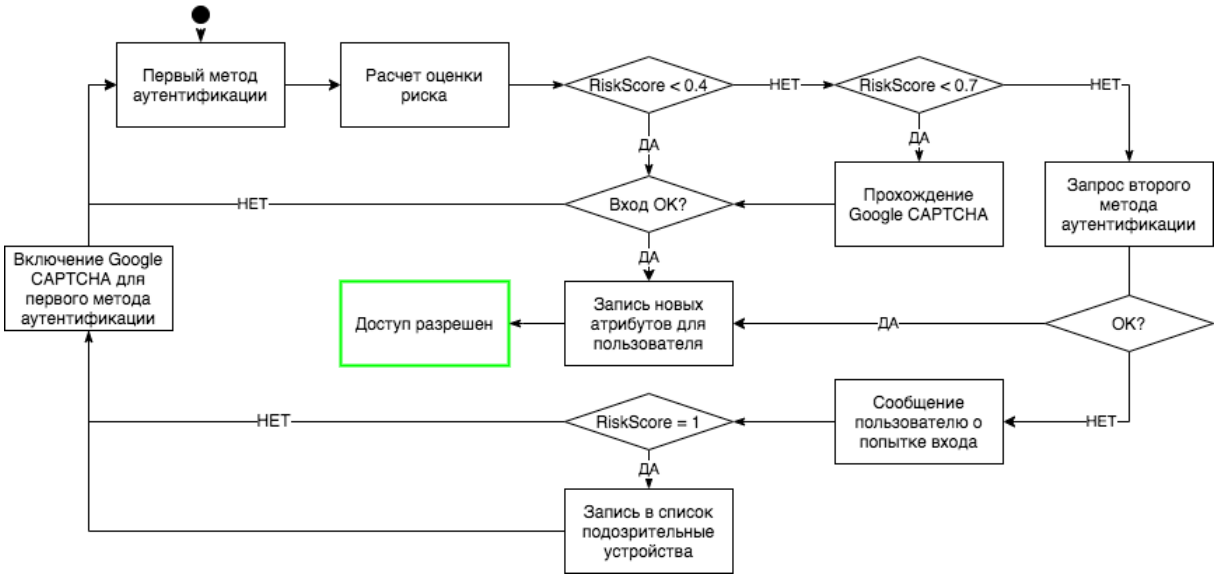


Рис. 2. Алгоритм работы аутентификации на основе рисков

Устанавливаются границы для каждого уровня: верхняя граница низкого уровня риска – 0.4, среднего уровня риска – 0.7, высокого – 1. Пользователь проходит проверку первым методом аутентификации по логину и паролю, после чего система рассчитывает оценку риска по переданным

от браузера атрибутам пользователя. В зависимости от результата система запрашивает дополнительную информацию: для среднего уровня требуется прохождение компьютерного теста CAPTCHA, для высокого – прохождение проверки вторым методом аутентификации (ввод *SMS*-кода). При отказе от прохождения проверки одним из методов аутентификации система оповещает владельца учетной записи о подозрительной попытке входа. При удачном прохождении проверок система записывает неизвестные атрибуты в базу данных для пересчета оценки риска. Если оценка риска достигает значения равного 1, то система записывает атрибуты пользователя в список подозрительных устройств.

Предложенная модель обеспечивает безопасность системы без требования дополнительных действий от пользователя. В перспективах развития представленной работы планируется разработка системы аутентификации на основе риск-ориентированной модели, внедрение более сложных атрибутов пользователя, формирование механизма корректировки весов атрибутов, границ уровней и количества неудачных попыток авторизации, внедрение модели в другие процессы веб-приложения.

Список используемых источников

1. Web Applications vulnerabilities and threats: statistics for 2019 [Электронный ресурс]. 13.02.2020. URL: https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/ (дата посещения: 05.03.2020).

2. Жаранова А. О., Капитоненко В. В., Котлова М. В. Обеспечение безопасности информационных систем на основе модуля регистрации событий // 73-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая Весна – 2019»: сб. науч. ст. в 2-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 137–141.

3. Paul A., Michael E., James L. Digital Identity Guidelines [Электронный ресурс]. Публикация NIST 800-63-3. 2017. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf (дата посещения: 21.02.2020).

4. Thuy O. Over 90 percent of Gmail users still don’t use two-factor authentication [Электронный ресурс]. 23.01.2018. URL: https://www.theverge.com/2018/1/23/16922500/gmail-users-two-factor-authentication-google (дата посещения: 15.02.2020).

5. Wiefling S., Iacono L., Durmuth M. Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild [Электронный ресурс]. 2019. URL: https://riskbasedauthentication.org/download/rba-study-paper.pdf (дата посещения: 20.01.2020).

6. Eckersley.P. How Unique Is Your Web Browser? [Электронный ресурс]. 2014. URL: https://panopticlick.eff.org/static/browser-uniqueness.pdf (дата посещения: 17.02.2020).

УДК 004.7:004.422.8
ГРНТИ 20.01.07

АНАЛИЗ ВЛИЯНИЯ РАСПРЕДЕЛЕННОСТИ НА КАЧЕСТВО ФУНКЦИОНИРОВАНИЯ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

А. О. Жаранова, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обоснована актуальность развития комплексных систем защиты информации. Определена цель анализа влияния распределенности на качество функционирования комплексных систем защиты информации. Выбран профиль качества функционирования комплексных систем защиты информации. Поставлена задача расширения модельного ряда комплексных систем защиты информации. Выбрана методология определения показателей профиля. Представлен типовой фрагмент расширения моделей.
информационная безопасность, комплексные системы защиты информации, распределенные системы, моделирование.

Согласно национальной программе «Цифровая экономика Российской Федерации» одной из главных задач на ближайшие несколько лет является создание эффективной, устойчивой и безопасной инфраструктуры передачи, обработки и хранения больших объемов данных. В подобных условиях актуализируется интенсивное развитие распределенных информационных систем.

Успешная реализация поставленных задач цифровой экономики неразрывно связана с обеспечением информационной безопасности как личности, так и государства в целом от внутренних и внешних информационных угроз, с целью обеспечения целостного и устойчивого функционирования национальной инфраструктуры. Согласно Указу Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» важнейшей задачей является формирование комплексной системы защиты информации при использовании и внедрении технологий искусственного интеллекта.

В связи с этим с каждым днем становится все более актуальным вопрос развития современных подходов к защите информации распределенных систем, сопровождающих профессиональную деятельность во всех секторах цифровой экономики, и повышения её качества на основе ускоренного внедрения технологий искусственного интеллекта. Соответственно, растет востребованность методологических и инструментальных средств, необходимых для оценивания степени доверия к комплексным системам защиты информации в распределенных инфраструктурах.

Успешное обеспечение безопасности распределенных систем основывается на обеспечении защиты данных, задействованных в процессах обработки информации, которые являются объектами большинства угроз в информационных инфраструктурах. Конфиденциальность информации и, как следствие, возрастающие требования к качеству их защиты, предопределяют объективную необходимость развития современных подходов к обеспечению информационной защищенности.

Высокий темп развития цифровых платформ и технологий проявляется в обширном многообразии архитектур распределенных систем. При широком спектре архитектурных решений в условиях разного рода неопределенностей ключевые задачи обеспечения информационной безопасности распределенных систем предлагается решать на основе интеллектуализации комплексных систем защиты информации.

Одним из возможных подходов к интеллектуализации комплексных систем защиты информации в системах с различной степенью распределенности является генерация и введение в их архитектуру модельно-аналитического интеллекта [1]. Объективным основанием для подобной приоритетности является предусматриваемая в этом подходе функциональность, обеспечивающая оценивание показателей качества защиты информации и соответствующей степени доверия при различных условиях неопределенностей относительно поведения окружающей среды.

В существующих на сегодняшний день моделях не учитываются вариации в разнообразии коммуникационного оборудования и сред, которые могут использоваться для организации распределенных комплексных систем. Появляется необходимость расширить модельный ряд, основываясь на гетерогенном характере комплексирования с учетом различных сред проводного и беспроводного секторов и различной степени территориальной распределенности оборудования.

В результате проведенного исследования и в соответствии с описанными принципами и концепцией объектно-ориентированного моделирования сформирован типовой фрагмент расширения моделей комплексных систем защиты информации при распределенном учете, ориентированный на повышение информационной защищенности.

Введение модельно-аналитического интеллекта в архитектуру комплексной системы защиты информации при наличии степени распределенности позволит варьировать конфигурацией комплексных систем защиты информации, характеристиками комплексируемых средств, способами комплексирования средств, математическим обеспечением способов комплексирования в целях обеспечения соответствия требуемой степени доверия к информационной защищенности.

На рис. представлен построенный в соответствии с описанными принципами и концепцией объектно-ориентированного моделирования типовой

фрагмент расширения моделей. Разработанный фрагмент является логической основой для формирования модельно-аналитического интеллекта комплексных систем защиты информации. Методология формирования модельно-аналитического интеллекта агентов, обеспечивающего гарантию качества их функционирования представлена в [2].

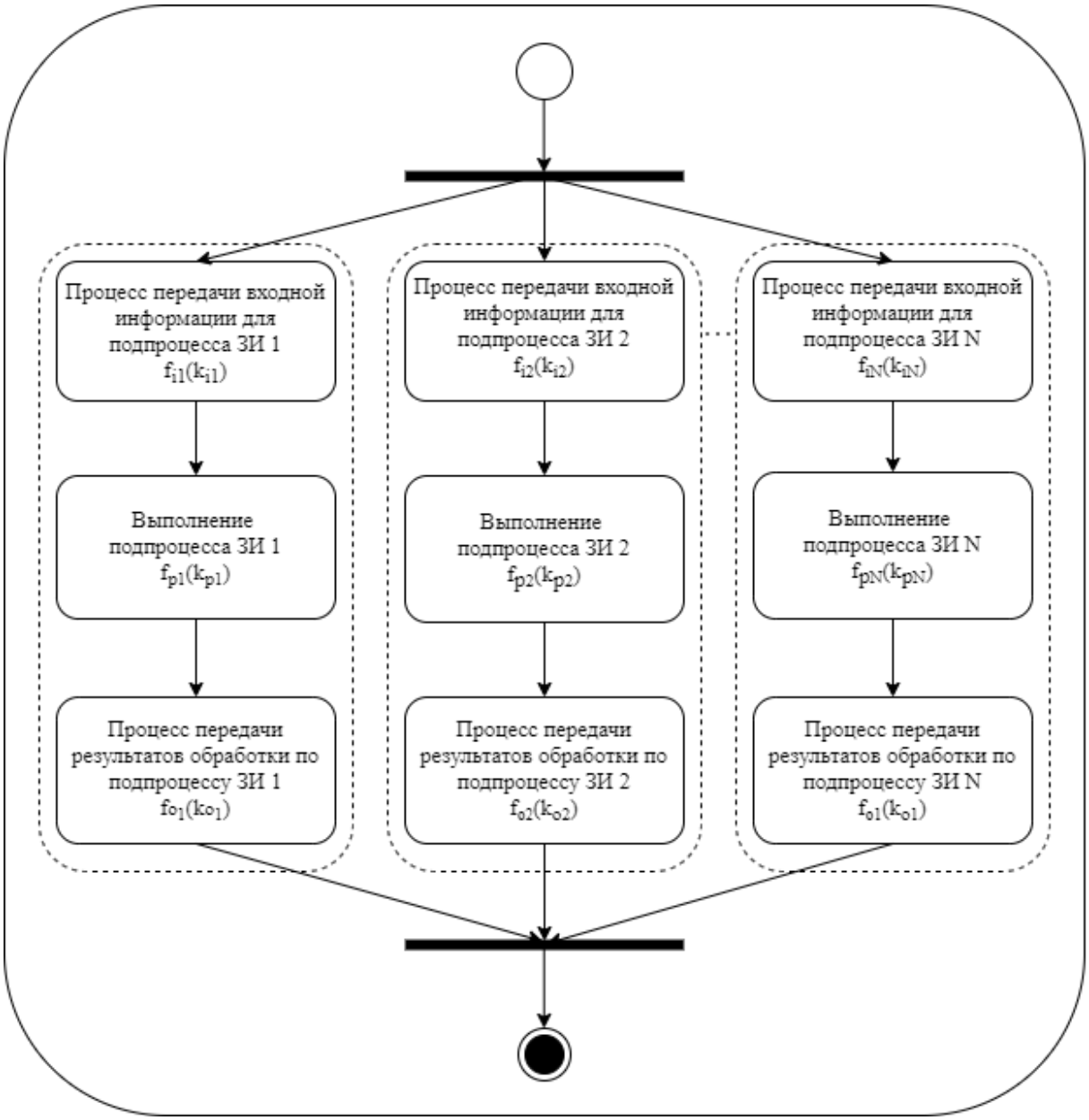


Рис. Типовой фрагмент расширения моделей

Ресурсы, реализующие операции при распределенной обработке, территориально расположены в разных местах, поэтому при передаче процесса и при обработке могут использоваться различные линии связи и телекоммуникационные каналы для передачи.

При моделировании считается, что каждый процесс определяется плотностью вероятностей времени его выполнения. На входе значение плотности распределения времени передачи входной информации по линиям связи и плотность распределения времени результатов обработки на выходе имеют разные значения, так как исходные данные для подпроцессов могут быть различными.

Математические объекты модели представляют собой следующие характеристики:

– $f_{iN}(k_{iN}),\ k_{iN} = 1,2,\dots,K_{iN}$ – плотность распределения вероятностей k_{iN} дискретного времени выполнения действия по передаче входной информации по линиям связи для подпроцесса защиты информации *iN;*

– $f_{pN}(k_{pN}),\ k_{pN} = 1,2,\dots,K_{pN}$ – плотность распределения вероятностей k_{pN} дискретного времени выполнения действия по выполнению подпроцесса защиты информации *pN*;

– $f_{oN}(k_{oN}),\ k_{oN} = 1,2,\dots,K_{oN}$ – плотность распределения вероятностей k_{oN} дискретного времени выполнения действия по передаче результатов обработки по подпроцессу защиты информации *oN*.

Предложенная модель комплексной защиты информации в распределенных системах обеспечивает отображение варьирования в их архитектуре в зависимости от уровня защищенности. Позволяет развернуть процесс формирования их математического обеспечения, предусматривающего определение и оценку показателей качества защищенности.

Научные исследования в данной области позволят развить известные традиционные подходы к жизненному циклу комплексных систем защиты информации за счет формирования новой модели их функционирования и метода ее анализа применительно к крупномасштабным распределенным системам для различных областей деятельности при переходе на сквозные цифровые технологии.

Список используемых источников

1. Птицын А. В., Птицына. Л. К. Генерация системно-аналитического ядра безопасных информационных технологий. СПб. : Изд-во Политехн. ун-та, 2011. 263 с.

2. Птицын А. В., Птицына Л. К. Аналитическое моделирование комплексных систем защиты информации. Гамбург. Saarbrucken: LAP LAMBERT Academic Publishing, 2012. 293 с.

УДК 004.67
ГРНТИ81.93.29

ВЗАИМОДЕЙСТВИЕ ПОЛЬЗОВАТЕЛЕЙ ПРИ РАБОТЕ В ЕДИНОМ ХРАНИЛИЩЕ ДАННЫХ

В. В. Жилин, В. А. Липатников

Военная академия связи

Рассмотрено взаимодействие пользователей при работе в едином хранилище данных. Современные операционные системы и вычислительные среды обеспечивают эффективную работу пользователей над всеми необходимыми для них данными. Однако отследить целостность информации для обычного пользователя является проблематичной задачей. Предложено решение задачи организации работы в замкнутой среде, где пользователи работают в едином информационном пространстве. Все действия могут быть отслежены распределяющим устройством.

распределяющее устройство, пользователи, права, операции, данные, чтение, запись, изменение, хеш-сумма.

Чаще всего пользователи автоматизированных мест оперируют данными, работая в какой-либо операционной системе. Перед отправкой информации на сервер с целью дальнейшего хранения, требуется сохранить данные на персональном компьютере в своей учетной записи.

Однако, крупные организации могут столкнуться со следующими проблемами:

1. Поиск необходимых данных станет время затратным процессом в том случае, если конечный пользователь не отправил информацию на сервер [1]. Доступ к компьютеру пользователя может быть недоступен в какой-либо момент.

2. В организациях, работа которых связана с обработкой конфиденциальной информации задача контроля за действиями пользователей является трудной для реализации.

Цель работы: обеспечение защищенности при оперировании данными, хранящимися на накопителях.

Основной задачей является разработка способа взаимодействия пользователей друг с другом при обмене данными.

Эти проблемы решаются с использованием единой среды работы пользователей. В такой среде конечные пользователи в режиме реального времени смогут отслеживать изменения всех данных, хранящихся на накопителях удаленного сервера. При этом прямой связи между пользователями и накопителями, как в одном компьютере, нет. Оперирование данными про-

исходит путем отправки запросов соответствующему устройству распределения. Таким образом, пользователи, взаимодействуя как с данными, так и друг с другом, обращаются к распределяющему устройству.

Распределяющее устройство, получая запросы на проведение той или иной операции, проверяет возможность эту операцию осуществить. Под такой операцией могут подразумеваться как сохранение данных на сервере, так и запрос на предоставление права чтения какой-либо конфиденциальной информации.

Для описания работы такой системы необходимо ввести некоторые обозначения.

Пусть в системе имеется множество информационных объектов системы [2]

$$I = (i_1, i_2, \dots, i_n), n = \overline{1, \dots},$$

множество субъектов, зафиксированных в системе:

$$U = (u_1, u_2, \dots, u_k), k = \overline{1, \dots},$$

а также доступные операции над данными:

$$O = \{w, r, c\}.$$

То есть, при формировании запроса А распределяющему устройству используются элементы данных множеств. Например, в распределяющее устройство поступил запрос субъекта u_m на предоставление прав чтенияинформационного объекта i_n. Тогда полученный запрос будет иметь следующий вид:

$$R = \{u_m, r(i_n)\}.$$

Каждый из пользователей обладает правом создания файла. Как только кто-либо из них создаёт файл, он автоматически становится его владельцем и доступом к этому объекту обладает только он. Например, пользователь u_m создал файл i_n, который был отправлен распределяющему устройству с целью удаленного распределенного хранения. Тогда в распределяющее устройство вносится следующая запись:

$$hash(u_1, i_1, r(i), w(i), c(i)).$$

В данной записи $r(i)$ – доступ на чтение, $w(i)$ – доступ на запись, $c(i)$ – доступ на изменение. В данном случае происходит вычисление хеш-суммы для того, чтобы в дальнейшем, при запросе пользователя к распределяющему устройству происходила проверка соответствия уровня доступа пользователя к той информации, которая хранится на сервере [3].

Как уже было сказано ранее, пользователи могут запрашивать и предоставлять доступ к каким-либо файлам, хранящимся в системе. Алгоритм предоставления доступа выглядит следующим образом:

Шаг 1: пользователь u_n хочет запросить доступ на проведениеоперации чтения $o(i), o = \{r, w, c\}$ над файлом i_m. Он формирует этот запрос распределителю:

$$u_n \xrightarrow{request((o(i_m)))} \text{РУ}.$$

Под операцией чтения подразумевается запись $o = \{r\}$.

Шаг 2: распределяющее устройство получив этот запрос, производит шифрование на внутреннем ключе имени файла.

$$E(i_m).$$

Шаг 3: производится поиск соответствующей записи в таблице 1 имён и владельцев файла, продемонстрированную ниже с целью определения владельца данных.

ТАБЛИЦА 1. Таблица владельцев и имён файлов

Имя владельца	Имя файла	Время доступа
$E(u_1)$	$E(i_1)$	$E(t_1)$
…		
$E(u_n)$	$E(i_m)$	$E(t_r)$

Шаг 4: происходит расшифровывание с целью определения владельца файла:

$$D\big(E(u_k)\big) = u_k.$$

Если имя пользователя u_k совпадает с именем пользователя u_n, делается вывод о том, что пользователь, запрашивающий доступ к файлу, возможно, является его владельцем. Он обладает всеми правами над созданным им файлом, а значит ему должен быть предоставлен доступ, вне зависимости от операции. Поэтому, в базе данных распределяющего устройства ищется запись, указанная в формуле (4). Это используется для того, чтобы избежать проблемы коллизии хеш-функций [4].

Кроме того, в таблице 1 указано время, в течение которого пользователь может оперировать данными. Предоставление доступа к информации с учетом времени может быть осуществлено следующими способами [5]:

1. Предоставление доступа к данным в течении ограниченного периода времени.

2. Указание промежутков времени, в течение которого возможна работа с данными. Эти промежутки могут быть указаны как единоразово, так и постоянно указываться владельцем данных.

Шаг 5: в таблице 2 происходит поиск записи, по которой определяется, обладает ли пользователь доступом к проведению соответствующей операции или нет. При этом, данные в этой таблице также представлены в виде хеш-сумм.

ТАБЛИЦА 2. Таблица управления доступом

$hash$(Имя файла, владелец файла)	Разрешённые операции, $hash$(Владелец файла, разрешённыйпользователь, файл)	Запрещённые операции, $hash$(Владелец файла, запрещённый пользователь, файл)
$hash(i_m, u_k)$	$hash(u_k, u_n, i)$	$hash(u_k, u_n, i)$

Для начала проверяется третий столбец таблицы. Если будет найдена запись о том, что пользователю запрещено проводить операции над файлом, доступ ему блокируется, а владелец файла уведомляется о попытке неправомерного доступа к файлу. Если запись о заблокированном доступе не найдена в третьем столбце, происходит поиск соответствующей записи во втором.

Шаг 6: если не было найдено соответствующей записи ни в одном из столбцов, то запрос на предоставление доступа отправляется непосредственно владельцу файла

$$\text{РУ} \xrightarrow{request(u_n(o(i_m)))} u_k.$$

Далее, пользователь u_k решает, предоставлять пользователю u_n право на проведение какой-либо операции с файлом i_m или нет. Если он предоставляет доступ, в таблицу управления доступом вносится соответствующая запись. Если нет, то действия являются аналогичными.

Следует отметить, что в случае, если пользователь запросил доступ на запись файла, и при этом он владельцем не является, то, в случае предоставления ему соответствующих разрешений, распределяющее устройство не изменяет сам файл. Вместо этого, оно создает его копию, уведомляя при этом владельца файла, что в системе наблюдается данная ситуация. Владелец файла принимает решение о принятии изменений и удалении исходного файла.

При этом распределитель с копией файла должен поступить так же, как и с обычным файлом, то есть разделить его, с целью хранения долей на раз-

личных накопителях. Таким образом, распределитель имеет таблицу 3 копий файлов, в которых также присутствует запись о месте расположения долей на накопителях. В таблице 3 также хранится время создания файла.

ТАБЛИЦА 3. Таблица копий

Имя файла	Имя копии	Дата внесения записи
i_{m1}	i_{m2}	dd.mm.yyyyhh.mm.ss

Сам владелец u_k файла i_m уведомляется о наличии файла-копии. При этом, в таблицу 3 добавляется запись о новом файле и его хранении, а владельцу посылается имя копии. Владельцу необходимо принять решение о принятии изменений или отказу от этих изменений. При принятии изменений, из информации, хранящейся в таблице 3 происходит поиск долей на накопителях первоначального файла с целью их удаления с дисков. Далее удаляется непосредственно запись о файле из таблицы. Файл-копия переименовывается с названием первоначального файла, а их таблицы 3 также удаляется соответствующая запись. Если изменения не приняты или соответствующий вывод не был сделан, из таблиц удаляются соответствующие записи, а удаление копии файла аналогично удалению оригинала в случае принятия изменений.

Предложен алгоритм работы при запросе пользователя на предоставление доступа к файлу. Для того, чтобы пользователь мог получить доступ к восстановлению файла, он посылает запрос на проведение данной операции распределителю. Тот же, в свою очередь, проверяет, является ли данный пользователь владельцем (создателем) данной информации.

В случае, если пользователь является владельцем, происходит восстановление файла, а в случае его изменения, осуществляется перезапись данного файла на накопителях с сохранением оригинального имени.

В случае, если пользователь является «гостем», в случае обладания права проведения каких-либо операций над файлом, происходит его восстановление, а в случае его изменения, файл сохраняется с новым именем. Таким образом, возникает ситуация, что один и тот же файл содержится на накопителях с двумя разными именами. Если пользователь не обладает правами доступа к файлу, то файл восстановлен не будет, а в лог-файл будет добавлена запись о попытке неправомерного доступа к защищенной информации [6].

Для каждого файла распределитель ведёт специальный лог-файл, в котором фиксируются все изменения, связанные с ним. Таким образом, владелец файла может в любой момент просмотреть все изменения, связанные с созданным им файлом. При этом сам файл хранится на устройстве пользователя и содержит информацию о тех файлах, владельцем которых он является.

Кроме того, модель устроена таким образом, что файлы, хранящиеся в системе доступны строго в определённое время. Другими словами, время работы с информацией, распределённой на накопителях, является ограниченным. Время доступа пользователя к информации хранится на распределяющем устройстве в зашифрованном виде.

Таким образом, данный способ взаимодействия пользователей и оперирования данными между ними позволит обеспечить высокий уровень защищенности при проведении различных операций. При возникновении каких-либо ситуаций, связанных с нарушением целостности данных, существует возможность определения источника угроз, а в последствии, принятия дальнейшего решения об ограничениях доступа какого-либо субъекта к объекту.

Список используемых источников

1. Могилевская Н. С., Кульбикаян Р. В., Журавлёв Л. А. Пороговое разделение файлов на основе битовых масок: идея и возможное применение // Вестник Донского государственного технического университета. 2011. Том 11. № 10 (61). С. 1749–1755.

2. Воронцова С. В. Обеспечение информационной безопасности в банковской сфере. М. : КНОРУС, 2015. 160 с.

3. Чмора А. Л. Современная прикладная криптография. 2-е изд. М. : Гелиос РВ, 2002. 256 с.

4. Blakley, G. R. Safeguarding cryptographic keys // In: Proc. AFIPS 1979, National Computer Conference, 1979. PP. 137–313. 1087 p.

5. Жилин В. В., Дроздова И. И., Черкесова Л. В., Сафарьян О. А. Трехмерная модель безопасности компьютерных систем // Молодой исследователь Дона. 2018. № 5 (14). С. 30–37.

6. Липатников В. А., Шевченко А. А. Модель системы защиты информации распределенной информационной сети на основе контроля за уязвимостями // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2018. Т. 1. С. 569–574.

УДК 621.391.18
ГРНТИ 81.93.29

ПОДХОД К КОНТРОЛЮ ИЗМЕНЕНИЙ ИНФОРМАЦИОННЫХ WEB-РЕСУРСОВ

Д. Л. Жусов, А. В. Козленко

Академия ФСО России

В работе обоснована актуальность задачи контроля изменений информационных web-ресурсов. Перечислены направления решения поставленной задачи с точки зрения исследования различных механизмов функционирования web-порталов. Предложен способ оценки периодичности контроля в условиях известной частоты проявления компьютерных атак и оценок времени модификации информационного ресурса при ее успешной реализации. Разработана функциональная модель анализа и режекции запросов пользователей к информационным web-ресурсам.

информационные web-ресурсы, контроль изменений web-ресурсов, компьютерные атаки.

В настоящее время информационные web-ресурсы в России обладают большой популярностью как для отдельных граждан, так и различных организаций и учреждений. Это связано с широким распространением технологии web-порталов, которые предоставляют пользователям единую точку персонифицированного доступа к разнородным информационным ресурсам, обеспечивают интеграцию разнородных информационно-справочных и информационно-аналитических систем, а также обеспечивают сравнительно простую масштабируемость указанных систем.

Информационные ресурсы, построенные по идеологии гипертекстовой структуры, могут выступать, с одной стороны, источниками периодически изменяемой информации для граждан, различных организаций и учреждений, а, с другой, являться объектом деструктивных воздействий с целью дискредитации как отдельных граждан, так и различных организаций и учреждений в целом. В связи с этим актуальной является задача контроля изменений информационных web-ресурсов.

Содержательно данная задача может быть сформулирована следующим образом: предложить механизмы контроля изменений содержимого информационных web-ресурсов, созданных с использованием современных принципов и технологий.

Возможными направлениями решения сформулированной задачи являются исследования механизмов: а) периодического контроля изменения непосредственно содержимого web-ресурсов, позволяющих отслеживать факт изменения информационного наполнения отдельной страницы в усло-

виях рассчитываемых временных интервалов контроля; б) оценки изменения семантики информационного web-ресурса; в) анализа запросов пользователей к информационным web-ресурсам с целью обнаружения конструкций, способных вносить изменения в содержимое информационных web-ресурсов.

Проводимые исследования по первому направлению позволили предложить аналитическое выражение для оценки вероятности сохранения целостности информационных ресурсов в условиях поступающих информационных запросов [1]:

$$P_{\text{КЦ}}(T_{\text{КЦ}}) = \begin{cases} \left(\sigma - \beta_{\text{КА}}^{-1}\right)^{-1} \left\{\sigma e^{-T_{\text{КЦ}}/\beta_{\text{КА}}} - \beta_{\text{КА}}^{-1} e^{-\sigma T_{\text{КЦ}}}\right\}, \text{если } \sigma \neq \beta_{\text{КА}}^{-1} \\ e^{-\sigma T_{\text{КЦ}}}\left[1 + \sigma T_{\text{КЦ}}\right], \text{если } \sigma = \beta_{\text{КЦ}}^{-1}; \end{cases}, \quad (1)$$

где σ – частота проявления компьютерных атак; $\beta_{\text{КЦ}}$ – среднее время изменения информационных ресурсов при успешной реализации компьютерной атаки.

Являясь модификацией модели [2], решение данного уравнения относительно $T_{\text{КЦ}}$ позволяет получить оценки периодичности контроля в условиях известной частоты проявления компьютерных атак и оценок времени модификации информационного ресурса при ее успешной реализации.

Результаты расчетов и имитационного моделирования позволяют сделать вывод, что вероятность сохранения целостности информационных web-ресурсов зависит в основном от частоты проявления компьютерных атак, а среднее время изменения информационных ресурсов при успешной реализации компьютерной атаки не оказывает существенного влияния. Это позволяет адаптировать периодичность контроля в зависимости от интенсивности реализации компьютерных атак на информационные web-ресурсы.

Проводимые исследования в рамках оценки изменения семантики информационного web-ресурса предполагают разработку анализатора его структуры с выделением различных элементов (текстовых, графических и др.), составляющих контролируемые семантические области (зоны). Каждой зоне сопоставляется эталонный образец информационного наполнения, позволяющий реализовать его сравнение с текущим информационным наполнением web-ресурса с заданной периодичностью. Информация об изменениях сохраняется в виде цепочки изменений, позволяющей впоследствии анализировать траекторию изменений содержимого информационного web-ресурса. Такой подход позволит, например, отслеживать изменения в составе органов управления учреждений и организаций, а также, например, государственных органов и социально значимых объектов.

С целью анализа запросов пользователей к информационным web-ресурсам для обнаружения конструкций, способных вносить изменения в содержимое информационных web-ресурсов предлагается модель (рис.):

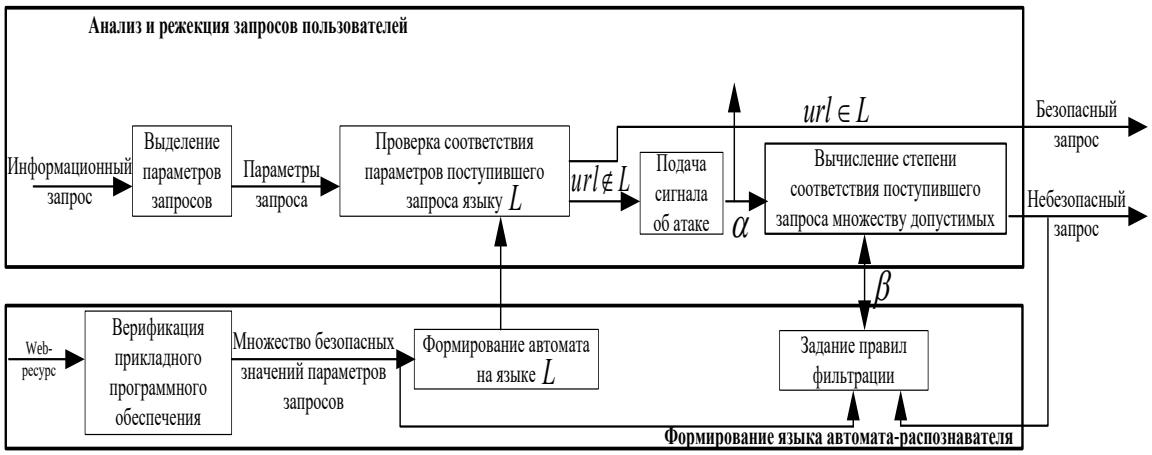


Рис. Функциональная модель анализа и режекции запросов пользователей к информационным web-ресурсам

Значения параметров доступа каждого поступающего запроса пользователя проверяются на соответствие безопасным значениям. В случае их корректности запрос обрабатывается и пользователю формируется ответ в виде запрашиваемого информационного web-ресурса. В противном случае осуществляется анализ запроса на степень его близости к сигнатурам компьютерных атак и безопасным запросам. По результатам анализа принимается решение об отнесении его к одному из классов.

Таким образом, проводимые исследования в рамках обозначенных направлений позволяют предложить подход к решению задачи контроля изменений информационных web-ресурсов. Решение указанной задачи позволит существенно повысить защищенность информационных web-ресурсов различных организаций и учреждений.

Список используемых источников

1. Жусов Д. Л., Козленко А.В., Толкунов А.А. Контроль целостности информационных ресурсов ведомственных веб-порталов // Информационная безопасность и защита персональных данных: Проблемы и пути их решения: материалы XI Межрегиональной научно-практической конференции / под ред. О. М. Голембиовской, М. Ю. Рытова. Брянск: БГТУ, 2019. 190 с., С. 113–117.

2. Безкоровайный М. М., Костогрызов А. И., Львов В. М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем "КОК": Руководство системного аналитика. 2-е изд. М. : Вооружение. Политика. Конверсия. 2002. 305 с.

УДК 004.05
ГРНТИ 81.93

УГРОЗЫ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВА

П. В. Закалкин

Военная академия связи

В статье рассматриваются основные техники, использующиеся в рамках APT-атак, проводимых хакерскими группировками. Помимо этого, излагаются основные черты и этапы проведения APT-атак в отношении критически важных объектов инфраструктуры государства.

APT-атаки, критическая инфраструктура, киберпространство.

Введение

Одним из основных негативных факторов, влияющих на состояние информационной безопасности Российской Федерации, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях. Постоянно повышается сложность, увеличиваются масштабы и растет скоординированность кибервоздействий на объекты критической инфраструктуры, усиливается разведывательная деятельность иностранных государств в отношении Российской Федерации, а также нарастают угрозы применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической, экономической и социальной стабильности Российской Федерации.

Критическая инфраструктура как объект APT-атак

К критически важным объектам инфраструктуры государства относят системы и средства, которые настолько жизненно важны для страны, что нарушение их работы или уничтожение оказывает необратимое негативное воздействие на национальную и экономическую безопасность, здравоохранение, правопорядок и т. д. [1].

Примером критически важных объектов инфраструктуры являются организации топливно-энергетического комплекса, поддерживающие работу промышленных и оборонных производств, а также других стратегических объектов. Энергетика обеспечивает жизнедеятельность городов, больниц, телекоммуникационных станций, правительственных учреждений и других

социально значимых объектов [2]. Другим примером может служить банковская сфера, сбой в которой потенциально приведет к нарушению работы банкоматов, платежных систем и т. д. Нарушение работы критически важных объектов инфраструктуры государства может привести к дестабилизации обстановки в отдельно взятом городе и стране в целом [3, 4, 5, 6, 7, 8].

Отличительной чертой всей критической инфраструктуры на планете является ее функционирование посредством мирового киберпространства, что позволяет оказывать деструктивное воздействие на военные системы, объекты экономики и т. д. любого государства без непосредственного вторжения на территорию страны и объявления войны. Практически любым объектом критической инфраструктуры (без привязки к его географическим координатам) из любой точки планеты посредством киберпространства возможно осуществлять как управление, так и перевод в режим функционирования, соответствующий собственным интересам, вплоть до полного отключения. При этом объекты воздействия не уничтожаются физически, и их восстановление после достижения поставленных целей не вызывает затруднений. Крайним случаем является перевод объекта в критический режим функционирования, приводящий к разрушению объекта.

Так, в 2019 г. после начавшихся протестных выступлений против действующего президента Венессуэлы, был осуществлен ряд кибератак на автоматическую систему контроля ГЭС «Эль-Гури». Это привело к отключению гидроэлектростанции и отключению электричества на 80 % территории страны. Далее последовал эффект «домино», когда отсутствие энергии вызвало нарушения функционирования многих производств. Крупные города стояли на гране гуманитарной катастрофы, осуществлена попытка военного мятежа и смены действующего режима. Это позволяет говорить о явных связях между событиями мирового масштаба и векторами атак.

Данный тип сложных атак, выполняемых хакерскими группировками преимущественно на инфраструктуру конкретных компаний, целых отраслей и государственных объектов, называют APT-атаками (*Advanced Persistent Threat*). Как правило, за такими атаками стоят группировки, имеющие значительные финансовые ресурсы, технические возможности, наличие узкоспециализированных специалистов, хорошо осведомленных о технологических процессах и специфике инфраструктуры [10].

Основные характеристики APT-атак

Ежегодно количество APT-атак возрастает, по состоянию на 2019 г. доля проведенных APT-атак по отраслям выглядит следующим образом: государственные учреждения – 70 %, промышленные компании – 60 %, финансовая отрасль – 45 %, топливно-энергетический комплекс – 41 % [11, 12, 13].

Уязвимыми компонентами в автоматизированных системах управления технологическими процессами являются: SCADA (в том числе распределенные системы управления и человеко-машинные интерфейсы), сетевые устройства и программное обеспечение.

В целом APT-атаки различных группировок развиваются по одному сценарию и похожи между собой, но при этом у каждой группировки можно выделить свои шаблоны поведения. Во многом это связано с различным опытом, навыками и составом группировки, наличия инструментов и способности их своевременно разрабатывать.

Тем не менее, высокая техническая квалификация и правильная внутренняя организация позволяет хакерским группировкам достигать основных целей – разрушительного воздействия на инфраструктуру и промышленный шпионаж.

Наиболее часто и успешно используемой техникой в рамках APT-атак является фишинг – одна из техник социальной инженерии, основной целью которой является получение доступа к конфиденциальным данным пользователей. Согласно отчета Positive Technologies порядка семи из девяти группировок проникают в инфраструктуру посредством фишинга. Далее по популярности идет компрометация ресурсов сторонних организаций (с последующим проникновением в целевую систем) и компрометация сайтов, посещаемых сотрудниками целевой организации (проникновение в целевую систему посредством посещения пользователей зараженного сайта).

Способность противостоять APT-атакам в существенной мере зависит от понимая тактики проведения атак и действий хакерских группировок. Для этого в первую очередь необходимо выделить характерные черты и этапы проведения APT-атак.

Отличительными чертами APT-атак являются:

- Целенаправленность. В качестве цели рассматривается отрасль или производство, способное остановить целую отрасль.
- Долговременность. Атака может планироваться и проводиться не один месяц и продолжаться до момента достижения цели или потери целесообразности.
- Многоэтапность. Атака содержит этапы от разведки и внедрения до уничтожения следов присутствия.
- Использование новейших техник. Для проведения атаки используется специально разработанное для конкретной системы узкоспециализированное программное обеспечение.

Существующие подходы к этапизации проведения APT-атак позволяют выделить следующие этапы:

1. Подготовка. На данном этапе осуществляется разведка, сбор данных, разработка стратегии и инструментов, применяемых для атаки.

2. Проникновение. На данном этапе разрабатываются техники обхода стандартных средств защиты, поиск и эксплуатация уязвимостей, осуществляется инвентаризация сети.

3. Распространение. На этапе распространения осуществляется закрепление в целевой системе, распространение в ней, получение прав доступа администратора и т. д.

4. Достижение цели. Данный этап включает в себя получение доступа к процессам управления системой, изменение данных и т. п. После этого осуществляется сокрытие результатов проникновения в систему (удаление созданных пользователей, очистка log файлов и т. д.), создается точка возврата в систему [14].

Предотвратить APT-атаки крайне сложно, и, как правило, стратегия защиты строится на выявлении действий злоумышленника в сети до момента причинения ущерба. Данная ситуация осложняется тем, что видимые признаки компрометации отсутствуют: технологические процессы не прерываются, показания системы мониторинга подменяются, и внешне система функционирует корректно.

Таким образом, для предупреждения APT-атак необходима корректная сегментация сетей и разграничение привилегий пользователей. Сложная сегментированная сеть, в которой реализовано разграничение доступа, заставит атакующих применять большое количество различных техник, что оставит следы в сетевом трафике и системных журналах.

Помимо этого, необходима система мониторинга событий информационной безопасности, работающая в режиме реального времени и позволяющая в случае возникновения события безопасности пересматривать прошедшие события в инфраструктуре. Это позволит на основе ретроспективного анализа выявлять присутствие злоумышленника в системе [12, 15, 16, 17].

Выводы

Использование критической инфраструктурой ресурсов киберпространства позволяет хакерским группировкам осуществлять технически сложные атаки на критическую инфраструктуру государств.

APT-группировки наращивают активность и мощность атак. Кибератаки усложняются и становятся более изощренными, атаки проводятся в несколько этапов, затрагивающих помимо цели атаки еще ряд дополнительных целей, или порождают сопутствующие явления.

Прослеживается четкая связь между действиями хакерских групп и громкими политическими событиями. Кибератаки стали политическим инструментом и методом влияния на общественное мнение.

Список используемых источников

1. Ромашкина Н. П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. № 1 (29). С. 4–12. DOI: 10.21681/2311-3456-2019-1-2-9.

2. APT-атаки на топливно-энергетический комплекс России. Обзор тактик и техник 2019 // Positive Technologies. 2019. С. 15.

3. Вершенник Е. В., Закалкин П. В., Стародубцев Ю. И. Кибернетические воздействия на информационно-телекоммуникационные сети связи // Проблемы технического обеспечения войск в современных условиях. Труды III Межвузовской научно-практической конференции: сб. 2018. С. 210–213.

4. Бречко А. А., Вершенник Е. В., Закалкин П. В., Стародубцев Ю. И. Взгляды командований зарубежных государств на проведение операции в киберпространстве // Проблемы технического обеспечения войск в современных условиях. Труды IV Межвузовской научно-практической конференции: сб. 2019. С. 132–136.

5. Бречко А. А., Вершенник Е. В., Закалкин П. В., Стародубцев Ю. И. Проблемы использования киберпространства при проведении операций // Проблемы технического обеспечения войск в современных условиях. Труды IV Межвузовской научно-практической конференции: сб. 2019. С. 137–140

6. Вершенник Е. В., Вершенник А. В., Закалкин П. В., Корнюшенко Р. А. Концепция проведения наступательных операций в киберпространстве // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2019. № 2. С. 80–84.

7. Стародубцев Ю. И., Бухарин В. В., Семенов С. С. Техносферная война // Информационные системы и технологии. 2011. № 1 (63). С. 80–85.

8. Стародубцев Ю. И., Гречишников Е. В., Комолов Д. В. Способ обеспечения устойчивости сетей связи в условиях внешних деструктивных воздействий // Патент на изобретение RUS 2379753 от 21.04.2008 г.

9. Закалкин П. В., Сагдеев А. К., Стародубцев Ю. И., Сухорукова Е. В. Проблема формирования системы динамической защиты государственных информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3-х томах. 2016. С. 239–243.

10. Что такое APT-атака и как от нее защититься [Электронный ресурс]. URL: http://www.spy-soft.net/apt-attack/ (дата обращения: 10.02.2020).

11. Cisco 2018. Годовой отчет по информационной безопасности // Cisco 2018. С. 68.

12. Positive Research 2018 // Сборник исследований по практической безопасности 2018 // Positive Technologies. 2018. С. 204.

13. Стародубцев Ю. И., Бречко А. А. Способ определения времени квазистационарного состояния процесса в целях повышения интеллектуализации принимаемых управленческих решений // Нейрокомпьютеры и их применение. XVI Всероссийская научная конференция: тезисы докладов. 2018. С. 109-А.

14. Таргетированные или целевые кибератаки [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/статья:APT_-_Таргетированные_или_целевые_атаки (дата обращения: 10.02.2020).

15. Закалкин П. В., Добрышин М. М. Способ мониторинга защищенности информационно-телекоммуникационных сетей от информационно технических воздействий // Информационные системы и технологии. 2018. № 5 (109). С. 74–82.

16. Нижегородов А. В., Закалкин П. В., Стародубцев П. Ю., Кабанов А. С. Роль мониторинга в системе обнаружения, предупреждения и ликвидации последствий компьютерных атак // Промышленные АСУ и контроллеры. 2013. № 7. С. 67–71.

17. Анисимов В. Г., Анисимов Е. Г., Гречишников Е. В., Белов А. С., Орлов Д. В., Добрышин М. М., Линчихина А. В. Способ моделирования и оценивания эффективности процессов управления и связи. Пат. на изобретение RUS 2673014 31.01.2018 г.

УДК 004.056.53
ГРНТИ 50.37.23

ИДЕНТИФИКАЦИЯ ТОЧЕК ВХОДА ВЕБ-ПРИЛОЖЕНИЙ МЕТОДОМ ДИНАМИЧЕСКОГО АНАЛИЗА

А. А. Зверев, Д. О. Маркин, А. И. Саклаков

Академия ФСО России

В статье описан алгоритм идентификации точек входа веб-приложений на основе динамического анализа средствами программно-управляемого веб-браузера. Исследованы проблемы формирования оптимальной информационной модели сайтов. Предложен алгоритм и приложение, позволяющие средствами программно-управляемого веб-браузера выполнять динамический анализ обфусцированного JavaScript кода.

фаззинг, обфускация, JavaScript, веб-приложения, Selenium, программно-управляемый веб-браузер.

Повсеместное внедрение информационных технологий, развитие цифровой экономики, а также повышение доступности и цифровизация государственных услуг обуславливает потребность в повышенном внимании к информационной безопасности предоставляемых услуг в целом и обеспечении защищенности веб-ресурсов, в частности. Как показывает статистика, современные веб-приложения имеют большое число проблем, связанных с обеспечением информационной безопасности, а поиск уязвимостей требует серьезных вычислительных ресурсов и высокой квалификации персонала, отвечающего за вопросы информационной безопасности. В связи с этим актуальной задачей является создание автоматизированных и автоматических средств поиска уязвимостей веб-приложений, позволяющих осуществлять эффективный анализ защищенности веб-ресурсов.

Одним из эффективных способ решения задачи автоматизированного анализа защищенности является фаззинг веб-приложений [1]. Вопросы оценивания защищенности информационных систем затрагивались в научных

трудах Хорева П. Б. и Петрова С. А. [3], Котенко И. В., Степашкина М. В. [4] Машкиной И. В., Саенко И. Б., Азарова А. А., Тулупьева А. Л.. Азарновой Т. В. и Полухина П. В. [5], Горюнова М. Н. и Мацкевича А. Г. [6] и других. Актуальные практические вопросы и инструменты оценивания защищенности веб-приложений представлены на свободных информационных ресурсах проектов OWASP, MITRE, White Hat, DISA и других. Однако в связи с постоянных совершенствованием информационных технологий и способов представления информации, кодирования веб-приложений, синтаксической и семантической разметки электронных документов проблема автоматизации тестирования защищенности остается актуальным. Данное обстоятельство указывает на объективную необходимость внедрения новых подходов по распознаванию структурных элементов веб-приложений, отвечающих за ввод данных (запрос) в информационную систему и получение ответа от нее.

На сегодняшний день существует множество фаззеров веб-приложений: Web Scarab, BurpSuite, Skyfish, SPIKE Proxy, OWASP WSFuzzer (SOAP), Rfuzz, Fuzzops, PowerFuzzer, w3af, WebFuzz, отдельные средства тестирования веб-приложений есть в составе таких инструментальных средств как X-Spider, Nessus, OpenVAS, nmap и других. Одним из общих существенных недостатков этих средств является проблема построения структурной модели произвольного веб-ресурса, которая позволила бы более эффективно направлять входные данные в исследуемые веб-приложения и его программное окружение.

На первый взгляд, решение данной проблемы лежит в разработке эффективного приложения, так называемого «робота-паука», способного эффективно распознавать все множество возможных точек входа в веб-приложения информационного ресурса, с учетом современного уровня развития и внедрения информационных технологий.

Однако факт наличия эффективного решения данной проблемы неочевиден по следующим причинам:

– информационные технологии, формы представления информации, кодирования веб-приложений, синтаксической и семантической разметки информационных ресурсов постоянно совершенствуются;

– веб-приложения могут разрабатываться с применением технологий обфускации и других технических решений по защите от анализа [7].

Современные технологии синтаксической и семантической разметки информационных ресурсов, а также средства разработки веб-приложений, функционирующих, в том числе на стороне веб-клиента, позволяют создавать в составе информационного ресурса различные точки входа веб-приложений [8].

Существенную сложность в распознавании точек входа веб-приложений создают технологии защиты исполняемого, а также интерпретируемого кода приложений от анализа [7], такие как обфускация и шифрование.

В настоящее время известно достаточно большое количество обфускаторов скриптовых языков. Наибольшее распространение получили обфускаторы и так называемые «крипторы» JavaScript-приложений [9]. Среди них такие инструменты как JS Packer, JSmin, YUI Compressor, Closure compile, Google Closure Compiler, jjencode, JSUnpack, WebStorage, uglifyjs2, jsfuck, aaencode, Caesar, Webpack. В работе [10] описано приложения для идентификации точек входа веб-приложений с динамически формируемым интерфейсом.

Идентификация точек входа веб-приложений методом динамического анализа обфусцированных JavaScript приложений

Для экспериментальной проверки эффективности динамического анализа обфусцированных JavaScript приложений в целях идентификации точек входа веб-приложений было разработано приложение на Python 3.6, в состав которого вошли следующие дополнительные модули:

– драйвера браузеров средства программного управления веб-браузерами Selenium (пример драйвера для веб-браузера *Chrome – chrome-webdriver\chromedriver.exe*);

– модуль прокси-сервера на базе Python «browsermobproxy» (*browsermob-proxy-2.1.4\bin\browsermob-proxy*);

– модуль набора правил синтаксического анализа содержания (парсинга) BeautifulSoup.

Модульная схема приложения представлена на рис. 1. Алгоритм приложения может выглядеть так, как показано на рис. 2.

Проверка эффективности разработанного в соответствии с представленным алгоритмом приложения показала, что, несмотря на невозможность идентификации сигнатурными методами точек входа удаленных веб-приложений, анализ har-логов прокси-сервера, функционирующего в комплексе с программно-управляемым веб-браузером, позволяет выявлять факт отправки HTTP-запросов средствами обфусцированных JavaScript приложений.

Вместе с тем, полнота динамического анализа ограничивается набором исходных данных для исследуемых обфусцированных JavaScript приложений. Данное обстоятельство не позволяет утверждать, что обнаруживаются все имеющиеся точки входа, а также не дает возможность оценить их количество.

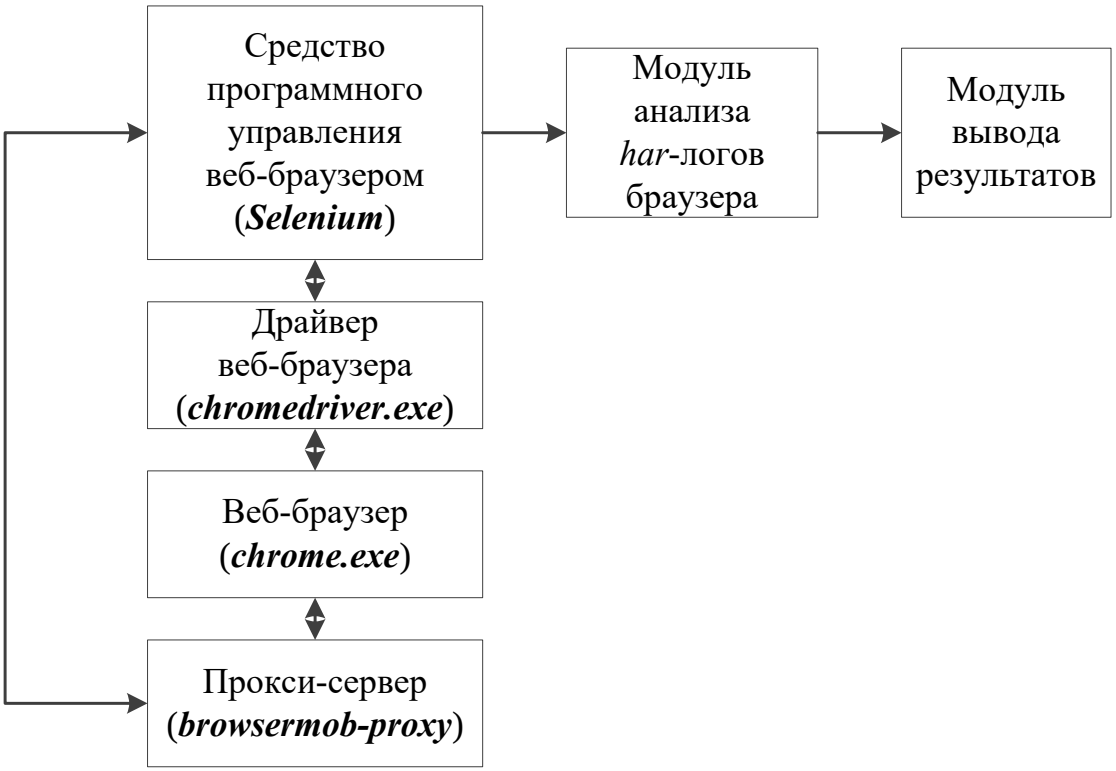


Рис. 1. Схема средства динамического анализа JavaScript кода

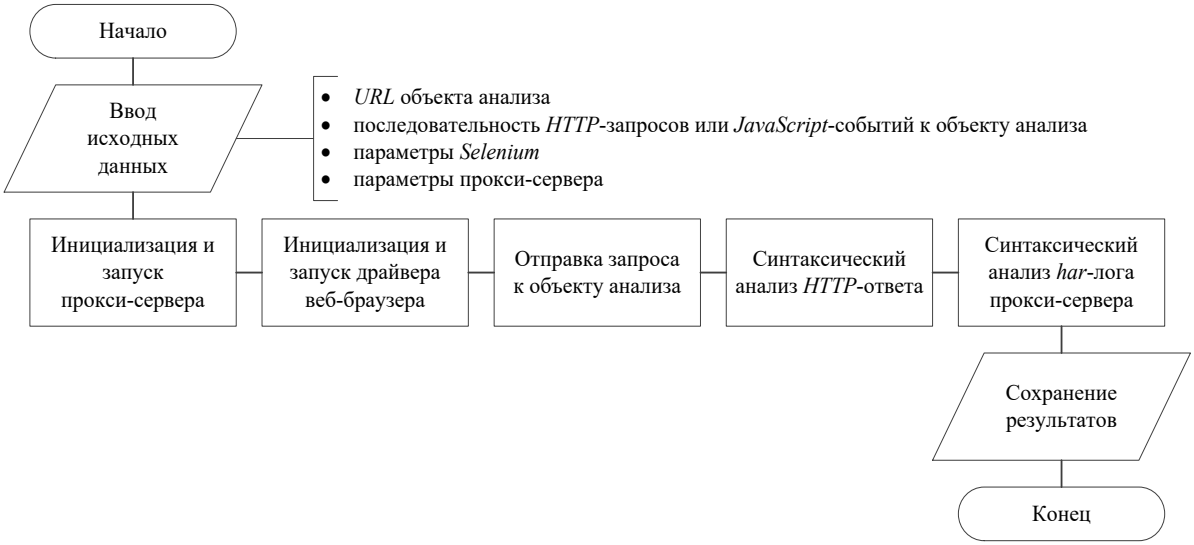


Рис. 2. Блок-схема алгоритма идентификации точек входа методом динамического анализа *JavaScript* кода

Повышение полноты анализа требует разработки и применения сложных сценариев, обеспечивающих наивысшую полноту покрытия кода обфусцированных JavaScript приложений.

В состав таких сценариев необходимо включать:

– программные действия, обеспечивающие переходы по перекрестным ссылкам удаленного веб-ресурса;

– программные действия, обеспечивающие выполнения обработчиков событий для пользовательских элементов управления;

– программные действия, обеспечивающие выполнение обработчиков для скрытых функциональных объектов.

Выводы

Существующие современные технологии синтаксической и семантической разметки электронных документов, а также средства разработки веб-приложений, функционирующих в том числе на стороне веб-клиента, позволяют создавать в составе информационного ресурса различные точки входа веб-приложений. В ряде случаев документы могут быть защищены от анализа с помощью средств обфускации и шифрования, что делает задачу распознавания точек входа технически сложной и требует разработки и применения новых методов и технологий распознавания.

Разработанное приложение динамического анализа JavaScript кода средствами программно-управляемого веб-браузера позволяет идентифицировать точки входа в обфусцированных JavaScript приложениях, что частично позволяет решить указанную проблему. Недостатком предлагаемого решения является невысокая полнота анализа исследуемого кода и, соответственно, идентифицируемых точек входа.

Список используемых источников

1. Саттон М., Грин А., Амини П. Fuzzing: исследование уязвимостей методом грубой силы. Пер. с англ. СПб. : Символ-Плюс, 2009. 560 с., ил.

2. Полухин П. В. Байесовские модели и алгоритмы управления процессом тестирования веб-приложений методом фаззинга: дис. … канд. техн. наук: 05.13.18 / Полухин Павел Валерьевич. Воронеж, 2016. 180 с.

3. Петров С. А., Хорев П. Б. Методы искусственного интеллекта в задачах обеспечения безопасности компьютерных сетей // Труды 18 МНТК. "Радиоэлектроника, электротехника, и энергетика". М. : Издательский дом МЭИ, 2012. Том 2. С. 63.

4. Котенко И. В., Степашкин Е. В., Дойникова Е. В. Анализ защищенности автоматизированных систем с учетом социо-инженерных атак // Проблемы информационной безопасности. Компьютерные системы. 2011. № 3. С. 40–57.

5. Азарнова Т. В., Полухин П. В. Исследование процесса фаззинга SQL-инъекций веб-приложений на основе динамической сети Байеса // Вестник Воронежского государственного ун-та. Серия: Системный анализ и информационные технологии. 2014. № 1. С. 120–129.

6. Горюнов М. Н., Еременко В. Т., Ершов А. Л., Мацкевич А. Г. Распознавание функциональных объектов программного обеспечения в условиях отсутствия исходных текстов // Информационные системы и технологии, 2013. № 5. С. 112–120.

7. Варнавский Н. П., Захаров В. А., Кузюрин Н. Н., Шокуров А. В. Современное состояние исследований в области обфускации программ: определение стойкости обфускации // Труды ИСП РАН. 2014. Т. 26. Вып. 3.

8. Маркин Д. О., Зверев А. А., Саклаков А. И., Рыков Д. А. Технологии распознавания моделей точек входа веб-приложений // Безопасные информационные технологии :

Десятая международная научно-техническая конференция : сб. трудов. (Москва, 3–4 декабря, 2019 г.). Москва : МГТУ им. Н.Э. Баумана, 2019. 409 с. : ил. С. 275–280.

9. Кузнецова А. О., Верхотурова Г. Н. Об особенностях применения методов обфускации программного кода языка JavaScript // Информационные технологии интеллектуальной поддержки принятия решений. 2019. С. 117–122.

10. Носеевич Г. М., Петухов А. А. Поиск входных точек для веб-приложений с динамическим пользовательским интерфейсом // Безопасность информационных технологий, 2013. № 1. С. 13–20.

11. Pedro F. A methodology for Assessing JavaScript Software Protections. OWASP AppSec Europe. 2018.

УДК 65.011.56
РГРНТИ 50.43.19

ОПТИМИЗАЦИЯ ДВИЖЕНИЯ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ

И. А. Зикратов, М. А. Казьмин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Одной из основных тенденций в современном мире является постепенное наращивание всё большего количества беспилотных транспортных средств благодаря тому, что это упростит множество жизненных аспектов как простых людей, так производственные циклы крупных компаний и корпораций. Здесь также учитывается, что за счёт тех процессов автоматизации и оптимизации управления в дальнейшем беспилотные транспортные средства должны снизить общий уровень аварийный инцидентов и уменьшить траффик на большинстве автодорог общего пользования.

беспилотные транспортные средства, автоматизация, оптимизация, управление, дорога.

В условиях расширения и развития множества различных областей экономики, обеспечение совершенно нового уровня мобильности особое значение, которое имеет решение транспортных задач в условиях действующих городских массивов. Ключевая роль в решении этой проблемы возложено на беспилотные транспортные средства.

Беспилотное транспортное средство – это в общем виде любой транспорт, который оснащён системой автоматизированного управления движения, и которое позволяет ему свободно перемещаться без полного или с частичным присутствием человека и, соответственно, владеть полным контролем за ситуацией на дороге.

Большинство систем автоматического управления транспортным средством рассчитывает на разного рода сторонние вспомогательные системы и их инфраструктуру в целом, например, позиционирование через сигналы GPS, передачу данных через мобильные сети сотовых операторов, использование сенсоров встроенных в дорогу. Однако, наиболее современные технологии шагнули намного дальше. Уже сейчас возможно в действительности симулировать присутствие человека на уровне принятия прямых решения в ориентации транспортного средства и величины скорости движения, благодаря физическим датчикам, таких как набор камер, сенсоров дистанции, радаров и систем определения геопозиции [1].

Можно разделить на следующие направления подобные системы:

1. Комплексная автоматизация автомобиля – ориентирована на комплексные решения в области беспилотного транспорта;

2. Автоматизация отдельных режимов движения – ориентирована на конкретные сложные сценарии, такие как парковка, движение на перекрестках, движение в пробках, перемещение по автомагистрали [2].

Упомянутые выше системы реализуются из совокупности следующих методов:

1. Метод нахождения транспортного средства контрольной области. Данный метод подразумевает, что в базе данных мобильного терминала транспортного средства содержатся сведения о географических координатах всех регионов, являющимися контрольными областями для данного вида транспорта. Например, для городского транспорта это может быть территория остановки, на которой происходит высадка и посадка пассажиров или, например, место базирования в таксопарке, на парковке. Для машин, принадлежащих муниципалитету, таковыми являются городские районы, пригороды, отдалённые микрорайоны. По факту каждая контрольная область представляет собой небольшой полигон, который сам определяется простым набором точек, чьи широта и долгота заданы или внесены заранее в систему;

2. Метод определения узловых точек. Стандартный режим функционирования GPS/ГЛОНАСС приёмника, встроенного в мобильный терминал, предусматривает непрерывную отправку данных, передаваемых геолокационной системой. Для множества современных транспортных задач достаточно получать текущие координаты движущегося автомобиля с частотой раз в секунду. При условии наличия стабильного дешёвого и скоростного канала связи. Затем эти данные могут сразу после получения переданы в дата центр организации, где происходит их дальнейшая обработка с использованием мощных вычислительных систем. В случае, если такой канал отсутствует, мобильное устройство не в состоянии своевременно передавать информацию на сервер. Запоминание этой информации на устройстве

с целью последующей передачи в момент, когда канал связи будет восстановлен, также не всегда получается, потому что современные мобильные терминалы достаточно часто используют в своём составе накопители памяти с низкой скоростью чтения и записи данных с них [3].

Нужно понимать, что интеллектуальная система беспилотного транспортного средства ставит перед собой цель полного или частичной замены субъекта, который им управляет. Основной задачей управления транспортного средства является выбор наиболее безопасной и эффективной (в части экономии топлива, времени прохождения, комфорта для пассажиров) траектории движения на основе анализа дорожной обстановки и технического состояния транспортного средства в режиме реального времени.

Нужно сказать, что траектория движения любого транспортного средства зависит от следующих групп факторов:

1. Управляющие воздействия на транспортного средства при помощи рулевого управления, тормозной системы, системы управления тягой;

2. Динамика движения автомобиля, связанная с его инерцией, сцеплением с дорогой и т. д.;

3. Состояние транспортного средства – работа тормозной системы, рулевого управления, тип и настройки подвески, загрузка и т. д.

Таким образом, для движения по выбранной траектории информационной системой беспилотного транспортного средства может выбирать управляющие воздействия, анализируя динамику, общее состояние транспортного средства и сведения дополнительных подсистем [4].

Входными данными модуля приёма/передачи данных интеллектуальной системы являются наборы характеристик управляющих сигналов от систем рулевого управления, торможения, управления газом, данные оценки состояния существующего дорожного покрытия и текущее состояние беспилотного транспортного средства. В состав модуля, осуществлявшего анализ, можно отнести следующие используемые данные [5]:

1. Угол поворота руля;

2. Давление в тормозной системе;

3. Уровень подачи топлива;

4. Скорость подачи топлива.

Также в качестве исходных данных для системы может использоваться сведения об общем состоянии дорожного полотна, что в данном случае определяется коэффициентом трения между протектором шины и покрытием дороги для каждого из четырех колес по отдельности на основе поступающих данных с датчиков.

Если заглянуть в ближайшее будущее следующее о чём ещё можно упомянуть это возможность взаимодействия автомобиля с единой информационной средой города (единая система управления трафиком). Можно выделить её основные свойства:

1. Оптимизация маршрута в реальном времени и по нескольким критериям. Единый система управления трафиком должна иметь возможность назначать маршруты в реальном времени, чтобы использовать большинство возможностей оптимизации, чтобы что большинство пассажиров могут добраться до места назначения в желаемое время с большой вероятностью. Система должна также уметь корректировать маршруты не экстренного транспорта создать интервалы времени в пути для автомобилей экстренных служб, таких как машины скорой помощи, полицейские и пожарные машины. Чтобы облегчить сложность назначения маршрута в реальном времени, должны быть предложены стимулы поощрять раннее бронирование своего пути. Также должна быть схемами транспортных расходов, которая позволяют снизить излишние транспортные затраты для автовладельцев и пассажиров с предварительным бронированием и/или при совместном использование транспортного средства

2. Масштабная оптимизация трафика. Еще одна проблема – масштабируемость. Дорожная сеть современного города может насчитывать десятки тысячи светофоров, а сотни тысяч автомобилей запрашивают инструкции по навигации. Поиск оптимального расписания движения автомобилей и светофоров ключевое направление.

3. Эффективное управление навигационным маршрутом. Знание навигационных маршрутов большинства автомобилистов и пассажиров открывает большие возможности для оптимизации движения. Это, однако, также приносит значительные проблемы для эффективного управления массивом такой информации, например, чтобы назначить маршрут для новых автомобилистов и пассажиров может производиться на основании огромного множества вариаций предыдущих запросов в конкретное время. Большое количество навигационных маршрутов должны храниться в структурированном виде и быть легко доступны в единой системе управления дорожным движением. Очень эффективным методы агрегации и интеллектуального анализа данных будут необходимы обработки данной информации, зная регулярные маршруты путешествий из исторической навигации, а также получить обзор состояния дорожного движения в реальном времени по текущим навигационным маршрутам позволит выполнять качественное управление потоками движения.

Все захватывающие технические идеи воплощаются повсеместно в то или ином виде в автомобильном транспорте, однако, не отменяют здравой оценки дальнейшей степени автоматизации и роботизации огромного количества возможных процессов в современном автомобиле, и то как это повлияет взаимодействие человека с машиной.

Список используемых источников

1. Allegretti M., Bertoldo S. Cars as a diffuse network of road-environment monitoring nodes. doi.org/10.4236/WSN.2014.69018.
2. Yang A., Naeem W, Irwin G., Li K. Novel Decentralised Formation Control for Unmanned Vehicles. doi.org/10.1109/IVS.2012.6232122.
3. Саврасов Ф. В., Дёмин А. Ю. Методы оптимизации динамического формирования маршрута движения транспортных средств // Известия Томского технического университета. 2011. Т. 318. № 5. С. 149–153.
4. Шадрин С. С., Иванов А. М., Синицкин И. В. Разработка и экспериментальные исследования автомобильной системы контроля движения в полосе // Беспилотные транспортные средства: проблемы и перспективы: сб. материалов 94 международной научно-технической конференции Ассоциации автомобильных инженеров, 2016 / гл.ред. С. М. Дмитриев. Нижний Новгород : Нижегородский государственный технический университет им. Р. Е. Алексеева, 2016. С. 25–31.
5. Тимошенко О. Б., Азаров А. В., Кириери Е. М., Енна Е. С. Беспилотный транспорт будущего // Молодой ученый. 2019. № 8.2. С. 44–46. URL https://moluch.ru/archive/246/56678/.

УДК 004.7:004.422.8
ГРНТИ 20.01.07

ОРГАНИЗАЦИЯ ИНТЕЛЛЕКТУАЛЬНОГО ПОИСКА КОНТЕНТА ДЛЯ СИСТЕМ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ

О. И. Золотов, Л. К. Птицына, М. В. Темникова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлены современные условия для развития общества знаний. Выделены основные направления совершенствования систем дистанционного образования в интересах цифровой экономики. Описаны определяющие факторы развития расширяемых структур моделей компетенций цифровой экономики. Проанализированы ключевые особенности методов и средств интеллектуального поиска контента для систем дистанционного образования. Предложены инновации в архитектуре интеллектуальных систем поиска контента. Инновации направлены на расширение ситуационной гибкости архитектуры. Построены концептуальные модели интеллектуальных систем поиска контента для систем дистанционного образования.

знания, образование, поиск, контент, интеллектуализация, сервис-ориентированная архитектура, сервис.

Современные условия жизнедеятельности в обществе знаний характеризуются быстрым расширением различных видов и форм взаимодействия, интенсивным развитием рынков и отраслей, высокотехнологических бизнесов, институциональных и инфраструктурных сред, технологических платформ и технологий, повышением конкуренции на глобальном рынке, возрастанием значимости образования и осознанием объективной необходимости создания экосистемы цифровой экономики.

Основной опорой цифровой экономики признаются наука, система образования и знания работающих, нацеленные на эффективное создание, распространение и целевое использование результатов деятельности.

Изменяющиеся производственные и культурные отношения, структура цифровой экономики и образования, эффективность и масштабы востребованности цифровых технологий становятся определяющими факторами для интенсивных трансформаций в процессах формирования и развития компетенций, относящихся к любым сферам жизнедеятельности.

Формирование исследовательских компетенций и технологических заделов, кадры и образование относятся к ключевым институтам, в рамках которых создаются условия для развития цифровой экономики.

В обществе знаний предусматривается создание благоприятной обстановки для подготовки кадров цифровой экономики; совершенствование системы образования, обеспечивающей цифровую экономику компетентными кадрами; создание системы мотивации по освоению необходимых компетенций и участию кадров в развитии цифровой экономики.

При формировании политики по развитию цифровой экономики особая значимость придается системе непрерывного образования на основе интеграции образовательных, когнитивных и инфотелекоммуникационных технологий в современной цифровой образовательной среде, обеспечивающей закрепление актуальных и приобретение новых компетенций, необходимых для повышения конкурентоспособности производимой продукции, товаров и услуг, а также укрепления национального технологического суверенитета.

В Национальной платформе открытого образования, разработанной ведущими университетами страны, осуществляется быстрая адаптация онлайн-образования к динамично изменяющимся условиям цифровой экономики.

Подобного рода адаптация может выполняться и в системах дистанционного образования, создаваемых на базе программных продуктов IBM Lotus Workplace Collaborative Learning (LWCL), Moodle, Oracle Learning Management (OLM), WebTutor, Claroline, ATutor, Dokeos, Learning Activity Management System (LAMS), Learning Management System. Анализ информации в системах дистанционного образования проводится на основе применения методов и средств Data Mining (DM).

Однако, несмотря на широкий спектр функционального разнообразия представленных в информационной инфраструктуре научно-образовательных сред, по-прежнему остается субъективная форма генерации и заполнения контента со стороны преподавателей, реализующих образовательные программы.

Изложенные обстоятельства актуализируют разработку новых архитектур интегрированной системы интеллектуального поиска контента для дистанционного образования.

Предлагаемая инновация для развития любой системы дистанционного образования базируется на её интеграции с сервис-ориентированной системой интеллектуального поиска контента, обладающей мягкой архитектурой, основные принципы которой представляются в [1, 2, 3, 4].

В зависимости от степени интеллектуализации мягкой архитектуры сервис-ориентированной системы различаются три разновидности её концептуальных моделей.

При этом каждая последующая модель архитектуры отличается от предыдущей расширением степени автоматизации процесса формирования контента.

Поиск контента распространяется на решение задач кадрового, материально-технического (МТО) и учебно-методического обеспечения образовательной деятельности.

В модели 1 сервис-ориентированной системы интеллектуального поиска контента для системы дистанционного образования целеполагание заключается в соблюдении гарантий эффективности её функционирования на основе диспетчеризации по интеграции, модельно-аналитического интеллекта и альтернативных стратегий планирования действий в зависимости от состояния окружающей среды (рис. 1).

Методические аспекты выбора алгоритма планирования для сервис-ориентированной системы с мягкой архитектурой представляются в [1, 5].

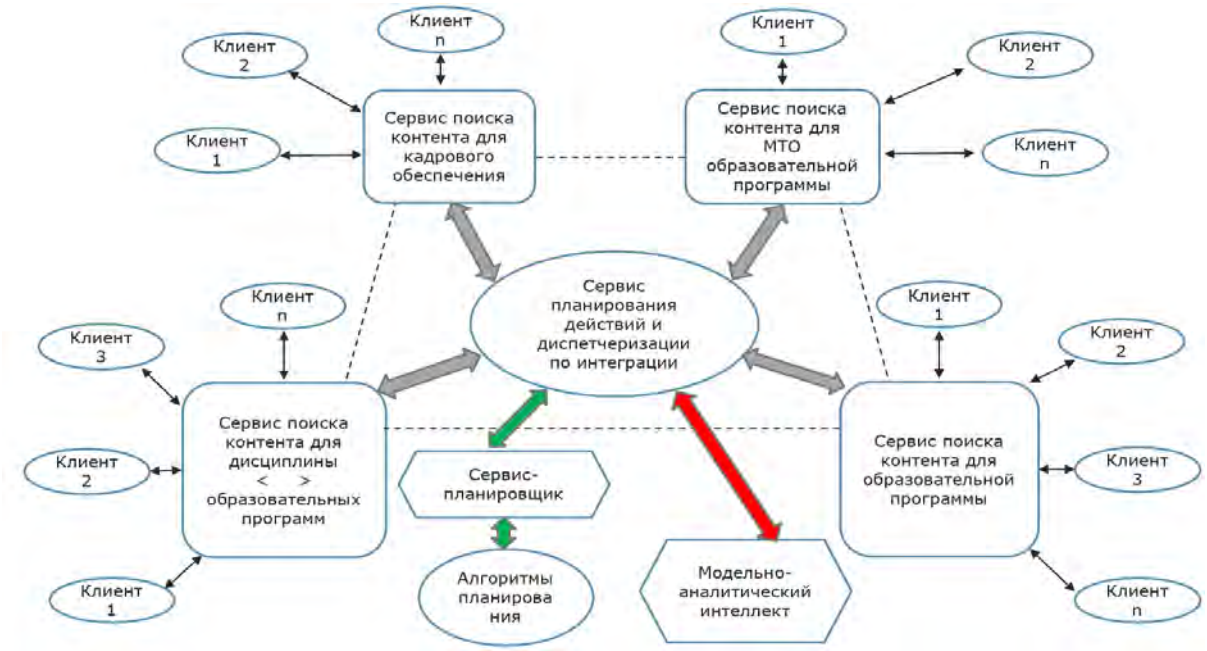


Рис. 1. Модель 1 сервис-ориентированной системы интеллектуального поиска контента для системы дистанционного образования

В модели 2 сервис-ориентированной системы интеллектуального поиска контента для системы дистанционного образования предусматривается выбор наилучшей стратегии планирования действий и диспетчеризации по интеграции образующих компонентов (рис. 2).

Модель 3 сервис-ориентированной системы интеллектуального поиска контента для системы дистанционного образования ориентируется на обеспечение гарантий эффективности её функционирования на основе выбора наилучшей стратегии планирования действий, диспетчеризации по интеграции и модельно-аналитического интеллекта (рис. 3).

Приведённые концептуальные модели описывают возможные вариации в архитектуре сервис-ориентированной системы интеллектуального поиска контента для дистанционного образования с применением методов и средств интеллектуального анализа данных.

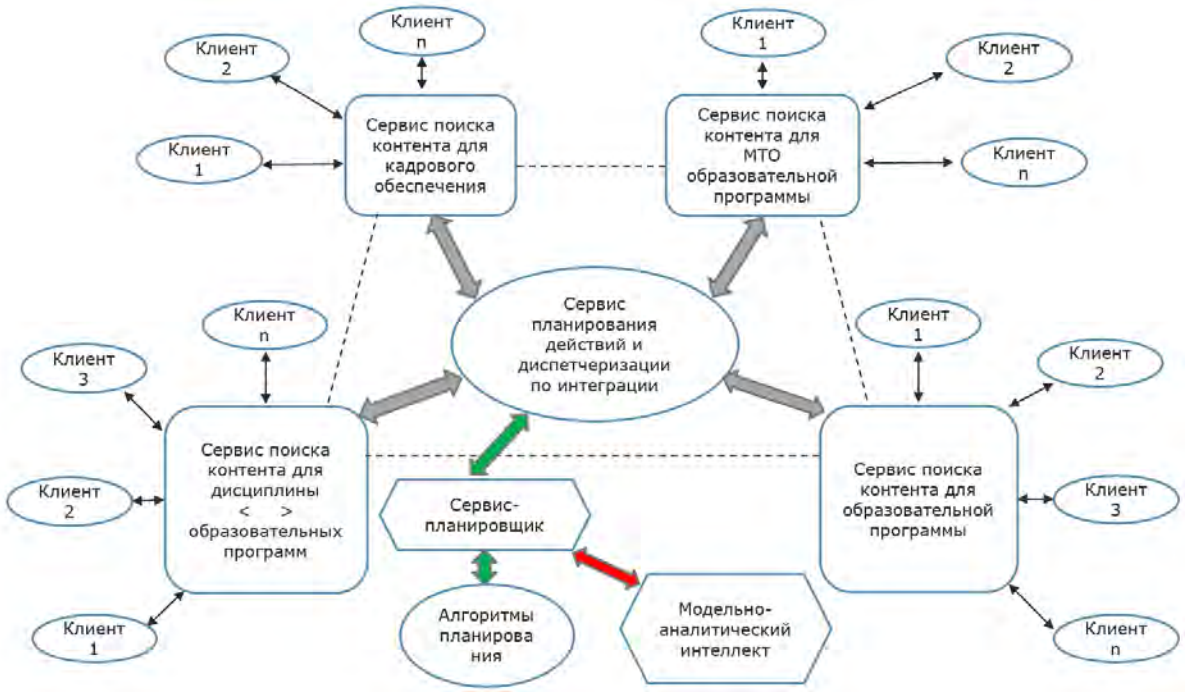


Рис. 2. Модель 2 сервис-ориентированной системы интеллектуального поиска контента для системы дистанционного образования

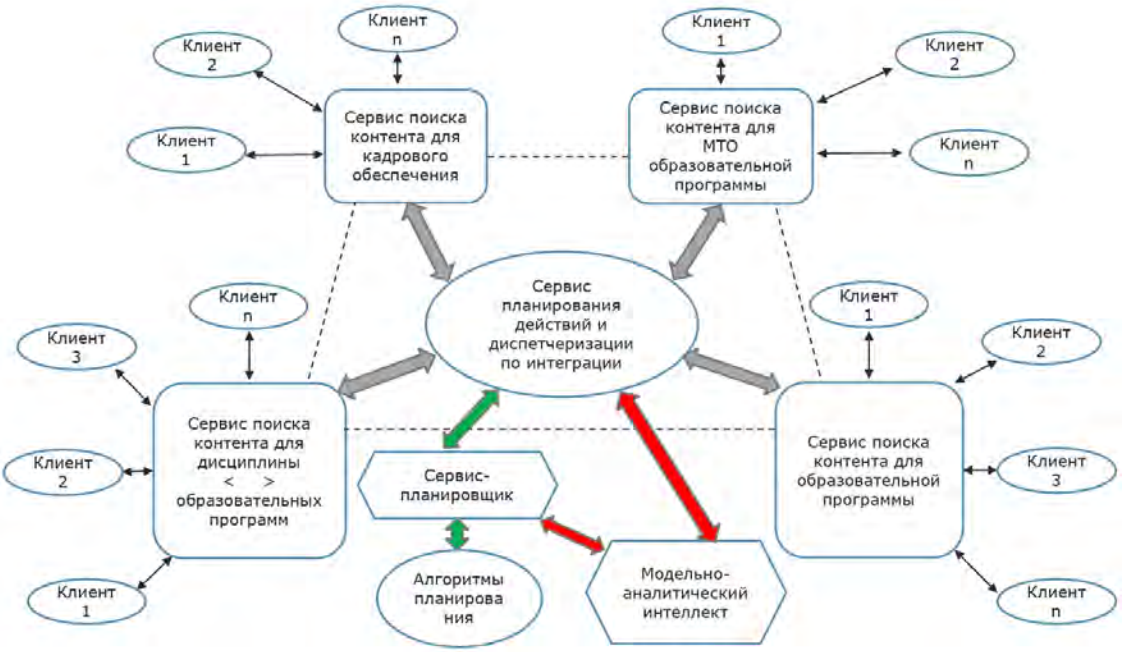


Рис. 3. Модель 3 сервис-ориентированной системы интеллектуального поиска контента для системы дистанционного образования

Использование предложенных решений в системах дистанционного образования позволяет, в отличие от их традиционной организации, задействовать новые подходы к интеллектуализации научно-образовательных сред, которые будут обеспечивать динамическую конфигурацию и соблю-

дение гарантий эффективности функционирования при реактивном реагировании на изменения в результатах развития цифровой экономики в целях повышения качества образования и своевременного формирования компетенций у обучающихся.

Список используемых источников

1. Птицына Л. К., Кондратьев Д. А., Эльсабаяр Шевченко Н. Выбор алгоритма планирования для интеллектуальных сервис-ориентированных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2017. Т. 3. 535 с., С. 277–282.

2. Птицына Л. К., Эль Сабаяр Шевченко Н. Н., Белов М. П. Моделирование сервис-ориентированных систем в условиях неопределённости // Международная конференция по мягким вычислениям и измерениям. 2018. № Секция 2. С. 291–294.

3. Птицына Л. К., Эль Сабаяр Шевченко Н. Интеллектуальная интеграция кластерных сегментов сервис-ориентированных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2018. Т. 2. С. 541–544.

4. Птицына Л. К., Эль Сабаяр Шевченко Н. Многофункциональное интеллектуальное ядро планирования действий с обеспечением качества функционирования городских сервисов для умных городов // V Всероссийская научно-техническая конференция «Модернизация информационной инфраструктуры для сетей 5G/IMT 2020 и для других перспективных технологий в интересах цифровой трансформации регионов»: сб. науч. ст. СПб. : СПбГУТ, 2019. С. 74–80.

5. Птицына Л. К. Интеллектуальные системы и технологии : учебное пособие. СПб. : СПбГУТ, 2019. 231 с.

УДК 004.654
ГРНТИ 20.53.17

ОРГАНИЗАЦИЯ ХРАНИЛИЩА ДАННЫХ В ПЕРСПЕКТИВНОЙ СИСТЕМЕ РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ

А. Ю. Иванов, Д. А. Клеверов, М. А. Клеверов, И. Б. Саенко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Рассматривается аспекты построения хранилища данных в перспективной системе разграничения доступа к информации облачной инфраструктуры, в которой при-

меняется атрибутивно-ориентированная модель разграничения доступа. Обосновывается необходимость и демонстрируется возможность совместного хранения данных, реализованных в формате SQL, XML и RDF.

хранилище данных, разграничение доступа, облачная инфраструктура.

В настоящее время высокую актуальность приобретает задача разграничения доступа к информации в облачных инфраструктурах. Это определяется рядом факторов, к числу наиболее важных из которых относятся: (1) широкое распространение таких инфраструктур среди автоматизированных систем различного назначения, (2) значительное удорожание активов, устройств, программного обеспечения и критически важных данных в таких системах, (3) стремительный рост количества воздействующих на них компьютерных атак. Под облачной вычислительной инфраструктурой (или просто «облачной инфраструктурой») понимается модель сетевого доступа в режиме «по требованию», предполагающая использование вычислительных ресурсов не компьютера, на котором работает пользователь, а сторонней инфраструктуры [1]. Данная модель в первую очередь направлена на повышение доступности вычислительных ресурсов. В свою очередь «модель разграничения доступа» обеспечивает требуемые полномочия доступа субъектов доступа к запрашиваемым объектам. Считается, что в облачной инфраструктуре вероятность реализации несанкционированного доступа к критическим информационным ресурсам существенно возрастает. Это обусловлено тем, что облачная инфраструктура является мультиарендной средой [2].

Известно множество моделей разграничения доступа, которые возможно использовать в облачных инфраструктурах. Наиболее распространенной является ролевая модель (*Role-Based Access Control*, RBAC) [3]. Ролевая модель получила широкое распространение в облачных структурах в связи с тем, что она тесно связана с процессами идентификации пользователей облачных хранилищ и сервисов.

Среди перспективных моделей разграничения доступа, которые возможно использовать в облачных инфраструктурах, следует выделить атрибутивную модель (*Attribute-Based Access Control*, ABAC) [4]. Эта модель выделяет атрибуты объектов, действий, субъектов и условий доступа. При применении этой модели значения атрибутов сравниваются с политикой безопасности, и принимается соответствующее решение о предоставлении доступа. Модель ABAC учитывает, что облачная инфраструктура, как правило, состоит из нескольких автономных корпоративных автоматизированных систем, изначально имеющих различные модели безопасности. Она способна реализовать достаточно гибкий механизм разграничения доступа, поддерживающий гетерогенные структуры и обеспечивающий безопасное функционирование мультиарендной среды. Считается, что недостатком

этой модели является ее узкое практическое распространение. Однако, говоря о перспективной системе разграничения доступа к информации облачной инфраструктуры, следует полагать, что эта система должны быть ориентирована в большей степени на использование модели ABAC.

Перспективная система разграничения доступа к информации облачной инфраструктуры должна решать множество задач, включая оценку качества политик разграничения доступа, их структурную оптимизацию, верификацию и реструктуризацию. Решение каждой из перечисленных задач базируется на соответствующих математических моделях и обеспечивается функционированием соответствующих компонентов, входящих в состав этой системы. Вместе следует отметить, что центральным компонентом этой системы является компонент хранения политик разграничения доступа, или информационное хранилище.

В информационном хранилище системы разграничения доступа должна содержаться информация различных форматов. В частности, информация, характеризующая пользователей облачной инфраструктуры, ее программное и вычислительное обеспечение, обрабатываемые информационные ресурсы, доступ к которым подлежит разграничению, могут иметь формат SQL. Их хранение обеспечивается реляционными СУБД. Однако сами политики разграничения доступа, представляющие собой логические выражения, иногда достаточно сложные, не целесообразно хранить в этом формате. Более удобно и эффективно хранить политики разграничения в форматах XML или PDF.

Этим обусловливаются следующие основные требования, предъявляемые к хранилищу данных в перспективной системе разграничения доступа к информации:

1) Возможность представлять данные в реляционном формате, в XML-формате, а также в RDF-формате. XML-формат позволяет хранить шаблоны политик разграничения доступа, которые записываются на XML-ориентированном языке представления. RDF-формат необходим для реализации логического вывода (верификации политик);

2) Достаточная производительность и отказоустойчивость. Учитывая, что хранилище данных является центральным узлом, достижение этих требований во многом будет определяться за счет использования для развертывания репозитория высокопроизводительной и отказоустойчивой аппаратной платформы;

3) Достаточная гибкость интерфейсов взаимодействия с остальными компонентами перспективной системы разграничения доступа. Для реализации этого требования предлагается ориентироваться на концепцию «сервис-ориентированной архитектуры».

В соответствии с данными требованиями, предлагается в архитектуре хранилища данных выделять два уровня элементов (рис.):

– уровень хранения данных;
– уровень веб-сервисов.

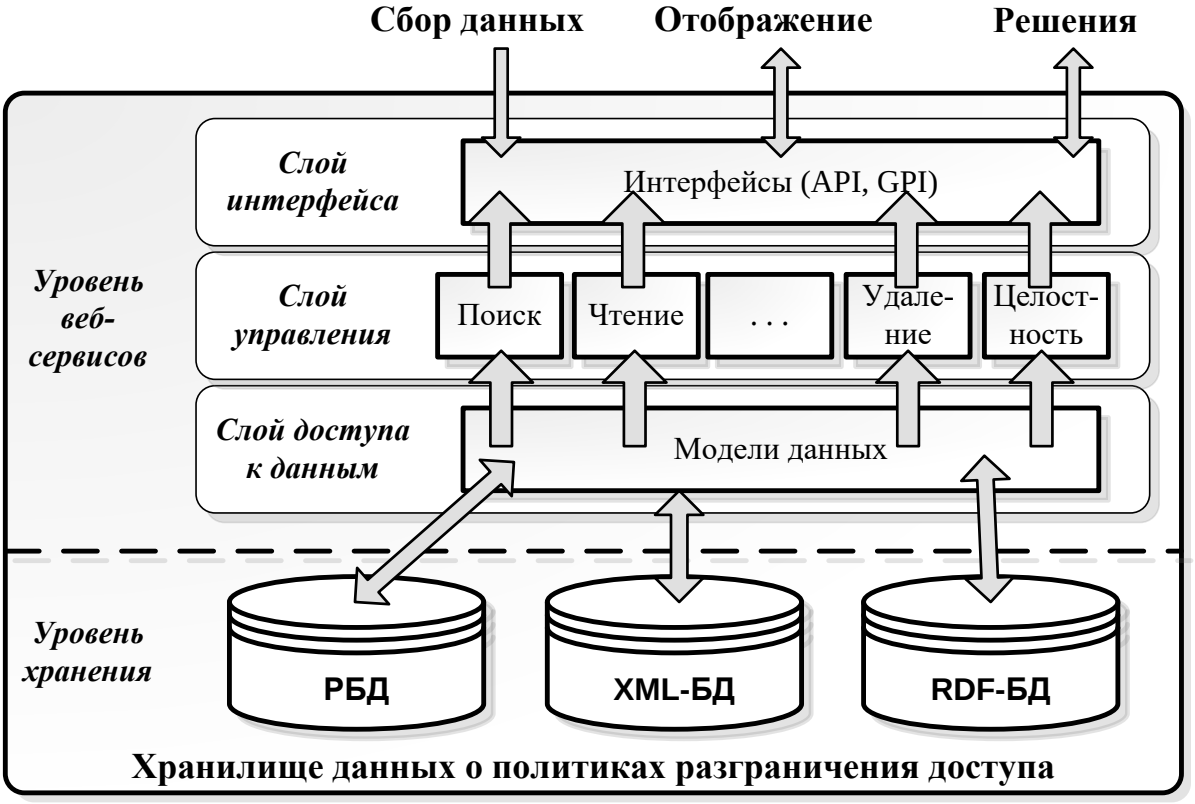


Рис. Архитектура хранилища данных перспективной системы разграничения доступа к информации

Уровень хранения предназначен для хранения всех видов информации, необходимой для решения задачи разграничения доступа в облачной инфраструктуре. Этот уровень архитектуры включает в себя три вида баз данных:

1) Реляционную базу данных (РБД);
2) Базу XML-данных;
3) Базу RDF-данных.

Последняя база данных иначе называется хранилищем триплетов. Тем самым обеспечивается гибридный подход к хранению данных о политиках разграничения доступа, сочетающий в себя достоинства всех базовых моделей представления данных и обеспечивающий, с одной стороны, формализацию политик разграничения доступа в виде сложных логических утверждений, а с другой – использование логического вывода для выработки решений.

Уровень веб-сервисов в свою очередь может быть разделен на делится на три основных слоя: (1) слой доступа к данным; (2) слой управления; (3) слой интерфейсов. Слой доступа к данным обеспечивает обращение

к базам данных с помощью соответствующих моделей данных. Слой управления реализует операции над данными. К числу основных операций на данными можно отнести операции поиска (обработки запросов), чтения, вставки, модификации (изменения), удаления, поддержания ограничений целостности и другие. Слой интерфейса реализует различные виды взаимодействия с компонентами системы разграничения доступа к информации.

Основными взаимодействующими компонентами рассмотренного хранилища являются следующие компоненты: компонент оценки качества политик разграничения доступа, компонент структурной оптимизации политик разграничения доступа, компонент верификации и обеспечения непротиворечивости политик разграничения доступа и компонент структурной реконфигурации политик разграничения доступа.

Реализация хранилища данных рассмотренной выше архитектуры была выполнена в среде комплексной семантической системы хранения Virtuoso (сайт разработчика – http://virtuoso.openlinksw.com). Оценка функциональных показателей сконструированного таким образом хранилища данных показала, во-первых, полноту реализации функций хранения и интеграцию политик разграничения доступа в различных форматах, и, во-вторых, достаточно высокую производительность при работе с RDF-данными.

Работа выполнена при частичной финансовой поддержке проекта РФФИ № 18-07-01369 и бюджетной темы 0073-2019-0002.

Список используемых источников

1. Саенко И. Б., Бирюков М. А., Ефимов В. В., Ясинский С. А. Модель администрирования схем разграничения доступа в облачных инфраструктурах // Информация и космос. 2017. № 1. С. 121–126.

2. Ngo C., Demchenko Y., De Laat C. Multi-tenant attribute-based access control for cloud infrastructure services // Journal of information security and applications. 2016. Vol. 27-28. PP. 65–84.

3. Саенко И. Б., Бирюков М. А., Ясинский С. А., Грязев А. Н. Реализация критериев безопасности при построении единой системы разграничения доступа к информационным ресурсам в облачных инфраструктурах // Информация и космос. 2018. № 1. С. 81–85.

4. Servos D., Osborn S.L. Current Research and Open Problems in Attribute-Based Access Control // ACM Comput. Surv. 2017. Vol. 49, No. 4. Article 65, 45 pages.

УДК 004.8
ГРНТИ 28.23.37

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ПОИСКА УЯЗВИМОСТЕЙ ИСХОДНОГО КОДА

К. Е. Израилов, С. А. Кузнецов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

*В статье рассмотрена возможность применения искусственного интеллекта в области информационной безопасности. Предлагается способ разрешения противоречия предметной области, заключающегося в следующем: «заточенность» типовых алгоритмов на обнаружение конкретных уязвимостей по строго заданным шаблонам **vs** тенденция постоянной модификации функций программного обеспечения, ведущая к соответствующей «флуктуации» его кода. Предложена гипотетическая система выявления уязвимостей программного обеспечения путем обучения искусственного интеллекта злонамеренными образцами исходного кода. Результаты такого обучения могут быть использованы для вероятностного обнаружения частей кода, относящихся к различным классам уязвимостей, но не являющихся тождественными ни с одним из имеющихся образцов. Предлагается базовая признаковая модель исходного кода, содержащая информацию об уязвимостях и подходящая для обучения нейронной сети.*

искусственный интеллект, нейронная сеть, исходный код, уязвимость, информационная безопасность.

Введение

В настоящее время наличие уязвимостей в исходном коде является одной из актуальнейших проблем в области информационной безопасности (ИБ). При этом уязвимости могут быть внесены туда как случайно – программистами в процессе разработки программного обеспечения (ПО), так и злонамеренно – инсайдерами при получении незаконного доступа к хранилищу кода [1, 2]. И если большинство существующих способов обеспечения безопасности исходного кода полагается на сигнатурный поиск злонамеренных образцов, то в случае мутационного или эволюционного их изменения (то есть развития) способы будут иметь низкую результативность. Данное противоречие – «заточенность» способов под конкретные шаблоны ***vs*** возможная модифицируемость уязвимостей – и определяет основное противоречие предметной области. Для разрешения противоречия может оказаться работоспособным подход, успешно применяемый в других задачах ИБ [3, 4, 5, 6], а именно – использование искусственного интеллекта (ИИ), позволяющего делать вероятностные предсказания относительно результатов исследований на основании неполного набора имеющихся знаний. С авторской точки зрения, востребованным в данном вопросе

должно стать решение задачи в виде применения методов машинного обучения (как составной части ИИ), основанных на нейронных сетях. Исследованию этого и посвящена данная статья.

Гипотетическая система

На основании исследования предметной области была разработана гипотетическая система (Система) интеллектуального поиска уязвимостей в исходном коде, основанная на применении нейронной сети и состоящая из двух элементов: генератора, создающего набор различных по содержанию и одинаковых по форме уязвимостей [7]; Нейронная сеть (Нейросеть), работающая с текстом исходного кода (включающего также и возможные уязвимости). Шаги схемы состоят из следующих:

1. В генератор подается файл с исходным кодом уязвимости.
2. Генератор создает множество уязвимостей, близких к исходным.
3. Исходный код уязвимостей преобразуются к некоторой битовой последовательности, описывающей последовательность токенов кода (ключевых слов, идентификаторов и т. п.).
4. Полученная битовая последовательность уязвимости приводятся к виду обучающей выборки Нейросети.
5. Производится обучение Нейросети по выборке.
6. Аналогичным образом исходный код, тестируемый на наличие уязвимостей, преобразуется к тестовой выборке.
7. Нейросеть проверяет тестовую выборку исходного кода на наличие в нем уязвимости согласно своей обучающей выборке.
8. На основании близости результата работы Нейросети к значению *1* (*Да*) или *0* (*Нет*) делается вывод относительно наличия уязвимости в коде.

Для каждой уязвимости применяется своя Нейросеть. Опишем более детально элементы Системы.

Генератор уязвимостей

Генератор уязвимостей может быть реализован на основании использования некоторого шаблона содержания входной уязвимости (ее алгоритма) путем внесения шумов в форму уязвимости (ее внешний вид). Так, например, по следующему шаблону уязвимости (наличие встроенного пароля администратора):

```
if (user == “admin” && password == “password”)
   run_login();
```

генератор создаст 3 следующие ее модификации:

```
if (password == “password” && user == “admin”)
   run_login();
```

```
if (user == “admin”)
  if (password == “password”)
    run_login();

if (password == “password”)
  if (user == “admin”)
    run_login();
```

Отметим, что, гипотетически для генерации модифицированных уязвимостей также возможно применение генетических алгоритмов из состава методов машинного обучения

Нейронная сеть

Нейросеть представляет собой систему связанных сигмоидных нейронов, определяемых следующими параметрами: вес входа (w) – изменяемый самой Нейросетью в процессе обучения, общее смещение (b) – барьер активации (например, величина, которую нужно прибавить к результирующей функции для дальнейшей работы с другими слоями Нейросети). После преобразований нейрон выдает некоторое значение, классически вычисляемое по формуле (1) и представляющее собой сглаженную ступенчатую функцию (рис. 1):

$$\sigma(x) = \frac{1}{1+\exp(-(w*x-b))} \quad (1)$$

где σ – сигмоидный нейрон, w – вес входного значения, x – входное значение, b – смещение.

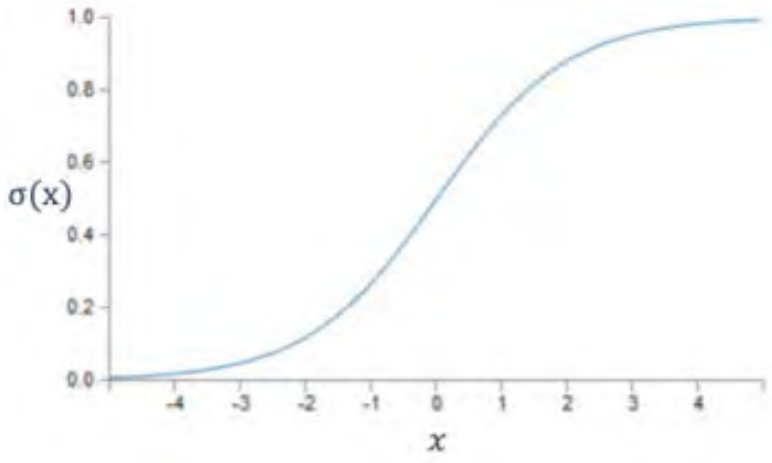


Рис. 1. График сглаженной ступенчатой функции

В интересах решения текущей задачи поиска уязвимостей в качестве топологии Нейросети имеет смысл использовать следующую: первый слой

имеет сгруппированные нейроны, каждый из которых ответственен за распознавание своего токена в последовательности исходного кода; второй слой ответственен за распознавания конфигурации этих токенов; третий – за принятие решения касательно отнесения исходного кода к уязвимости. Описанная Нейросеть показана на рис. 2.

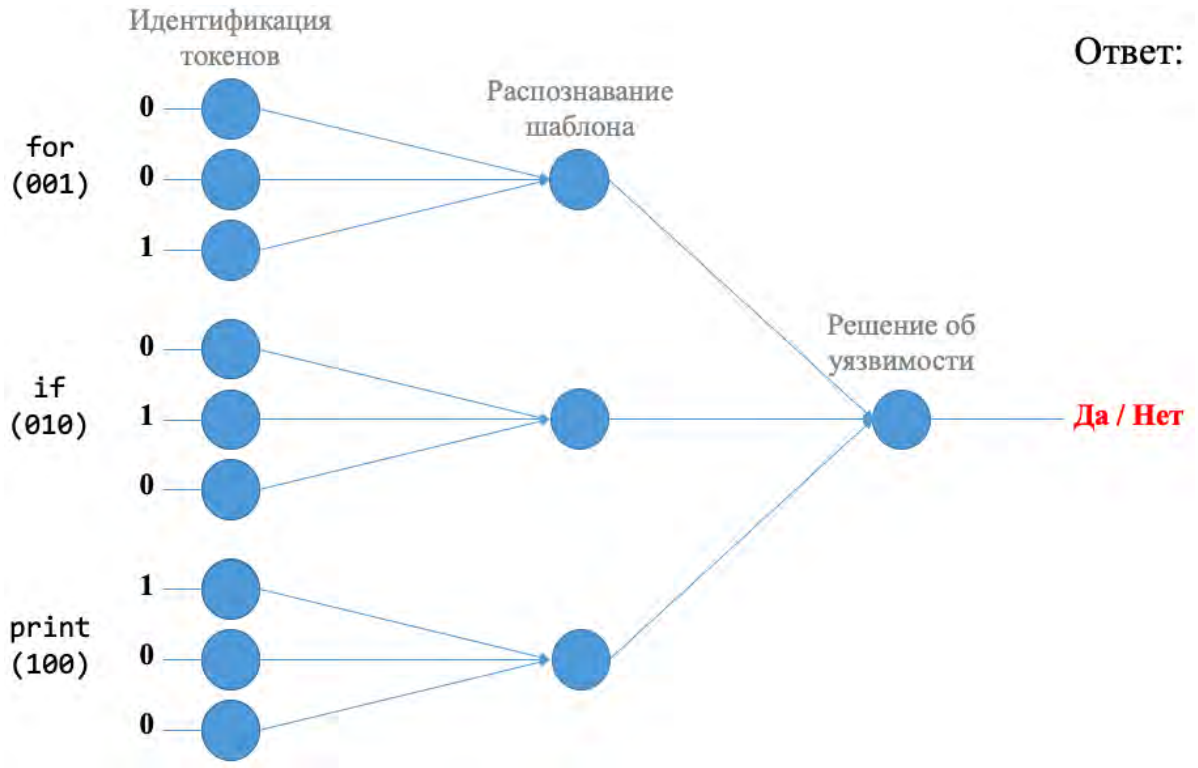


Рис. 2. Нейросеть выявления уязвимостей в исходном коде

В случае низкой результативности предложенной Нейросети количество ее скрытых слоев может быть увеличено; тем не менее, это негативно скажется на скорости работы и времени обучения. Также для проектирования входного слоя необходимо вычислить максимальный размер обучающей выборки – данная величина зависит от размера кода и количества типов токенов исследуемой уязвимости.

Входные и выходные данные

Входными данными Нейросети может быть последовательность битовых векторов – то есть признаковая модель кода, каждый из которых ответственен за свой токен. Вектор представляет собой уникальный набор бит, полученный, например, при помощи алгоритмов Word2Vec для каждого токена. Пример такой векторизации представлен в таблице.

ТАБЛИЦА. Пример векторизации токенов исходного кода

Токен	Вектор
For	001
If	010
Print	100

Выходными данными сети будет ее предположение относительно соответствия входной последовательности токенов исходного кода последовательности одной из обученных ранее уязвимостей. Таким образом, Нейросеть с некоторой вероятностью сможет отнести тестируемый код к разряду небезопасных.

После завершения этапов разработки, настройки и подготовки, необходимых для работы Нейросети, составляется валидационная выборка.

Необходимо отметить и возможные недостатки предложенного решения. Существенной проблемой всех нейросетей является их свойство «недообучаться» и «переобучаться». Недообученная сеть не может правильно присвоить исследуемый объект к ранее обученным классам данных, а переобученная, наоборот, ищет зависимости там, где их нет. Это может быть разрешено так называемой *валидационной выборкой*.

Выводы

Как показало исследование, гипотетически возможно применение Нейросети для поиска уязвимостей в исходном коде. Следующим шагом должна стать практическая реализация интеллектуальных алгоритмов, проверка их на практике и обоснование достоверности сделанных предположений. Все эти этапы планируется осуществить авторами в последующих публикациях.

Список используемых источников

1. Буйневич М. В., Израилов К. Е., Мостович Д. И., Ярошенко А. Ю. Проблемные вопросы нейтрализации уязвимостей программного кода телекоммуникационных устройств // Проблемы управления рисками в техносфере. 2016. № 3(39). С. 81–89.

2. Израилов К. Е. Архитектурные уязвимости программного обеспечения // Шестой научный конгресс студентов и аспирантов СПбГИЭУ (ИНЖЭКОН-2013): сборник тезисов докладов научно-практической конференции факультета информационных систем и экономике и управлении «Инфокоммуникационные технологии и математические методы». 2013. С. 35.

3. Ушаков И. А., Котенко И. В., Крылов К. Ю. Анализ методик применения концепции больших данных для мониторинга безопасности компьютерных сетей // Информационная безопасность регионов России (ИБРР-2015): материалы конференции. 2015. С. 75–76.

4. Котенко И. В., Ушаков И. А. Использование технологий больших данных для мониторинга инцидентов информационной безопасности // Региональная информатика «РИ-2016»: материалы конференции. 2016. С. 168–169.

5. Штеренберг С. И., Виткова Л. А., Просихин В. П. Методика применения концепции адаптивной саморазвивающейся системы // Информационные технологии и телекоммуникации. 2014. Т. 2. № 4. С. 126–133.

6. Виткова Л. А. Исследование распределенной компьютерной системы адаптивного действия // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 44–48.

7. Израилов К. Е., Татарникова И. М. Подход к анализу безопасности программного кода с позиции его формы и содержания // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международной научно-технической и научно-методической конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. С. 462–467.

УДК 004.05
ГРНТИ 20.53.01

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИСТЕМ АНТИЛПАГИАТА

К. Е. Израилов, И. М. Татарникова, А. В. Федорова, В. Ю. Ширев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье дается определение понятий, связанных с программами проверки текста на наличие заимствований и выявления оригинальности – так называемых программ проверки на плагиат или антиплагиата. Приводятся результаты эксперимента по проверке научных работ в трех различных системах. Выполняется сравнительный анализ наиболее известных программ по различным критериям. По результатам проведенных экспериментов и научных изысканий делаются выводы, связанные с дальнейшим развитием информационных систем и технологий по разработке программного обеспечения в рассматриваемой области.

плагиат, заимствование, оригинальность текста, уникальность, критерии проверки, программы антиплагиата, экспертные системы.

Заимствование – процесс, который можно наблюдать на протяжении всей истории человеческой цивилизации. В некоторых областях человеческой деятельности заимствование является положительной практикой. Примером может служить лингвистика. Научная и техническая лексика во многом заимствована из тезауруса латинского и греческого языков. Термин «анализ» произошел от древнегреческого слова ἀνάλυσις, означающего «разложение, расчленение». Термин «диагноз» – от латинского слова

diagnosis, что переводится как «распознавание»: от dia «врозь» + gnosis «знание», диалектика [1]. В XX–XXI вв. в технической сфере для обозначения новых понятий используют слова английского языка: *принтер, компьютер*, *роутер*.

Однако технические возможности, открытый доступ к источникамзнаний, поиск которых не ограничен ни временным ресурсом, ни расстоянием, сегодня породили явление несамостоятельности подготовки научных работ. В зависимости от обстоятельств применяется два термина, характеризующих отсутствие уникальности материала. Термин «плагиат», как правило, используют в тех случаях, когда рассматриваются юридические аспекты проблемы. Кроме того, под плагиатом чаще понимают заимствование идей, изложенных другим словами или включение уже опубликованных текстов в собственный научный труд. Когда речь идет скорее о проблемах оформления и соблюдения стандартов, упоминают «некорректные заимствования» [2].

Оригинальность и качество научных исследований – ключевые критерии при аттестации научных и научно-педагогических работников. Порядок выявления плагиата в диссертационных исследованиях, процедурные аспекты применения рекомендаций по выявлению плагиата, порядок рассмотрения обращений и материалов о предполагаемом наличии в диссертации нарушения авторских прав в ВАК при Минобрнауки были рассмотрены в работе Шахрая С. М., Аристера Н. И. и Тедеева А. А. [3].

Для оценки уникальности текста применяют специальные сервисы и программы, работающие по различным алгоритмам. Например, Севостьянов О. И. в своей работе описывает методы дактилоскопии, анализа «множества слов», анализа шаблона цитат, изучения языковых стилей [4].

Для выявления различий в результатах работы программных средств данного класса был проведен эксперимент, заключающийся в сравнении двух систем обнаружения текстовых заимствований: «Антиплагиат» [5] и «Руконтекст» [6]. Для этого была проведена проверка уникальности 20 научных работ посредством сервисов обеих систем, а также одной из бесплатных программ, доступных в сети. Диаграмма, иллюстрирующая уникальность систем при проверке различных образцов текста представлена на рис. Здесь по оси абсцисс отложены идентификаторы образцов, а по оси ординат – выявленный с помощью программ процент уникальности текста. Кроме того, был проведен сравнительный анализ функциональности этих систем, который строился на сопоставлении наличия компонент, включенных в предлагаемое к приобретению программное обеспечение (табл., см. ниже).

На рисунке (см. ниже) можно увидеть, что уникальность текстов при проверке программным обеспечением «Антиплагиат» в среднем ниже, чем

при проверке с помощью системы «Руконтекст», т. е. эти проверки выполнены более качественно. Однако, анализ составляющих компонент предлагаемых систем показывает, что программа «Руконтекст» имеет некоторые преимущества. Например, возможность увидеть, откуда именно заимствован текст: в правой колонке представлен оригинальный текст с указанием страниц. Эта дополнительная функция дает возможность пользователям более скрупулезной работы в информационном пространстве.

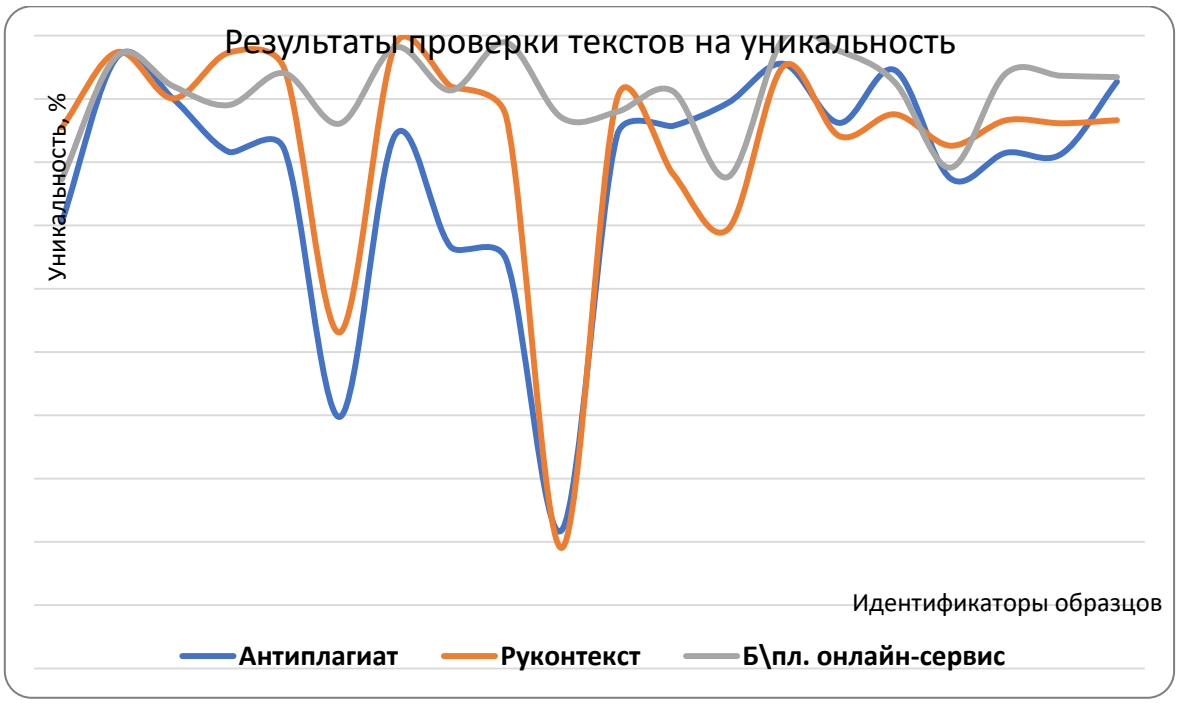


Рис. Результаты эксперимента на проверку текстов системами обнаружения текстовых заимствований

ТАБЛИЦА. Результаты сравнительного анализа систем «Антиплагиат» и «Руконтекст»

Антиплагиат	Руконтекст
Количество индексируемых документов	
– ежемесячно индексируется более 20 млн новых документов – дополнительно был разработан алгоритм поиска текстовых заимствований	– заявлено 2 млрд документов в индексе
– открытые источники сети Интернет (более 480 млн источников), включая: • журналы ВАК • сайты ученых советов • Википедия • Arxiv.org • Cyberleninka.ru • другие открытые сайты (рефераты, аналитика, СМИ)	– открытые источники сети Интернет (1,8 млрд источников), включая: • базы рефератов • Cyberleninka.ru • Википедия • Студопедия • авторефераты ВАК • сайты СМИ

Антиплагиат	Руконтекст
– коллекция Патентов: обеспечивает поиск по текстам патентов на русском и иностранных языках	– коллекция ФИПС: обеспечивает поиск по текстам патентов только на русском языке
– коллекция РГБ	– коллекция РГБ
– коллекция eLibrary	– коллекция eLibrary
– коллекция ГАРАНТ	– коллекция НПБ «Кодекс»
– коллекция Национальной Библиотеки Белоруссии	
– сводная коллекция ЭБС: • Университетская библиотека онлайн • ЦНМБ ПМГМУ им. Сеченова • ЭБС Лань • ЭБС БиблиоРоссика • ЭБС Юрайт • ЭБС Айбукс • ЭБС Book.ru • ЭБС Консультант студента ИГ	– подключены отдельные ЭБС: • Университетская библиотека онлайн • ЦНМБ ПМГМУ им. Сеченова • ЭБС БиблиоРоссика
– собственная коллекция вуза: неограниченный объем по количеству и по объему загруженных документов; возможность пакетной загрузки в Хранилище (без ограничения количества файлов, без проверки на заимствования) – коллекция «Кольцо вузов»	– собственная коллекция вуза: доступна пакетная загрузка на проверку, ограничение – не более 20 файлов – доступна проверка по некоторым базам других вузов
Дополнительные возможности	
– модуль поиска перефразированных заимствований:перефразирование используется для искусственного завышения оригинальности документа, когда исходный текст источника подвергается переписыванию, или рерайту	– обнаружение заимствований с использованием перефразировки
– определение общеупотребительных выражений, что позволяет не учитывать их в качестве заимствований	– возможность ручной маркировки фрагмента как общеизвестного факта
– определение библиографических записей, что позволяет маркировать их как цитирования и не учитывать в качестве заимствований	– список литературы не проверяется
Иностранные языки, на которых возможна проверка	
английский, казахский, белорусский, киргизский – поиск переводных заимствований	английский
Возможности при работе с отчетом	
– 2 вида отчета: краткий и полный – краткий отчет содержит процент оригинальности, заимствования, цитирования,	– 2 вида отчета в формате pdf (оба содержат процент оригинальности, заимствования, цитирования, а также список

Антиплагиат	Руконтекст
а также список найденных источников заимствования – полный отчет содержит процент оригинальности, заимствования, цитирования, список найденных источников заимствования, а также полный текст загруженного документа с наложением разметки заимствований	найденных источников заимствования, нет размеченного текста документа); отличаются только видом отображения – отчет по заимствованиям в виде двухколоночного текста: фрагмент текста проверяемой рукописи и фрагмент из источника, откуда заимствование (с указанием страницы, где это найти)
– возможна выгрузка отчета в формате pdf, docx	– возможна выгрузка отчета в формате txt, xsl, docx
– полный отчет редактируется: исключать источники и отдельные блоки, изменять тип источника с цитирования на заимствование и наоборот	– редактировать можно источники и блоки заимствования: • пометить как общеизвестный факт • пометить как работу автора • пометить как корректное заимствование
– результаты корректировок сохраняются	
Механизм выявления и оповещения о попытках «обхода» системы	
– обходы разделены на несколько типов: • замена символов • невидимые символы • очень мелкий текст • мелкий шрифт • изменение цвета текста на фоновый – при обнаружении обходов, текст очищается от лишних слов и символов, данный текст проверяется и результаты попадают в итоговый процент заимствований	– существует отображение обходов, выделяется 2 типа: • замена символов • скрытый текст – при этом текст с обходами не проверяется, что искажает процент заимствований
– разработан и внедрен способ извлечения текста документа с использованием техник оптического распознавания: на проверку поступает именно тот текст, который отображается при просмотре документа	

Итак, по результатам проведенных исследований и поставленных экспериментов можно сделать следующие выводы:

1. Область исследований, оперирующая с понятиями «оригинальность текста», «уникальность текста», «заимствование», «плагиат» и «антиплагиат» является междисциплинарной. С этими терминами так или иначе связаны философия, юриспруденция, лингвистика, информатика, программирование.

2. В настоящее время в связи со все более увеличивающимися информационными потоками и необходимостью переработки информации тематика, связанная с выявлением оригинальности текстов, является актуальной. Многообразие появляющихся задач, требующих решения, позволяет говорить о необходимости новых разработок.

3. Программы, позволяющие проверить оригинальность текста и процент заимствований, или, по-другому, программы класса антиплагиата, работают по разным алгоритмам, предоставляют разный набор функций и дают различные результаты при проверке одного и того же текста.

4. Различным организациям для различных целей требуется разный функционал подобных программ, что, в итоге, может повлиять на выбор соответствующих программных средств, а также являться стимулом для научных изысканий и практических разработок в конкретных областях.

В области информационных систем и технологий в основном рассматриваются задачи построения алгоритмов работы программ и систем проверки на антиплагиат. И здесь разработчикам необходимо не только предлагать новые алгоритмы и функции проверки, но и предупреждать различные способы «обхода» пользователями алгоритмов проверки, включая рерайтинг текста и проч.

Одной из нетривиальных задач, связанной с разработкой систем проверки на наличие плагиата, является разработка моделей и методов настройки конкретной программы проверки на нужды пользователя, т. е. предоставления возможности выбора необходимого функционала и степени или «глубины» проверки, впоследствии выполняемой в экспертном режиме. Также здесь можно говорить о разработке специализированных экспертных систем, позволяющих сделать выбор в пользу того ил иного программного продукта или использования его функционала.

Список используемых источников

1. Нарожная В. Д., Садыкова Л. Греко-латинские заимствования в русском языке // Вестник Московской международной академии. 2011. № 1. С. 82–87.

2. Чехович Ю. В. Об обнаружении заимствований при экспертизе научных статей // Научная периодика: проблемы и решения. 2013. № 4 (16). С. 22–25.

3. Шахрай С. М., Аристер Н. И. и Тедеев А. А. О плагиате в произведениях науки (диссертация на соискание ученой степени): научно-методическое пособие. М. : МИИ, 2014. 176 с.

4. Севостьянова И. О. Обзор систем проведения проверки на плагиат: общероссийские и зарубежные // Научное обозрение. Педагогические науки. 2017. № 5. С. 162–166.

5. Антиплагиат. URL: https://www.antiplagiat.ru/

6. Руконтекст. URL: https://text.rucont.ru/

Статья представлена научным руководителем, профессором кафедры БИС СПбГУТ доктором технических наук, профессором М. В. Буйневичем.

УДК 004.7:004.422.8
ГРНТИ 20.01.07

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО СТИМУЛИРОВАНИЮ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПЕДАГОГОВ

А. Н. Кадынцев, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Актуализировано развитие информационных систем образовательных учреждений. Показана целесообразность создания информационно-аналитической системы поддержки принятия решений по стимулированию образовательной деятельности педагогов. Представлены условия стимулирования. Рассмотрены основания для выбора решающих правил. Описаны ключевые особенности метода таксономии. Раскрыто математическое обеспечение информационно-аналитической системы поддержки принятия решений по стимулированию образовательной деятельности педагогов. Продемонстрированы возможности комплексной оценки эффективности образовательной деятельности педагогов.

образование, педагог, информационно-аналитическая система, поддержка принятия решений, стимулирование, математическое обеспечение.

В Российской Федерации сфера образования является основой социума для перспективного развития информационного общества с высоким качеством жизни. В настоящее время наблюдается достаточно много проблемных ситуаций в сфере образования. Они, прежде всего, касаются условий труда и заинтересованности молодого поколения педагогов в сфере образования.

С 2017 года реализуется программа «Цифровой экономики Российской Федерации», нацеленной на переход к новому качественному состоянию экономического развития. Одновременно с этим с 2019 года особое внимание обращается на развитие искусственного интеллекта, для ускорения которого принята «Национальная стратегия развития искусственного интеллекта». Искусственный интеллект становится важной частью жизни человека, общества, экономики и государства. Каждым субъектом информационного общества ощущается влияние реализуемых возможностей технологий искусственного интеллекта на настоящее и будущее.

В связи с этим повышаются требования к качеству деятельности образовательных организаций, к содержанию образования, к организации учебного процесса, к уровню квалификации педагогических работников. В то же

время, в системе образования наблюдается низкий уровень входного потока молодых специалистов, невысокий уровень интереса и мотивации работающего персонала в карьерном росте и самосовершенствовании.

В сложившихся условиях управление образовательным учреждением становится быть целенаправленным и включающим в себя планируемое стимулирование деятельности работников для достижения максимально возможного результата.

За счет реализации системы стимулирования работников повышается интерес к профессиональной деятельности и эффективность выполнения должностных обязанностей, наблюдается развитие удовлетворенности работников результатами и процессом деятельности.

При использовании информационных систем для управления образовательным учреждением планируемое стимулирование деятельности работников может рассматриваться одним из системообразующих процессов, предусматривающим оценивание качества образования и информационно-аналитическую поддержку принятия решений для последующего начисления надбавок к заработной плате педагога.

Многочисленные существующие системы поддержки принятия решений разрабатываются применительно к прикладным задачам профессиональной деятельности и основываются на обработке больших массивов информации с помощью соответствующих алгоритмов и выбора оптимальных стратегий. Ярким примером подобного обстоятельства является система WebQUIK, предназначенная для просмотра массивов информации и принятия решений применительно к различным предметным областям. В качестве другого, не менее яркого примера, может рассматриваться мощный пакет технического анализа Meta Stock Pro, представляющий собой новый стандарт программного обеспечения, разработанного для профессиональных трейдеров и управленцев, позволяющий проводить графический анализ состояния исследуемого параметра и принимать решение относительно выбора оптимальной стратегии управления в режиме реальном времени.

Каждая из рассмотренных систем по своему функционалу не согласуется со спецификой работы образовательной организации и больше ориентируется на сопровождение работы с финансовыми рынками.

В связи с представленными основаниями актуализируется разработка информационно-аналитической системы поддержки принятия решений по стимулированию образовательной деятельности педагогов, которая, с одной стороны, относится к системам управления персоналом [1], а, с другой стороны, – к интеллектуальным системам принятия решений и управления [2].

В разработанной информационно-аналитической системе осуществляется выявление наиболее эффективных педагогов образовательного учреждения с целью последующего поощрения путем выплаты стимулирующих

надбавок. В архитектуре этой системы объединяются экспертная подсистема оценки количественных показателей качества деятельности педагогов, подсистема поддержки принятия решения по ранжированию баллов на основе таксономического метода и экспертная подсистема по распределению надбавок из бюджета.

Экспертные подсистемы строятся на базе сформированных продукционных правил.

В подсистеме поддержки принятия решения применяется таксономический метод для определения рейтинга анализируемым образовательным учреждениям на основе тех критериев, что задействованы в экспертной подсистеме.

Таксономический метод реализуется за пять этапов.

На первом этапе формируется матрица наблюдений. На втором этапе проводится стандартизация признаков путем перехода к нормированным безразмерным значениям. На третьем определяются стимуляторы и дестимуляторы. На четвертом этапе вычисляются расстояния каждой точки до эталона. На пятом этапе рассчитываются значения показателя уровня развития.

В информационно-аналитической системе на основании анализа интегральных показателей получаются таксономические коэффициенты эффективности деятельности педагогов.

На рис. приводится пример диаграммы рангов педагогов по значениям таксономических коэффициентов.

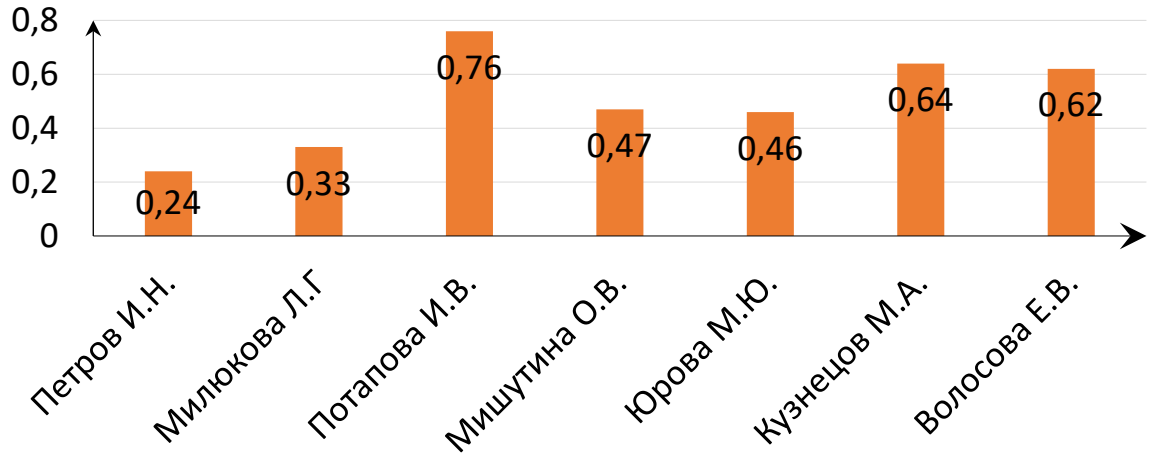


Рис. Пример диаграммы рангов педагогов
по значениям таксономических коэффициентов

Представленная информационно-аналитическая система поддержки принятия решений по стимулированию образовательной деятельности пе-

дагогов обеспечивает исключение субъективизма, автоматический контроль изменений, быстрое определение показателей и избавление от рутинной работы, занимающей много времени.

Список используемых источников

1. Базаров Т. Ю. Управление персоналом : учебник. 15-е изд., стер. М. : Академия, 2018. 314 с.
2. Еременко Ю. И. Интеллектуальные системы принятия решений и управления: учебное пособие. 2-е изд., стер. Старый Оскол : ТНТ, 2018. 402 с.

УДК 004.7:004.422.8
ГРНТИ 20.01.07

МОДЕЛИРОВАНИЕ МУЛЬТИАГЕНТНОЙ СИСТЕМЫ МОНИТОРИНГА ОБОРУДОВАНИЯ ЭЛЕКТРОСЕТЕЙ, ГАЗОВОГО ОБОРУДОВАНИЯ И СРЕДСТВ ВОДОСНАБЖЕНИЯ СФЕРЫ ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА

Д. В. Кадынцева, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Описаны причины развития интеллектуальных систем мониторинга в сфере жилищно-коммунального хозяйства. Обоснована актуальность создания мультиагентной системы мониторинга оборудования электросетей, газового оборудования и средств водоснабжения сферы жилищно-коммунального хозяйства. Построена расширенная объектно-ориентированная модель предлагаемой системы мониторинга. Выбраны показатели качества функционирования системы мониторинга и метод анализа построенной модели. Представлен модельно-аналитический интеллект системы мониторинга в сфере жилищно-коммунального хозяйства.

интеллектуальные системы, мониторинг, жилищно-коммунальное хозяйство, мультиагентная система, модель, качество, модельно-аналитический интеллект.

Неотъемлемой составляющей инфраструктур жизнедеятельности являются жилищно-коммунальные системы. Интенсивное расширение различных видов и форм взаимодействия в средах информационных инфраструктур, быстрое развитие технологических платформ и технологий, целевое формирование экосистемы цифровой экономики в национальном масштабе

становятся движущими силами создания и сопровождения инновационных систем для жилищно-коммунального хозяйства.

Наибольшая техническая значимость в сфере жилищно-коммунального хозяйства ассоциируется с оборудованием электросетей, газовым оборудованием и средствами водоснабжения. Эксплуатация оборудования электросетей, газового оборудования и средств водоснабжения относится к определяющим процессам не только эффективности жилищно-коммунального хозяйства, но и безопасности жизнедеятельности. С учетом подобных обстоятельств повышается степень актуализации обновлений в системах мониторинга представленного оборудования и средств.

Характерная на настоящее время разобщённость в концепциях и реализациях отдельных средств мониторинга оборудования жилищно-коммунального хозяйства является одним из тех факторов, которые не позволяют добиваться не только высокого качества обслуживания населения и необходимого уровня безопасности жизнедеятельности, но создают недопустимые в развитом информационном обществе условия для злоупотреблений.

В контексте Программы «Цифровая экономика России» и Национальной стратегии развития искусственного интеллекта до 2030 года ставится цель развития информационно-эксплуатационного сопровождения систем жилищно-коммунального хозяйства на основе сквозных интеллектуальных информационных технологий.

Для достижения поставленной цели решаются следующие задачи:

– анализ бизнес-процессов работы диспетчерских служб жилищно-коммунального хозяйства;

– разработка концептуальных основ архитектуры мультиагентной интегрированной системы мониторинга электросетей, газового оборудования и системы водоснабжения;

– построение объектно-ориентированной модели мультиагентной системы мониторинга в сфере жилищно-коммунального хозяйства;

– построение расширенной объектно-ориентированной модели мультиагентной системы мониторинга в сфере жилищно-коммунального хозяйства и предложение перспектив ее развития;

– разработка методики определения статистического профиля функционирования мультиагентной системы мониторинга в сфере жилищно-коммунального хозяйства;

– формирование модельно-аналитического интеллекта мультиагентной системы мониторинга в сфере жилищно-коммунального хозяйства.

Мультиагентные системы относятся IT-специалистами к одному из перспективных направлений развития искусственного интеллекта, которое ориентируется на решение сверхсложных задач или глобальных про-

блем. Они проектируются на основе интеграции информационных и коммуникационных технологий, развивая их наукоемкую сущность и расширяя представительность эффективных средств индустрии информации [1].

Разнообразие типовых архитектурных решений организации мультиагентных систем предоставляет широкие возможности для вариаций построения мультиагентных систем в сфере жилищно-коммунального хозяйства.

Типовая схема распределенного решения задачи представляется на рис. 1.

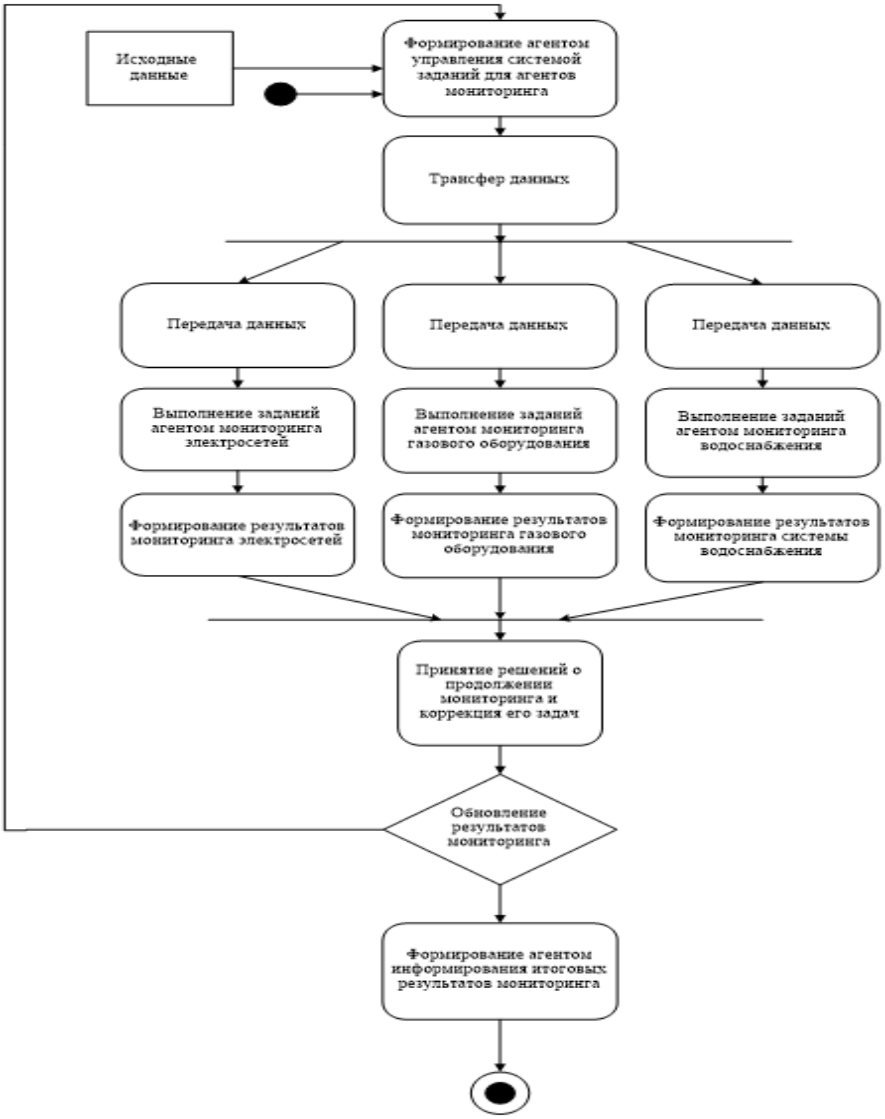


Рис. 1. Распределенный мониторинг оборудования электросетей, газового оборудования и средств водоснабжения жилищно-коммунального хозяйства

В состав мультиагентной системы мониторинга вводятся:

– агент управления системой;
– агент мониторинга электросетей;
– агент мониторинга газового оборудования;

– агент мониторинга системы водоснабжения;
– агент информирования.

На основе разработанной архитектуры мультиагентной системы строится расширенная объектно-ориентированная модель процесса мониторинга, ориентированная на проведение последующего анализа качества её функционирования (рис. 2).

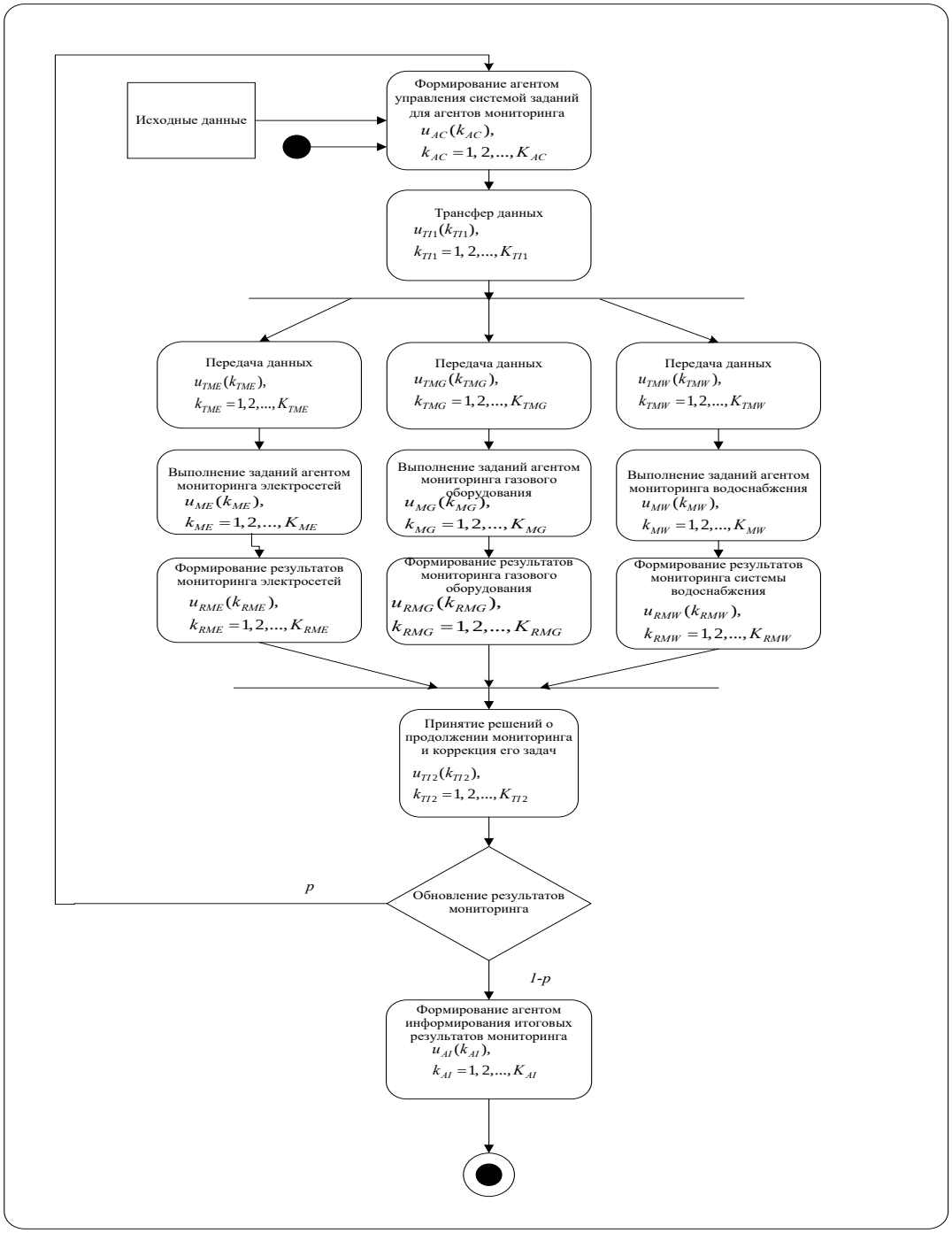


Рис. 2. Расширенная объектно-ориентированная модель процесса мониторинга оборудования электросетей, газового оборудования и средств водоснабжения жилищно-коммунального хозяйства

Для анализа качества функционирования мультиагентной системы выбираются статистические характеристики времени принятия решений о состоянии оборудования и средств, а также риск срыва временного регламента принятия решения о проявлении внештатной ситуации.

На основе преобразования приведённой расширенной объектно-ориентированной модели процесса мониторинга формируется её модельно-аналитический интеллект, обеспечивающий оценивание в реальном режиме функционирования выбранных показателей качества.

Преобразование модели осуществляется посредством применения модифицированного метода свёртки и формализаций, обеспечивающих учет обратных связей в анализируемых моделях [2, 3, 4, 5].

Предложенный вариант организации мультиагентной системы мониторинга оборудования электросетей, газового оборудования и системы водоснабжения в жилищно-коммунальном хозяйстве с модельно-аналитическим интеллектом позволяет повысить степень автоматизации соответствующих технологических процессов и качество предоставляемых услуг. Модельно-аналитический интеллект является частью программного обеспечения рассматриваемой системы.

Применение мультиагентной системы мониторинга оборудования электросетей, газового оборудования и системы водоснабжения позволяет перейти на новый уровень развития информационных структур жилищно-коммунального хозяйства, связанных с территориальной интеграцией распределенных систем.

Список используемых источников

1. Птицына Л. К. Интеллектуальные системы и технологии : учебное пособие. СПб. : СПбГУТ, 2019. 231 с.

2. Птицына Л. К., Лебедева А. А., Белов М. П. Формирование модельно-аналитического интеллекта информационных агентов для реактивных инфокоммуникационных сред // Международная конференция по мягким вычислениям и измерениям. 2016. Т. 1. Секции 1–3. С. 324–326.

3. Птицына Л. К., Лебедева А. А., Хроменков С. В. Расширение модельного пространства агентных технологий // Труды учебных заведений связи. 2016. Т. 2, № 3. С. 45–50.

4. Птицына Л. К., Лебедева А. А. Методика формирования динамических характеристик интеллектуальных информационных агентов в условиях активной инфокоммуникационной среды // Информация и космос. 2017. № 1. С. 105–111.

5. Птицына Л. К., Лебедева А. А., Белов М. П. Метод анализа реактивных действий информационного агента при воздействии инфокоммуникационной среды // Международная конференция по мягким вычислениям и измерениям. 2017. Секция 2. С. 155–158.

УДК 004.056:378 (06)
ГРНТИ 81.93.29

РИСК-ОРИЕНТИРОВАННЫЙ АЛГОРИТМ РАБОТЫ МНОГОФАКТОРНОЙ БИОМЕТРИЧЕСКОЙ ПОРОГОВОЙ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА С ГЕНЕРАЦИЕЙ КЛЮЧА

М. А. Казарин, В. А. Липатников

Военная академия связи

Известные методы аутентификации пользователей информационных систем с применением специальных мер защиты в современных условиях недостаточно эффективны, так как любой аутентификационный фактор может быть скомпрометирован. Цель – разработка метода аутентификации пользователей информационных систем на основе пороговой схемы, повысить результативность аутентификации пользователей информационной системы.

аутентификация, информационные сети, пороговые схемы, алгоритмы, многофакторная биометрическая система.

Проблема защиты конфиденциальной информации на автоматизированных рабочих местах (АРМ) и в настоящее время стоит наиболее остро по причине того, что угрозы нарушения информационной безопасности (ИБ) носят глобальный и трансграничный характер, способы реализации угроз и формы их проявления непрерывно совершенствуются, высокая технологичность этих угроз требует адекватных мер противодействия, предъявляет требования к квалификации специалистов [1].

Использование традиционных способов аутентификации пользователей ИС являются распространёнными и в то же время простыми методами, но не являются достаточно защищенными из-за ряда причин [2, 3]. В [4] предложена биометрическая криптосистема, полученная путем интеграции многофакторной биометрии, пороговой криптографии (схема Шамира) и методов преобразования нечетких биометрических параметров в ключевые последовательности, а также обсуждены преимущества такого решения. Однако, сохраняется вероятность несанкционированного доступа (НСД) к закрытой информации. Также в данной статье не указана область применения предложенной автором схемы.

Объектом в данной работе является система аутентификации пользователей АРМ ИТКС. Предметом является риск-ориентированная биометрическая система аутентификации на основе пороговой схемы.

Цель работы – повысить результативность аутентификации пользователей АРМ ИТКС. Задача – разработать риск-ориентированный алгоритм аутентификации пользователей АРМ ИТКС.

ИТКС – иерархическая модель (рис. 1), представлена тремя уровнями: базовый, распределения и доступа [6].

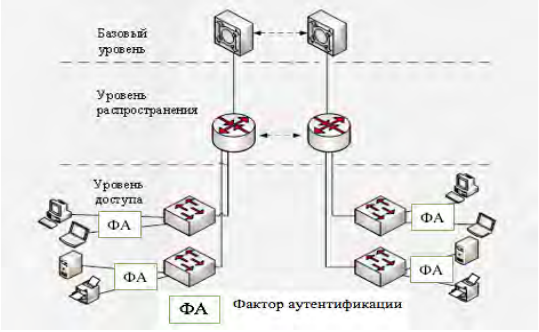


Рис. 1. Модель ИТКС

Эффективность биометрической аутентификационной системы характеризуется двумя параметрами [7]. Ошибочный отказ возникает, когда система не подтверждает личность законного пользователя (типичные значения FRR – порядка одной ошибки на сто). Ошибочное подтверждение происходит в случае подтверждения личности незаконного пользователя (типичные значения FAR – порядка одной ошибки на десять тысяч). В совершенной биометрической системе оба параметра ошибки должны быть равны нулю. Но биометрические системы тоже не идеальны. Обычно системные параметры настраивают так, чтобы добиться требуемого коэффициента ошибочных подтверждений, что определяет соответствующий коэффициент ошибочных отказов.

На данный момент существует два способа, которые позволяют генерировать из биометрических данных ключи, которые удовлетворяют требованиям современной криптографии, и которые обладают при этом низкой вероятностью ошибки второго рода: нейронные сети и нечеткие экстракторы.

Пороговая схема разделения секрета – схема разделения секрета, в которой количество долей, необходимых для восстановления секрета может быть меньше общего количества участников. Пусть n – общее число участников, k – количество долей, необходимое для восстановления секрета. Восстановить секрет может любая группа из k и более участников. Такая схема носит название (k, n)-пороговой схемы разделения секрета [8]. Схема имеет две составляющие: разделение и восстановление секрета. К разделению относится формирование частей секрета и распределение их между членами группы. Обратная схема должна обеспечить его восстановление при условии доступности его хранителей в некотором необходимом количестве [9].

Для снижения вероятности несанкционированного доступа к закрытой информации можно использовать пороговую криптосистему разделения секрета вкупе с многофакторной биометрией и методами преобразования нечетких биометрических параметров в ключевые последовательности. Для входа в систему требуется не один, а несколько биометрических параметров [10]. Это снижает риск того, что злоумышленник получит доступ к защищаемой информации, так как скомпрометировав один биометрический

параметр, например, отпечаток пальца, оставленный на столе, вероятность того, что он скомпрометирует еще какой-либо параметр не велика [11].

Работу риск-ориентированной многофакторной биометрической пороговой криптографической системы разделения секрета с генерацией ключа, основанной на схеме Шамира, можно разделить на три части (рис. 2):

1) Расчет рисков по различным угрозам, учитывая имеющиеся средства защиты, наличие VPN-соединения, наличие у пользователей выхода в Интернет и т. д., сравнение полученного значения риска системы с допустимым;

2) Введение контрмер (многофакторная биометрическая пороговая криптографическая система);

3) Расчет рисков по различным угрозам с учетом введенных контрмер и подсчет эффективности контрмеры.

Рис. 2. Работа риск-ориентированной многофакторной биометрической пороговой криптографической системы разделения секрета с генерацией ключа

Критерий Неймана-Пирсона целесообразно применять в ситуациях, в которых последствия ошибок 1 рода и ошибок 2 рода неодинаковы. Очевидно, что последствия ошибки 2 рода (пропуск события) особо тяжелые, чем ошибки 1 рода (ложная тревога). В этом случае необходимо стремиться к уменьшению условной вероятности ошибки 2 рода за счет увеличения вероятности ошибки 1 рода. Но увеличивать вероятность ошибки 1 рода следует до определенной степени, так как большая вероятность такой ошибки приведет к большим финансовым потерям, а так же к подрыву доверия к системе в целом. Поэтому самый рациональный вариант – это зафиксировать вероятность ошибки 1 рода.

Алгоритм 1 (выработка ключевой информации) и алгоритм 2 (получение секрета) представлены на рис. 3.

Коэффициент риска после внедрения контрмер рассчитывается по формуле (1).

$$E = \frac{R_{old} - R_{new}}{R_{old}}. \quad (1)$$

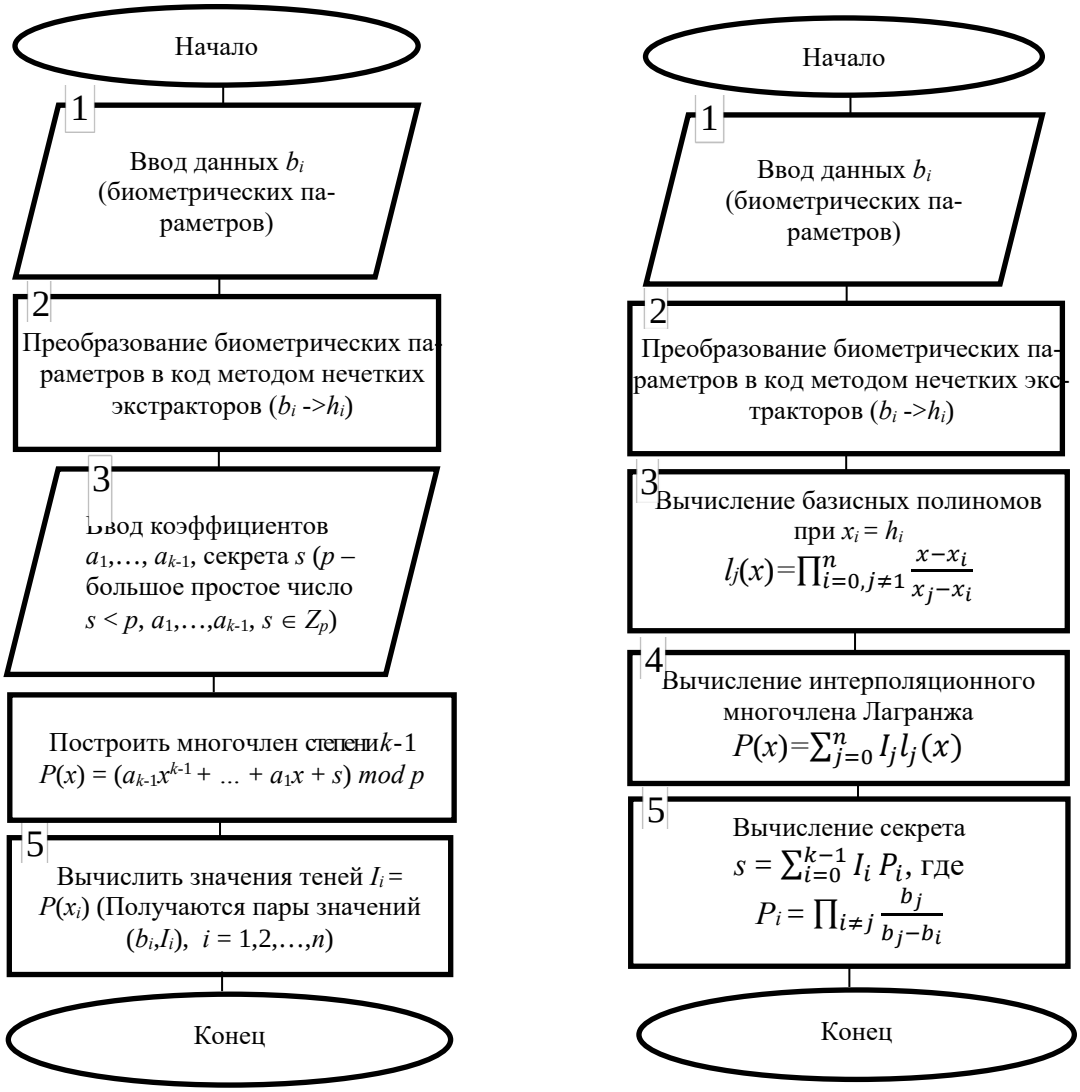


Рис. 3. Структурные схемы алгоритма выработки ключевой информации и алгоритма получения секрета

Суть данной схемы состоит в том, что пользователь в процессе аутентификации вводит n биометрических параметров, которые считываются, затем преобразуются в код, затем формируются доли секрета, и пользователь получает доступ к защищаемой информации, введя k параметров, причем $k < n$ ((k, n)-пороговая схема).Также возможен следующий пример исполь-

зования данной схемы. Для доступа к защищаемой информации, которая доступна *n*, не обязательно, чтобы собрались все, чтобы получить доступ к этой информации. Достаточно, чтобы *k* человек ввели свои биометрические признаки, и доступ к конфиденциальной информации будет открыт.

Новизна предложенного алгоритма работы многофакторной биометрической пороговой криптографической системы разделения секрета с генерацией ключа, основанная на схеме Шамира заключается в том, что в отличие от многофакторной биометрической пороговой криптосистемы [2, 5, 6] введен расчет риска системы по угрозам, введение необходимых контрмер и перерасчет риска системы, а также определение коэффициента риска после внедрения контрмер. Так же найдено практическое применение разработанного алгоритма – аутентификация пользователей АРМ ИТКС, защита от НСД. Предложенный алгоритм с принятием решения по критерию Неймана-Пирсона повышает результативность аутентификации пользователей на АРМ ИТКС за счет введения нескольких факторов аутентификации, что уменьшает вероятность ошибки 2 рода (пропуск события) за счет фиксации вероятности ошибки 1 рода (ложная тревога).

Список используемых источников

1. Цыбулин А. М. Подход к построению автоматизированной системы управления информационной безопасностью предприятия // Вестник Волги. Технические инновации. 2011. № 5. С. 86–89.

2. Багров Е. В. Мониторинг и аудит информационной безопасности на предприятии // Вестник Волгу. Технические инновации. 2011. № 5. С. 54–56.

3. Комаров А. Современные методы аутентификации: Токен и это все о нем..! // T-Comm — Телекоммуникации и Транспорт. 2008. № 6. С. 13–16.

4. Бардаев С. Э. Многофакторная биометрическая пороговая криптосистема. Известия ЮФУ. Технические науки. 2010. № 11. С. 148–155.

5. Схемы разделения секрета. Пороговая криптография [Электронный ресурс]. URL: http://cryptowiki.net/index.php?title=Схемы_разделе-ния_секрета._ Пороговая_ криптография

6. Трехуровненвая иерархическая модель компании Cisco [Электронный ресурс]. URL: http://www.network.xsp.ru/8_5_7.php.

7. Биометрическая аутентификация пользователя [Электронный ресурс]. URL: https://studref.com/322474/informatika/biometricheskaya_autentifikatsiya_polzovatelya.

8. Shamir A. How to share a secret // Commun. ACM — New York City: ACM, 1979. Vol. 22, Iss. 11. P. 612–613. ISSN 0001-0782. doi:10.1145/359168.359176.

9. Практически оптимальные схемы разделения секрета [Электронный ресурс]: URL: https://ru.bmstu.wiki/.

10. Липатников В. А., Шевченко А. А. Модель системы защиты информации распределенной информационной сети на основе контроля за уязвимостями // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2018. Т. 1. С. 569–574.

11. Липатников В. А., Тихонов В. А., Шевченко А. А. Метод управления кибернетической безопасностью в системах критических инфраструктур, основывающийся на

интеллектуальных сервисах защиты информации // Технологии построения когнитивных транспортных систем. Материалы всероссийской научно-практической конференции с международным участием. 2019. С. 207–214.

УДК 004.738.52
ГРНТИ 19.31

CPA-КАНАЛ, КАК МЕТОД ЭФФЕКТИВНОГО ПРИВЛЕЧЕНИЯ ЦЕЛЕВОГО ТРАФИКА

М. А. Калегин, Т. В. Мусаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

CPA-модель – это модель оплаты интернет-рекламы, при которой оплачиваются только определённые (целевые) действия пользователей на сайте рекламодателя. Действием может выступать прямая покупка товара, регистрация, подписка на рассылку, просмотр продвигаемого видеоролика, загрузка файлов, пополнение баланса, установка приложения, заполнение формы обратной связи и так далее

CPA, лид, партнерская сеть, реклама, веб-мастер.

С развитием интернета у маркетологов появилась возможность использовать принципиально новые маркетинговые модели по привлечению клиентов на сайт.

На сегодняшний день таких моделей множество. Каждая из них имеет свой набор функциональных критериев, которые ее отличают от других аналогичных систем. Имеющиеся недостатки влекут за собой ряд проблем. Поэтому, анализ и поиск наиболее актуальной, эффективной, стабильной модели является важной задачей.

Для выявления наиболее значимых критериев и недостатков были исследованы такие модели как: SEO, SMM, CPA-модель, CPC-модель, CPL-модель, Крауд-маркетинг, Cost Per Action (CPA-модель). Данный анализ позволил осуществить выборку из рассмотренного списка наиболее перспективной модели Cost Per Action (CPA-модель), на примере которой проанализированы и выявлены все существующие проблемы и достоинства.

CPA-модель – это модель оплаты интернет-рекламы, при которой оплачиваются только определённые (целевые) действия пользователей на сайте рекламодателя. Действием может выступать прямая покупка товара, реги-

страция, подписка на рассылку, просмотр продвигаемого видеоролика, загрузка файлов, пополнение баланса, установка приложения, заполнение формы обратной связи и так далее.

Участниками данной модели данной модели являются такие сущности, как:

1. Компания (рекламодатель). Получает целевой (конвертируемый в реальных клиентов) трафик.

2. Партнёр (вебмастер). Вебмастер – это закрепленное условное название человека, привлекающего трафик (пользователей) на сайт рекламодателя. Источником трафика чаще всего выступают принадлежащие вебмастеру веб-сайты и приложения.

3. Пользователь (посетитель, потенциальный клиент). Посещает сайт компании через уникальную ссылку вебмастера, выполняет необходимые действия, за что и производится оплата.

4. CPA-сеть. Контролирует соблюдение правил партнёром и компанией, является неким «доверительным звеном», за что получает свой процент [1]. CPA-сети являются агрегаторами автоматизирующими большую часть работы по CPA-каналу.

Хотя сущности Компания и Пользователь являются классическими резидентами и для других моделей интернет-маркетинга, Веб-мастер и CPA-сеть являются уникальными сущностями.

Переходы с площадки Веб-мастера на площадку Компании осуществляется через ссылки **(**точки захвата внимания [2]). Форматы ссылок для Вебмастеров устанавливаются CPA-сетью и различаются от сети к сети, но обобщенный их список выглядит так:

– текстовые блоки – обычные ссылки в теле статьи;

– баннеры – кликабельные цепляющие изображения;

– тизерные блоки – интригующее изображение плюс цепляющий текст;

– гиперконтекст – ссылка, при наведении на которую выводится реклама;

– реклама в видео – ролик перед основным видео, ссылка в его описании;

– реклама в изображениях;

– брендирование фона – кликабельный фон сайта, оформленный в стиле рекламируемого продукта (рис.);

– pop-up – всплывающее окно;

– робот консультант.

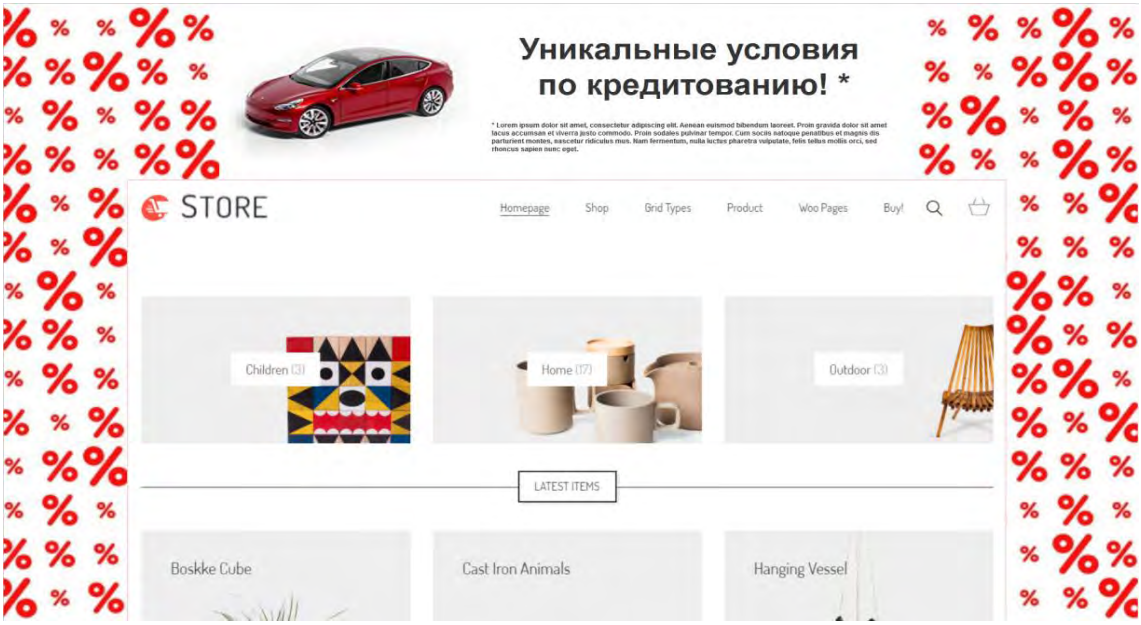


Рис. Пример модели сайта, где используется CPA реклама с брендированным фоном

При переходе Пользователем на сайт Компании через CPA-ссылку в его Cookie (системное хранилище браузера) записывается уникальный идентификатор приведшего его Вебмастера. Если пользователь после этого совершит целевое действие на сайте Компании, то этот Вебмастер получит вознаграждение.

Вместе с идентификатором в Cookie записываются и другие данные из ссылки необходимые для аналитики. Стандартным набором данных являются:

– utm_source [3] – уникальный идентификатор Вебмастера;

– utm_medium – тип рекламы (например, CPA, контекст, социальные сети и др);

– utm_campaign – название рекламной компании (например, компания продвижение нового продукта, компания поддержки и др.);

– utm_content – дополнительная информация, которую можно отслеживать, если совпадают другие параметры;

– utm_term – ключевое слово, с которого начался показ объявления (например, билеты, театр, рыбалка и др.).

Другие данные могут входить в набор по требованию Компании, или CPA-сети.

В результате исследования CPA-модели были выявлены следующие проблемы:

- Необходимость для CPA-сети постоянного контроля входящего трафика на предмет подтасовки результатов и мошенничества (ФРОДа).
- Сложность входа для малых рекламодателей – сетям интересны только те партнёры, которые готовы платить долго, много и стабильно (идеальный партнёр – банк, авиакомпания).

• Могут возникнуть проблемы в случае, если рекламодатель пытается продвинуть товар со сложным коммерческим предложением, или новой для рынка услугой. Рекламное предложение может быть неверно истолковано Веб-мастером и неверно размещено (например, не в той категории услуг).

• Необходимость конкурировать с другими рекламодателями за веб-мастеров – повышать размеры и длительность выплат.

Но также были выявлены и преимущества по сравнению с другими аналогичными моделями, которые были рассмотрены при выборке. К ним относятся:

– фиксированные расходы на интернет-маркетинг: стоимость целевого действия заранее чётко определяется, что сильно упрощает планирование;

– размещение на тематических площадках без необходимости договариваться, рассылать баннеры и платить каждому владельцу в отдельности;

– в высококонкурентых тематиках (банки, техника, авто и т. р.) цена конверсии по CPA может быть ниже, чем при работе с другими моделями, например, с контекстной рекламой, или SEO-оптимизацией;

– вся работа по обслуживанию ложится на CPA-сеть, от рекламодателя требуется только стартовая настройка.

Применение CPA-модели позволяет всем сторонам процесса сконцентрироваться на решении поставленных задач:

– веб-мастерам поставлять качественный трафик;

– рекламным сетям – находить качественных веб-мастеров и приводить их трафик на сайт рекламодателя;

– рекламодатель может сосредоточиться на повышении эффективности и качестве своих бизнес-процессов, не задумываясь о конверсии, трафике и т. д. [4].

Таким образом, можно подвести итог, что использование данной модели маркетинга актуально для любых сайтов, при любом бюджете и объеме персонала. Но наибольшую эффективность CPA-модель будет показывать для продающих сайтов с понятным для Пользователя и Веб-мастера коммерческим предложением.

Список используемых источников

1. CPA-агрегаторы [Электронный ресурс] // ООО «Оптимизм.ру». URL: https://www.optimism.ru/wiki/CPA-агрегаторы/ (дата обращения: 20.12.2019).

2. CPA-сети для начинающих [Электронный ресурс] // Пузат.Ру. URL: https://puzat.ru/knowledge/cpa-seti-dlya-nachinayushhix (дата обращения: 20.12.2019).

3. Генератор UTM-меток [Электронный ресурс] // Tilda Publishing. URL: https://tilda.cc/ru/utm/ (дата обращения: 20.12.2019).

4. Романенков А., CityAds Как работает CPA-модель в рекламных сетях [Электронный ресурс]. URL: https://www.cossa.ru/trends/147949/ (дата обращения: 20.12.2019).

УДК 004.056
ГРНТИ 81.96

РАЗРАБОТКА АЛГОРИТМА ПРИНЯТИЯ РЕШЕНИЙ ЭКСПЕРТНОЙ СИСТЕМЫ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Н. В. Киреева, И. С. Поздняк, Н. В. Филиппов

Поволжский государственный университет телекоммуникаций и информатики

В современном мире экспертные системы применяют для решения различных задач. В частности, вопросы аудита информационной безопасности автоматизированной системы также возможно рассмотреть с помощью экспертных систем. В статье предлагается один из вариантов алгоритма принятия решений экспертной системы оценки информационной безопасности для борьбы против современных информационных угроз, направленных на критически важные информационные объекты промышленных систем и цифровых производств.

экспертная система, отраслевая составляющая, стандарты, риски, информационная безопасность, принятие решений.

Важным направлением в мире в настоящее время является повышение надежности защиты всех типов информации, циркулирующей в корпоративных сетях различного уровня. Промышленные системы и цифровые производства, которые являются непосредственными составляющими цифровой трансформации на российском и международных рынках, нуждаются в надежной реализации проектов по обеспечению информационной безопасности (ИБ) информационных систем.

Главные задачи, которые при этом ставятся перед специалистами в области ИБ, являются:

– соблюдение организационно-правового обеспечения, согласно указаниям органам государственного регулирования;

– обеспечение основных составляющих информационной безопасности: конфиденциальности, целостности, доступности;

– минимизация ущерба (финансовые потери, падение репутации), в случае реализации возможных угроз.

Далеко не все предприятия могут позволить себе содержать штат специалистов, которые должным образом следят за соблюдением требований информационной безопасности. Несмотря на это, организации хотят избежать инцидентов, приводящих к значительному ущербу. Тогда они должны понимать, что необходимым условием является обеспечение комплексной системы защиты информации.

При этом стоит помнить, что ни одна существующая информационная система не является на сто процентов защищенной, так как невозможно предусмотреть и обнаружить все уязвимости. Кроме того, существуют уязвимости нулевого дня. Для того, чтобы помочь найти возможные угрозы и уязвимости в системе, дополнительно проводят тесты на проникновение.

При разработке системы безопасности необходимо учитывать финансовую сторону используемых действий, которая, также как и принимаемые меры, должна сопоставляться с ценностью защищаемой системой информации и быть максимально эффективной.

Система объективно-комплексного подхода характеризуется различными механизмами, которые включают создание конкретных защитных алгоритмов и регулярные непрерывные процессы аудита, которые в большинстве своем основаны на экспертных системах (ЭС). Они являются наиболее типичной реализацией искусственного интеллекта, используемой в различных отраслях экономики для оценки рисков информационных систем.

Описание процесса наполнения базы знаний экспертной системы в области информационной безопасности представлено в [1]. В данной работе речь пойдет об одном из следующих этапов – разработке алгоритма принятия решений в ЭС.

При создании экспертной системы оценки уровня информационной безопасности очень важным является правильно принятое решение о необходимости применения тех или иных мер, направленных на улучшение системы защиты и снижение рисков предприятия. Разработка алгоритма принятия решений экспертной системы будет способствовать объективной оценке и эффективному исследованию используемой системы безопасности. Рассматривая информационную систему предприятия с точки зрения своевременности, точности, полноты и достоверности оценки данной системы, которая является результатом действия разработанного алгоритма принятия решения ЭС анализа информационной безопасности, можно сказать, что она осуществляет:

– выявление уязвимых мест системы;
– оценивает основные параметры предложенной безопасной системы;
– выявление недооцененных рисков;
– принятие корректирующих мер, направленных на усовершенствование процедур обеспечения безопасности информации;
– определение алгоритма последующих событий, который позволяет добиться более высокого уровня системной безопасности предприятия.

Для того, чтобы методы и алгоритмы принятия решений были успешно реализованы, необходимо правильно и четко поставить задачу. Для успешной реализации этого этапа необходимо ясно представлять преимущества, недостатки и специфику различных методов. Для начала, необходимо установить конкретные границы экспертной системы, в рамках которой будем

применять предлагаемые методы. Далее, в рамках этой ограниченной системы или ее части (в случае применения декомпозиции) следует определить показатель эффективности, по которому будем определять наилучшее или наихудшее решение. Обычно это показатели экономического (ущерб) или технологического (производительность) характера. Следующим шагом является построение модели, описывающей взаимодействие переменных (определяемых заранее) параметров и показателей эффективности.

После успешной и четкой постановки задачи можно приступать к пошаговой разработке алгоритма процедуры принятия решений. Один из вариантов такого алгоритма для ЭС представлен в [2], который основан на теории статистических гипотез. Обращение к базе знаний экспертной системы происходит на третьем шаге при определении решающего факта. В нашем случае рассматриваются вопросы, основанные на стандартах ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»; ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» и ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». После выбора необходимого вопроса и формирования на его основе запроса пользователю, система вызывает соответствующий фрейм для ответа пользователя. Чтобы выбрать более подходящий алгоритм принятия решения, пользователь должен ответить на вопросы (как рассмотрено выше), которые представляются как взаимосвязанные вопросы с различными вариантами на каждый из них. Такая взаимосвязь, также как и избранный ответ, позволяет системе удалить из полного перечня всех алгоритмов те, которые не удовлетворяют данным ответам. Это приводит к тому, что в системе остается единственно возможный алгоритм принятия решения, который производит оценку используемой системы безопасности и защиты предприятия.

В качестве альтернативного подхода к выбору алгоритма принятия решения представляется использование выбора алгоритма в так называемом явном виде. Это возможно тогда, когда пользователю точно известен алгоритм оценки рисков предприятия.

После интерпретации ответа пользователя следует уточнение и гипотеза. Такой алгоритм позволяет подробно проработать решения при грамотно поставленных задачах.

При этом необходимые исходные данные пользователь может, как задать самостоятельно вручную, так и скопировать из тех документов, которые были приготовлены заранее.

Особый интерес представляют выходные данные, формирующиеся в образе отчета, что является особенностью описания комплексной итоговой оценки безопасности системы. Данный отчет будет содержать результирующую оценку информационной безопасности системы, для формирования которой использовались различные математические методы. Кроме того, данная оценка содержит материал в виде рекомендаций, который предполагает уменьшение уязвимостей и снижение различных возможных рисков предприятия. Также, необходимо добавить, что важным моментом является характеристика эффективности применения рассматриваемой системы защиты предприятия, которая может быть определена экспертной системой с помощью модуля аналитической отчетности.

Определение и обоснование альтернативных вариантов, зависящих от конкретных задач и реализующихся компонентов системы, возможно при наличии разработанной самостоятельно или готовой базы знаний, которая включает один или несколько наборов правил выбора определенных моделей и соответствующих алгоритмов принятия решений.

Руководство крупных предприятий нуждается в точной информации о состоянии своей системы информационной безопасности, а также в оптимальных решениях, направленных на ее улучшение. Это определяет качественное управление предприятием, характеризует способность эффективного планирования его деятельности и выживаемость в современных условиях жесткой и непримиримой конкуренции. При этом в качестве определяющего значения выступает четкость формы представления информации, быстрота получения различных структурных видов отчетов, а также возможность обзорной оценки действующих и ранее полученных данных. Разрабатываемый алгоритм принятия решений экспертной системы оценки информационной безопасности сможет предоставить руководителям предприятий такие возможности.

Список используемых источников

1. Kireeva N., Pozdnyak I., Gagigulina A. Filling a knowledge base for expert system in information security [Электронный ресурс] // «TechSys 2019»: Materials of 8th International Scientific Conference–Engineering, Technologies And Systems Technical University of Sofia, Plovdiv Branch, 16-18 May 2019. IOP Conf. Series: Materials Science and Engineering 618 (2019) 012085. URL: https://iopscience.iop.org/article/10.1088/1757-899X/618/1/012085 (дата обращения: 21.01.2020).

2. Волков А. Л. Алгоритм принятия решения в Expert V 2.0 [Электронный ресурс]. URL: http://it-claim.ru/Library/Books/ITS/wwwbook/ist4b/its4/volkov.htm (дата обращения: 21.01.2020).

УДК 004.6
ГРНТИ 20.53.19

КОНТЕЙНЕРИЗАЦИЯ ДЛЯ АНАЛИЗА БОЛЬШИХ ДАННЫХ НА ПРИМЕРЕ KUBERNETES И DOCKER

Д. А. Козинцев, А. А. Шиян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С каждым днем объемы обрабатываемой информации растут в геометрической прогрессии. В связи с этим, востребовано увеличение ресурсов, задействованных в вычислениях, данное действие ограничено, поскольку всегда есть какой-то предел в возможностях. В связи с этим необходимо увеличивать эффективность утилизации имеющихся ресурсов. Для этих целей были созданы средства виртуализации и кластеризации.

виртуализация, контейнеризация, Data Lake, ETL, распределенные системы, BigData.

С этой задачей отлично справляются инструменты обработки данных, базирующиеся в многочисленных ЦОДах и собственных серверных ресурсах компаний. Однако, после обработки, данные не удобны для анализа человеку, в связи с этим производится их визуализация. С помощью нее происходит аналитика, для принятия управленческих решений, развития компании и увеличении прибыли.

Сложность заключается в том, что трудно предоставить конечному пользователю необходимый объем уже подготовленных данных так, чтобы не возникало проблем в работе с ними. Но с помощью современных средств виртуализации можно создавать решения облегчающие подобные задачи.

Подход заключается в разработке архитектуры, позволяющей пользователю производить анализ данных независимо от их объема, поскольку большой объем данных снижает производительность конечных приложений. Для создания подобной архитектуры потребуется задействовать средства, позволяющие «упаковать» необходимое приложение со всем его окружением и зависимостями в контейнер, который можно перенести в любую Linux систему. Этим средством является «Docker».

Помимо этого, «Docker» упрощает процессы развертывания и управления в средах с поддержкой контейнеризации [4]. А для верхнеуровневого контроля над подобной структурой необходимо задействовать технологию «Kubernetes», которая создана для управления целым кластером контейнеров Linux как единой системой [3].

В совокупности, использование данных средств, позволяет упростить процессы масштабирования и управления распределенными системами. Основная проблема существующих систем извлечения, преобразования и загрузки (от англ. *Extract, Transform, Load,* далее – ETL системы) заключается в том, что они не могут использовать многопоточность, что существенно увеличивает время обработки информации. Эта проблема решается использованием технологии контейнеризации. При нераспределенной работе системы ETL процессы выполняются последовательно (рис. 1).

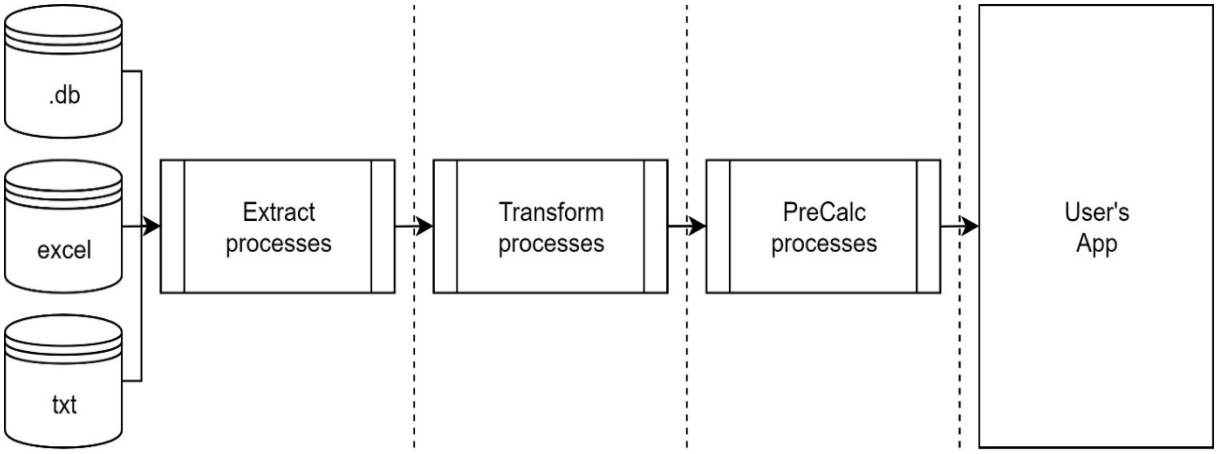


Рис. 1. Пример поэтапной работы системы ETL

Использование «Docker» и «Kubernetes» позволяет запускать такие процессы параллельно, что существенно ускоряет ETL процессы. Ниже на рис. 2 представлен более эффективный вариант ETL системы.

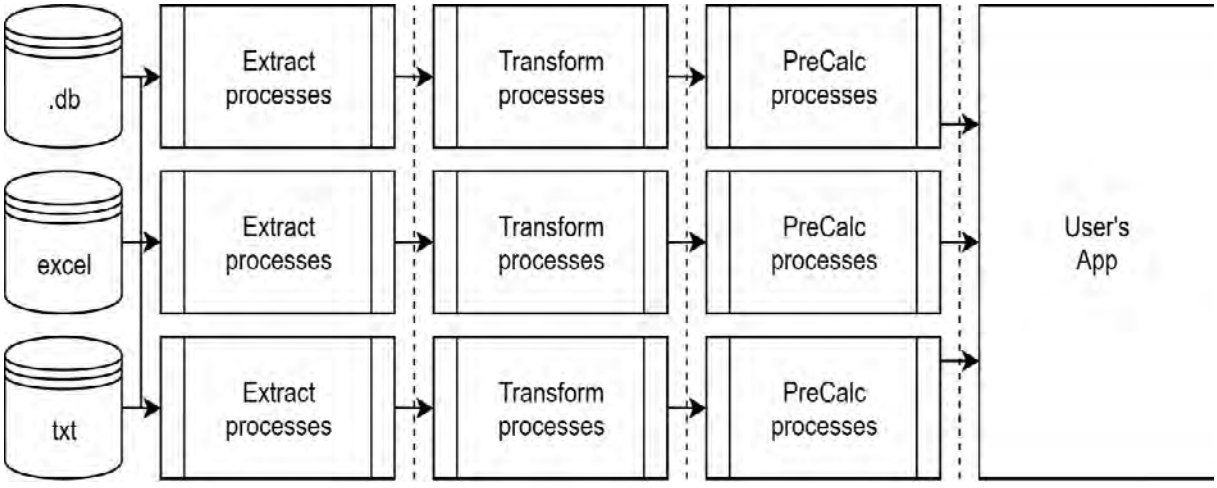


Рис. 2. Многопоточная ETL система

На рис. 3 представлена архитектура целевой системы.

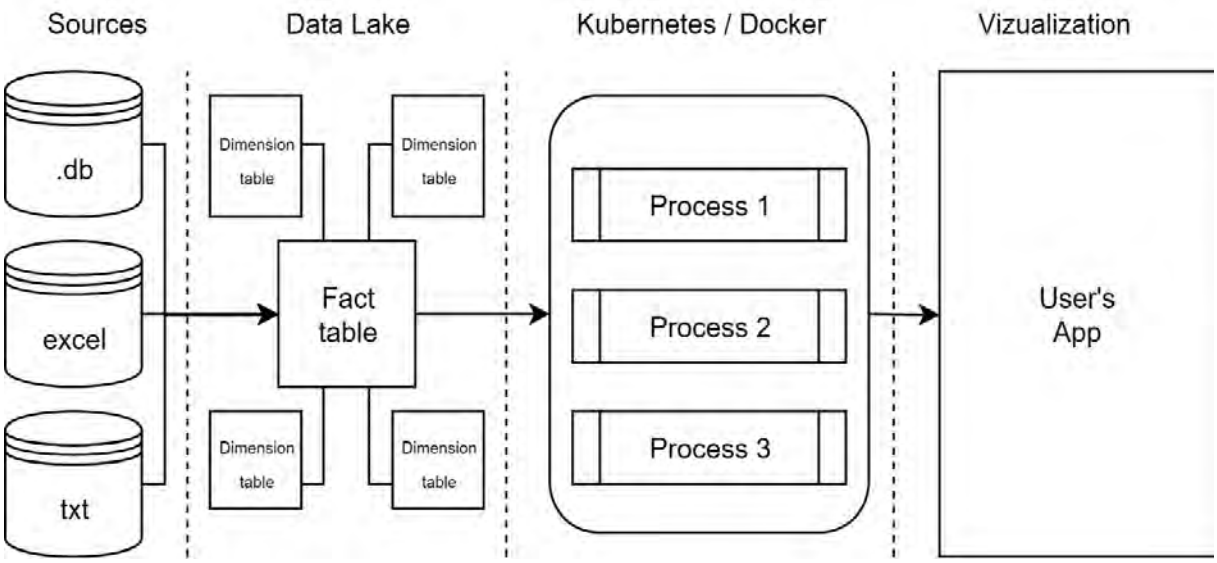


Рис. 3. Пример целевой архитектуры системы

В результате получаем следующую архитектуру системы:

– источники данных;
– проиндексированная модель данных;
– слой обработки данных;
– конечное приложение.

Данная архитектура основывается на следующем принципе работы:

– выгрузка данных из источников в «Data Lake» («Озеро Данных») и их индексация в модели данных «звезда»;
– многопоточная обработка данных в контейнерах;
– загрузка данных в конечное приложение и их визуализация.

За счет использования технологий контейнеризации, такая система может быть развернута с любым набором необходимых технологий, согласно потребностям. Помимо всего прочего, данная система, при необходимости, может автоматически масштабироваться, в зависимости от различных показателей [1]. Автомасштабирование позволяет автоматически увеличивать и уменьшать рабочие нагрузки в зависимости от использования ресурсов. Работает оно следующим образом: периодически, внутри системы происходит сбор информации о загрузке основных показателей, таких как использование центрального процессора (ЦП) и памяти, а также специфических показателей, задаваемых разработчиком.

На наш взгляд, подобная конфигурация системы позволит пользователю проводить анализ данных задаваясь не только частными вопросами, но и более общими визуализируя отношения, позволяющие глубже понимать и анализировать данные. Помимо выгод для конечного пользователя, появляется и ряд преимуществ для поддержки такой системы.

– автоматическая балансировка нагрузки с помощью постоянного мониторинга сведений о производительности и использовании ресурсов [2];

– наличие средств изоляции приложений, с целью предоставления запущенным приложениям и командам минимально необходимого набора привилегий для использования ресурсов;

– отказоустойчивость [7].

Однако не обошлось и без минусов. Основными минусами такой системы являются:

– усложнение инфраструктуры;

– время реализации;

– стоимость решения и поддержки.

Следует уточнить, что для небольших проектов не стоит использовать подобную архитектуру, поскольку она рассчитана на гораздо больший объем обработки данных.

Список используемых источников

1. Горизонтальное автомасштабирование подов Kubernetes и Prometheus для высокой доступности и работоспособности инфрастр-ры [Электронный ресурс]. URL: https://habr.com/ru/company/otus/blog/457742/ (дата обращения: 25.12.2019).

2. Развертывание и масштабирование микросервисов Kubernetes [Электронный ресурс]. URL: https://www.8host.com/blog/razvertyvanie-i-masshtabirovanie-mikroservisov-kubernetes/ (дата обращения: 25.12.2019)

3. What is Kubernetes? [Электронный ресурс]. URL: https://www.redhat.com/en/topics/containers/what-is-kubernetes (дата обращения: 25.12.2019).

4. Что такое Docker? [Электронный ресурс]. URL: https://docs.microsoft.com/ru-ru/dotnet/architecture/microservices/container-docker-introduction/docker-defined (дата обращения: 25.12.2019)

5. Зачем и как использовать контейнеры: разбираемся с Docker, Kubernetes и другими инструментами [Электронный ресурс]. URL: https://tproger.ru/articles/containers-explained/ (дата обращения: 25.12.2019).

6. Kubernetes – система оркестрации контейнеров для масштабных проектов [Электронный ресурс]. URL: https://mcs.mail.ru/blog/kubernetes-for-much-stuff (дата обращения: 24.12.2019)

7. Масштабирование Docker с помощью Kubernetes [Электронный ресурс]. URL: http://rus-linux.net/MyLDP/vm/docker/scaling-docker-with-kubernetes.html (дата обращения: 23.12.2019).

УДК 621.372.8
ГРНТИ 84.01.85

АДАПТАЦИЯ СИСТЕМЫ МОНИТОРИНГА РАСПРЕДЕЛЕННЫХ ОБЪЕКТОВ С ЦЕЛЬЮ ПОВЫШЕНИЯ УРОВНЯ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Л. П. Козлова, И. С. Кучеренко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

С появлением новых интеллектуальных технологий обработки и анализа поступающей информации с объектов мониторинга открываются новые возможности в сфере обеспечения безопасности распределённых объектов предприятий. В статье рассмотрена оптимизация типовой архитектуры информационной системы мониторинга, обеспечивающей всесторонний контроль и оперативное реагирование в случае нештатных ситуаций.

информационная система, мониторинг, распределенные объекты, безопасность, архитектура.

Распределенные инфокоммуникационные системы, ориентированные на обработку и анализ данных, и в дальнейшем принятия решений в различных областях знаний, характеризуются большим количеством инфраструктурных составляющих общего назначения (связь, инженерия, транспорт, энергетика и т. д.). Решение задач по созданию эффективных систем мониторинга объектов предприятий и обеспечения необходимого уровня безопасности распределенных подсистем, восстановления целостности и поддержания работоспособности в критических и аварийных ситуациях является актуальной задачей и все чаще встречается в концепциях и программах развития информационного общества и обеспечения безопасности на корпоративном (отраслевом), федеральном и региональном уровне.

Для обеспечения охраны социально значимых и стратегически важных объектов в России накоплен определенный опыт планирования, реализации и эксплуатации систем безопасности объектов предприятий и ситуационных центров. Расширение сфер взаимодействия предприятий с внешним окружением, прогресс информационно-коммуникационных технологий выдвигает новые требования к архитектуре и интеграции подсистем безопасности, обеспечению их взаимодействия с технической семантической и организационной точки зрения, развитию правового и научно-методического

обеспечения, разработок распределенных интеллектуальных систем мониторинга и обеспечения безопасности объектов предприятий.

Анализ накопленного опыта проектирования и реализации систем безопасности на объектах с достаточно высокими порогами риска возникновения угроз показывает, что основные проблемы создания эффективных систем охраны связаны с первоначальной неопределенностью степени состояния внутренней и внешней среды, применением не соответствующих требованиям моделей оценки уязвимости объектов и вероятности возникновения рисков при реализации и эксплуатации проектов.

Адаптация и улучшение правового и организационно-методического обеспечения разработок информационных систем мониторинга требует совершенствования национальных стандартов в сфере информационных технологий, средств защиты информации и объектов, а также их гармонизации со стандартами в сфере строительства и всех этапов жизненного цикла технологических процессов предприятий, управления проектами, реализации и т.д. на национальном и международном уровнях. Помимо этого, необходимым этапом обеспечения работоспособности системы мониторинга распределенных объектов предприятия (СМРОП) является дополнение и расширение программ дополнительного образования для проверки знаний специалистов, обслуживающих комплекс входящих в систему безопасности, а также сертификация специалистов по контролю навыков на всех этапах жизненного цикла информационной системы.

Первоочередными стандартами, обобщающими опыт разработки и эксплуатации интегрированных систем безопасности и программ развития информационных технологий, являются ГОСТ Р 55062-2012 «Информационные технологии. Системы промышленной автоматизации и их интеграция. Интероперабельность» [1], ГОСТ Р 56875-2016 «Информационные технологии. Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий», и ГОСТ 31937-2011 «Здания и сооружения. Правила обследования и мониторинга технического состояния».

Для комплексного подхода к проектированию и последующей реализации интеллектуальной системы мониторинга с целью обеспечения интероперабельности используется методология открытых систем, учитывающая задачи стандартизации и унификации функциональных элементов, протоколов передачи и обмена данными, интерфейсов и системной архитектуры в целом.

К основным моделям, необходимым для проектирования интеллектуальной системы мониторинга, следует отнести: модели основных потоков передаваемых между подсистемами данных, сопутствующего документо-

оборота, описания вероятных рисков и угроз безопасности подсистем предприятия, модели деятельности ответственных служб и подразделений, модели оценки защиты и обеспечения целостности системы при вероятных воздействиях (внутренних и внешних), а также описания основных ресурсов, объектов, процессов, организации поддержки в актуальном состоянии баз данных, функциональные модели комплексов программного и аппаратного обеспечения и их технического сопровождения и обслуживания [2].

Первоочередной задачей при реализации функциональной модели системы контроля и мониторинга является уточнение и описание бизнес-модели предприятия, на следующем этапе – создание модели основных процессов системы мониторинга, предусматривающей в перспективе внедрение и эксплуатацию реструктуризированной системы при внутренних и внешних воздействиях, ее автоматизацию и своевременное применение новых технологий и проектов в существующих элементах комплекса безопасности предприятия. На полученной базе интеллектуальной системы строится многозадачный комплекс охраны распределенных объектов предприятия с возможностью проведения мониторинга различных показателей и контроля системы изменений, что в свою очередь способствует повышению эффективности и ускорению принятий управленческих решений.

В состав функциональных компонент входят программно-технические и программно-методические комплексы, приведенные в приложении Б ГОСТ Р 56875-2016 [3].

Стандартизация протоколов обмена данными, интерфейсов, типизация архитектуры и входящих элементов способствуют решению задач интеграции и функциональной совместимости предлагаемых типовых компонент, а также их проверке на совместимость и соответствие международным и национальным стандартам. Типовая схема системы мониторинга распределенных объектов предприятия представлена на рис.

Унифицированные интерфейсы программно-технических и методических комплексов средств информационно-коммуникационных технологий позволяют реализовать «персональную» СМРОП с учетом интересов и условий конкретной предметной области.

Базовые ПМК и ПТК при применении методологии открытых систем могут быть развернуты на различных информационно-коммуникационных платформах с использованием программных и аппаратных решений различных производителей.

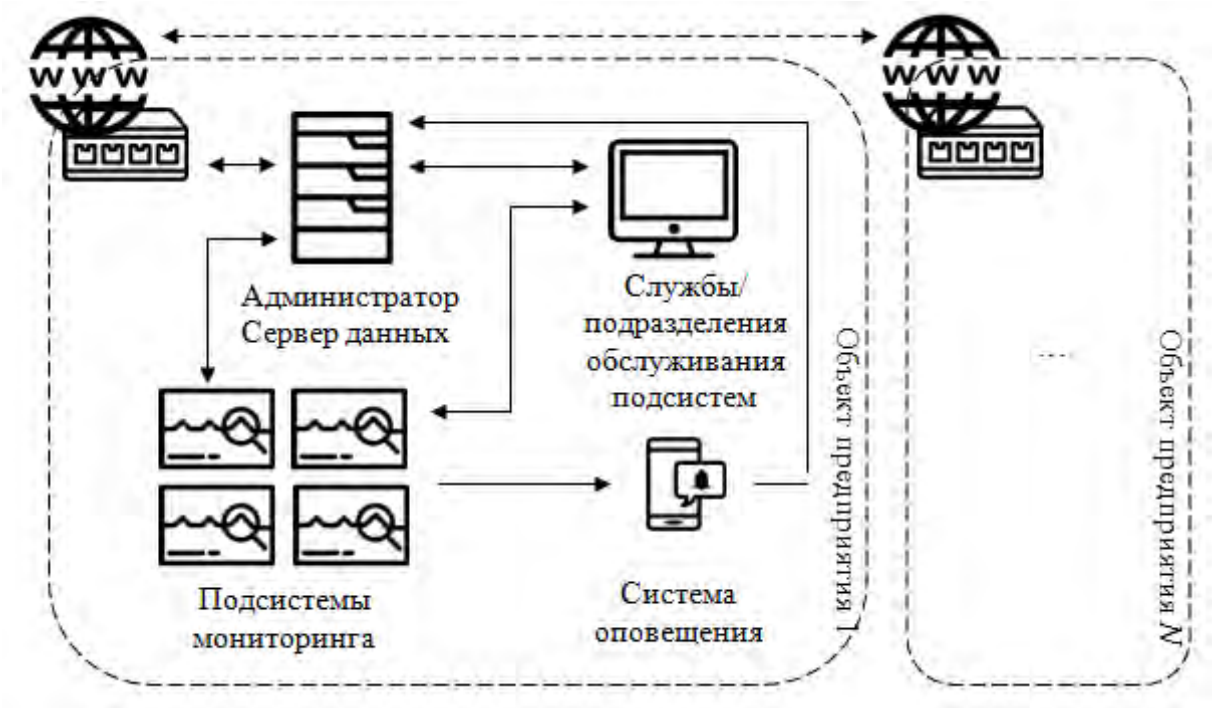


Рис. Типовая схема СМРОП

Заключение

Системы мониторинга распределенных объектов предприятия являются востребованными в решении задач использования сопровождения распределенных интеллектуальных информационных систем, к функционированию которых предъявляются повышенные требования к отказоустойчивости и надежности. Эффективность создания комплекса правового и организационно-методического обеспечения, регламентов, стандартов на типовые элементы и интерфейсы систем охраны и безопасности объектов предприятия зависит от того, что ущерб от несоблюдения требований стандартов и технических регламентов, несанкционированного доступа, внешних и внутренних воздействий, некорректно определенной степени рисков, несогласованности действий ответственных служб и подразделений безопасности влечет за собой огромные финансовые потери. Применение унифицированных платформ и базовых архитектур СМРОП и интеграции оборудования различных производителей с учетом разработки минимально необходимого комплекса стандартов предоставит возможность существенно уменьшить совокупные затраты на воплощение проектируемых СМРОП и их внедрение в предприятия различных предметных областей.

Список используемых источников

1. ГОСТ Р 55062-2012. Информационные технологии. Системы промышленной автоматизации и их интеграция. Интероперабельность. М. : Стандартинформ, 2012. 20 с.
2. Куделькин В. А., Денисов В. Ф. Опыт интеграции распределенных информационных систем // Электронный научный журнал ИТ-Стандарт. 2017. № 2. URL: http://journal.tc22.ru/wp-content/uploads/2018/02/opit_integracii_raspredelennih_informacionnih_sistem.pdf (дата обращения: 21.02.2020).
3. ГОСТ Р 56875-2016 Информационные технологии (ИТ). Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий. М. : Стандартинформ, 2016. 40 с.

УДК 651.011.42
ГРНТИ 84.01.85

СОВРЕМЕННЫЕ ПОДХОДЫ К РАЗВИТИЮ РАСПРЕДЕЛЁННЫХ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Л. П. Козлова, Р. З. Лаба

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время электронный документооборот является одним из ключевых элементов цифровизации в любой сфере деятельности, позволяющий ускорить процессы, связанные с движением и согласованием документов, и сделать их более прозрачными. В статье рассмотрены основные современные подходы к развитию систем электронного документооборота, в основе которых положены новые технологические тенденции, такие как повсеместная мобильная корпоративность, облачные модели и многое другое.

распределённая система, электронный документооборот, масштабирование, прослеживаемость, защита информации, приложение.

Введение

С быстрым развитием технологий и их повсеместным внедрением распределенные системы электронного документооборота (РСЭД) получили широкое развитие, успешное внедрение которых приводит к уменьшению расходов на фонд оплаты труда за счёт сокращения стоимости часа работы специалистов, трудозатрат специалистов, минимизацию расхождения в документах и уменьшению их дублирования, однократной фиксации докумен-

тов, уменьшению расходов на архивацию документов, за счет централизованного хранилища, а также за счет возможности автоматизированного использования удаленных документов с истекшим сроком хранения данных, и главное это структуризация бизнес-процесса организации.

Система управления электронным документооборотом служит основой и улучшением систем класса управления предприятием, систем управления продажами и других важных для современной организации информационных систем, поэтому от ее функционирования зависит работа всех информационных систем организации, а значит и работа всей организации [1].

На рис. представлена в обобщенном виде топология РСЭД.

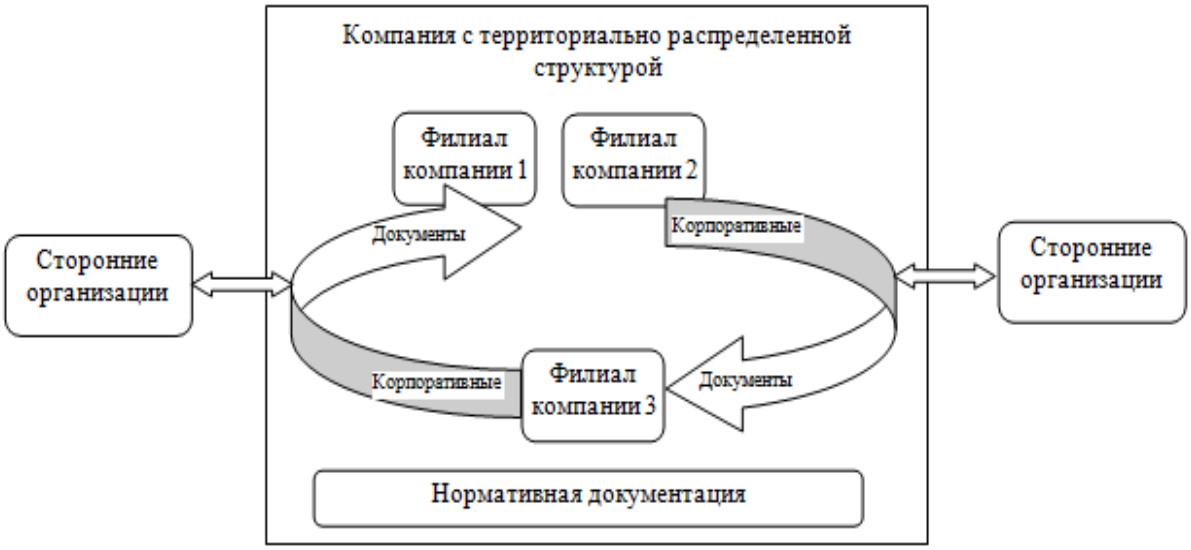


Рис. Схема РСЭД

Из обобщенной топологии РСЭД (рис.) видно, что филиалы компании могут располагаться не только на одной площадке, но и территориально разнесены, но при этом возможно: использование инфраструктуры общей компьютерной сети; использование единой базы данных; использование корпоративных документов, корпоративных справочников и бизнес-сервисов.

Основными характеристиками РСЭД являются маршрут движения, который включает все инстанции от создания первоначального документа до его подшивки в дело, и время, затрачиваемое на прохождение их по этому маршруту. Отсюда главное правило организации РСЭД это оперативное прохождение документа по наиболее короткому и прямому маршруту с наименьшими затратами времени.

В работе [2] формальная модель РСЭД (ДТ) представлена в виде функции на основе диаграммы Эйлера-Венна:

$$ДТ = \{\mathbf{У, Д, Ф}\},$$

где **У** – множество участников, определяемое как конечное множество ролей, назначаемых фактическими участниками РСЭД; **Д** – конечное множество действий, выполнение которых допустимо в пределах рассматриваемой системы РСЭД; **Ф** – конечное множество состояний документов, которые могут принимать документы после выполнения участником множества **У** действий из множества **Д**.

Взаимодействие элементов этих множеств и их связей полностью задает производственные сценарии, реализуемые РСЭД. На основе декомпозиции множеств строятся две составляющие формальной модели документооборота: логическая и функциональная.

Логическая модель определяет событийную составляющую системы документооборота, описывающая действия, происходящие в системе, и декларируемые моменты времени или условия событий, после которых эти действия будут выполнены.

Функциональная модель представляет собой описание системы на языке выполняемых ею функций. Это представление формальной модели позволяет описать и воспроизводить работу системы с точки зрения последовательности выполняемых действий и получаемых результатов, которые представлены состояниями документов, выстраиваемых в последовательность изменяемых состояний. Это позволяет представить документооборот в виде конечного автомата, который оперирует документами в виде алфавита и действиями участников [3].

Ключевой целью РСЭД является снижение транзакционных издержек при работе с документами посредством создания общего цифрового пространства для работников в рамках подготовки документов с использованием технологий совместной работы и инструментов интеллектуализации основных процессов взаимодействия и разработки документов.

При этом для участников процесса необходимо обеспечивать переход от рутинной работы с формулировками и текстами документов к работе с ключевыми решениями и смыслами.

Для качественного функционирования РСЭД необходимо реализовывать требования по защите информации от несанкционированного доступа (НСД) [4]:

– обеспечение исключения несанкционированного доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение защищаемых данных, а также иные несанкционированные действия;

– проведение мероприятий, направленных на предотвращение НСД (закрытие технических каналов, выбор средств защиты от НСД), которые должны быть определены на этапе технического проектирования;

– реализация своевременного обнаружения фактов НСД к защищаемой информации;

– реализация невозможности воздействия на технические средства автоматизированной обработки информации, в результате которого может быть нарушено их функционирование;

– обеспечение возможности незамедлительного восстановления информации, модифицированной или уничтоженной вследствие НСД.

Методы защиты информации и реализующие их технические решения не должны снижать функциональные возможности системы, вносить принципиальные ограничения по производительности и времени реакции РСЭД.

Современные РСЭД должны иметь модульную структуру, допускающую подключение дополнительных функциональных блоков без необходимости внесения серьезных изменений во внедренную и эксплуатируемую версию и включать набор инструментов для «быстрой» адаптации (без программирования, отключения пользователей и перезагрузки сервера для применения изменений) при настройке, в том числе:

– основных элементов системы без использования программирования: настройка карточек документов, справочников;

– обязательностей заполнения полей для различных типов карточек и различных переходов, подстановка значений полей по умолчанию;

– настройки и хранения шаблонов документов, карточек документов, резолюций, поручений, отчетов, списков рассылки, поисковых запросов и пр.

Современные РСЭД должны иметь полнофункциональный Веб-клиент для пользователей и администраторов Системы, а также мобильное рабочее место в виде отдельного приложения, машинный код которого исполняется в операционной системе мобильного устройства («нативное» приложение). Интерфейс приложения должен быть интуитивно понятным, детализация информации осуществляться по принципу от общего/основного к частному, от документа в списке до конкретного исполнителя.

Система должна предоставлять инструментарий для использования электронной подписи, хранения и использования сертификатов ключей.

Заключение

Эффективность работы организации в значительной степени зависит от качества управления бизнес-процессами и документооборотом. Внедрение РСЭД напрямую отражается на исполнении документов и дает преимущество перед другими организациями, повышая скорость работы, качество, при этом происходит ускорение движения информационных потоков, улучшается контроль всех делопроизводственных процессов, т. е. растет конкурентоспособность организации.

Список используемых источников

1. Филенко Е. Н. Развитие понятия «документ» с внедрением новых информационных технологий // Делопроизводство. 2006. № 3 С. 64–65.
2. Глушков В. М. Введение в АСУ. К.: Техніка, 1972. 312 с.
3. Круковский М. Ю. программный комплекс поддержки системы композитного документооборота на основе моделей процессов // Математичні машини і системи. 2006. № 1. С. 81–92.
4. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

УДК 004.7
ГРНТИ 20.53

BLOCKCHAIN – ВОЗМОЖНОСТЬ ПОСТРОЕНИЯ ДЕЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ ОБРАБОТКИ ДАННЫХ

О. А. Козлова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современные технологии не стоят на месте, и предложенная несколько лет назад концепция построения децентрализованной системы обработки данных набирает все большую популярность, находя свое применение в первую очередь в экономической сфере. В статье изложены принципы построения таких систем, их особенности, достоинства и недостатки.

Blockchain, децентрализованные системы, криптография.

Blockchain (в иных источниках блокчейн или блок-чейн) – технология позволяющая создавать децентрализованную систему обработки данных. Если переводить дословно, то название делится на две часть block – блок и chain – цепочка. В сущности, эти два слова исчерпывающе объясняют, что эта технология представляет собой, а именно последовательность соединенных между собой элементов, содержащих в себе данные.

Что же такое технология блокчейн? Как уже говорилось выше, структура системы представляет собой набор записей, объединенных в блоки. Структура блока представлена на рис.

В свою очередь, блоки объединены между собой в цепочку, которая, во-первых, соблюдает строгий хронологический порядок, а, во-вторых, каждый блок фиксирует адрес предыдущего. Ни один блок не подключен к объединяющему серверу, что делает технологию децентрализованной. Т. е. чтобы воспользоваться данными, вся цепочка должна быть продублирована на всех использующих ее базовых станциях.

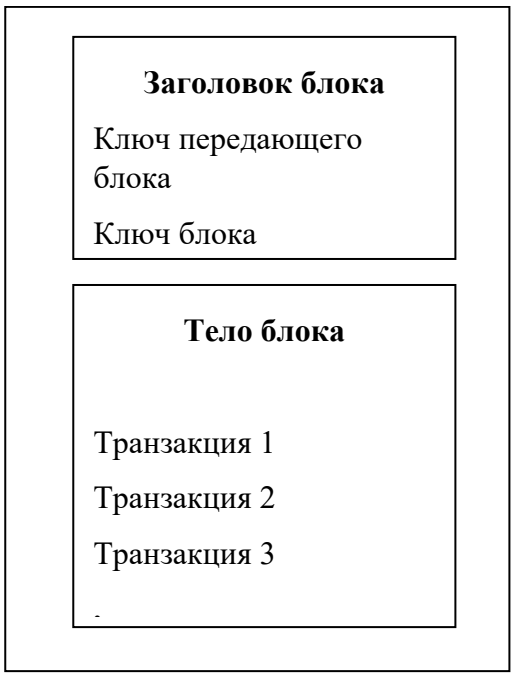


Рис. Структура блока

Соединяются блоки благодаря криптографической подписи, которая отвечает в первую очередь за защиту информации от несанкционированного изменения, а значит, за защиту данных. Для этого в системе редактирования выделяются следующие элементы:

1. Криптографические ключи. Информация о ключе может быть известна как одному человеку, так и всем пользователям системы. Не существует двух одинаковых ключей. По своей структуре ключ представляет собой случайную последовательность.

2. Конфиденциальность. Для ее достижения используются алгоритмы взаимной аутентификации, симметричное и асимметричное шифрование, цифровые подписи, т. п.

3. Аутентификация. Соединяет только тех пользователей, которые допущены в систему. Требует подтверждения прав.

4. Целостность данных. Для сохранения имеющейся информации применяется шифрование данных.

5. Подлинность данных – подтверждается путем использования цифровой подписи.

Для того, чтобы понять смысл криптографической подписи для системы блокчейн, стоит выделить понятие хэш-функции.

Она необходима для переработки информации в цифровые или буквенные выражения, которые и являются хэшем. Причем длина такой строки ограничена. Каждый следующий блок ссылается на хэш предыдущего, что обеспечивает защиту информации в самом «тонком» месте системы – добавлении новых блоков [1].

Архитектура любой системы предполагает расширение ее данных. Блокчейн не исключение. Каждый новый блок, как показано на рис., включает в себя хронологически упорядоченные записи о проводившихся в системе операциях – транзакциях. Как только блок полностью сформирован,

его должны одобрить все участники сети. В противном случае, блок будет отклонен. После добавления нового элемента база обновляется у всех участников. Такова исходная концепция. Однако существует различие для публичных и приватных систем.

Публичные системы предполагают добавление любого желающего. При добавлении нового блока они действуют по алгоритму, изложенному выше.

Приватные системы имеют серьезное отличие. Для того чтобы попасть в такие системы, требуется одобрение, основанное на прохождение определенного алгоритма, которое дают организаторы блокчейна. Также добавлять новые блоки могут только организаторы [2].

К достоинствам системы, построенной по технологии блокчейн можно отнести:

- Открытость данных при высокой степени безопасности. Последнее осуществляется благодаря методам шифрования.
- Живучесть системы. Благодаря особенностям архитектуры, система существует до тех пор, пока существует хотя бы одна станция, допущенная до информации. Отсюда вывод из строя одной, или даже большей части станций, фактически, не нанесут вред сети.
- Отсутствие посредников при обмене информацией.
- Невозможность односторонней замены или подмены данных, что обеспечивает их достоверность.
- Полная идентичность данных у всех участников сети, а, соответственно, одинаковая информативность.
- Возможность соблюдать анонимность при выполнении операции в сети.

Разумеется, помимо достоинств существуют и недостатки:

- Объем данных, хранящихся на станциях пользователей, растет с добавлением каждого нового блока. Однако количество действий за отрезок времени сильно ограничено. Отсюда вытекают сложности с масштабируемостью системы.
- Большое количество потребляемой энергии при использовании вычислений в сети.
- Утверждение о том, что блокчейн-сеть полностью безопасна абсолютно неверно. Опасность появляется, если некая группа накопит 51 % вычислительной мощности [3].

Между объявлением о технологии и первой функциональной ее реализацией прошло сравнительно немного времени – чуть меньше года, а именно, 2008 год – создание, 2009 год – воспроизведение. Первое применение блокчейн-сеть нашла в экономической сфере – она легла в основание ныне широко известной концепции криптовалют. В последствие сфера применения расширилась. Благодаря особенностям архитектуры такие системы

могут быть применены для создания умных городов, разработки над которыми уже ведутся, проведения финансовых сделок, различные социальные сферы. Архитектура также пригодилась для приложений государственного управления.

На сегодняшний день все еще хватает сложностей в работе с системами, построенными по принципу блокчейн, но учитывая очевидный набор достоинств распространение их в ближайшее время не вызывает сомнения.

Список используемых источников

1. Бауэр В. П., Сильвестров С. Н., Барышников П. Ю. Блокчейн как основа формирования дополненной реальности в цифровой экономике // Информационное общество. 2017. № 3. С. 30–40.

2. Поляков И. А. Блокчейн и инфраструктура // Рынок ценных бумаг. 2017. № 4. С. 24–25.

3. Смирнов Ф. А. Трансформация мировой финансовой системы: блокчейн, «умные контракты» и внебиржевые деривативы // Аудитор. 2017. № 6. С. 49–54.

Статья представлена заведующим кафедрой ИУС СПбГУТ, доктором технических наук, профессором Л. К. Птицыной

УДК 004.056
ГРНТИ 81.96

ВЫЯВЛЕНИЕ ПРОГРАММНЫХ ЗАКЛАДОК В ПРИЛОЖЕНИЯХ СРЕДСТВАМИ ДИНАМИЧЕСКОЙ БИНАРНОЙ ИНСТРУМЕНТАЦИИ

А. А. Колесников, А. В. Ушаков

Академия ФСО России

В данной статье описан способ реализации динамического анализа с помощью технологии динамической бинарной инструментации. Основным средством, рассматриваемым в работе, является DynamoRIO. Описан процесс инструментации, использующийся в данном средстве. Целью данной работы является повышение безопасности приложений путём выявления в них программных закладок.

динамический анализ, динамическая бинарная инструментация, фаззинг, базовый блок.

На сегодняшний день, безопасность программного обеспечения становится одной из важнейших проблем. Связано это с тем, что человечество использует огромное количество отраслей, связанных с использованием

программного обеспечения. Более того, увеличивается и сложность самих программных продуктов. Одной из важнейших проблем является то, что некоторые недобросовестные разработчики преднамеренно встраивают в свой продукт программные закладки, тем самым имея возможность использования недекларированных возможностей. Традиционно использовались два вида анализа программного обеспечения: статический и динамический. Статический анализ используется в том случае, если известен исходный код приложения. Однако, современные приложения собираются и определяются во время своего выполнения, используя разделяемые библиотеки, виртуальные функции, динамически генерируемый код и прочие динамические механизмы. Именно с этим связано развитие динамического анализа. Динамический анализ – анализ, который осуществляется в ходе выполнения исследуемой программы. Однако, из-за сложности алгоритмов современного программного обеспечения, данные виды анализа невозможно осуществить за разумное время. Это является причиной того, что традиционные подходы к анализу программного обеспечения становятся менее пригодными. Решением является автоматизация динамического анализа.

Для реализации автоматизированного динамического анализа существует технология, которая называется как динамическая бинарная инструментация (*Dynamic Binary Instrumentation*, DBI). Суть данной технологии заключается во вставке в бинарный исполняющийся код анализирующих процедур. Одним из преимуществ данного вида инструментации является то, что она не требует перекомпиляции приложения, она способна в режиме реального времени динамически встраиваться в исполняемый код. Важной особенностью динамической бинарной инструментации является то, на какой платформе происходит перезапись инструкций. Платформы делятся на две категории:

– с фиксированной длиной инструкций: в этом случае при перезаписи инструкции на инструкцию передачи управления всегда переписывается только одна инструкция. Примеры таких платформ – ARM и SPARC;

– с переменной длиной: в данном случае при перезаписи инструкции на инструкцию передачи управления может переписаться несколько инструкций (при этом последняя не полностью), что вносит определенные трудности. Примерами таких платформ являются x86 и x86–64 [1].

Благодаря наличию систем динамической бинарной инструментации приложений расширяются возможности поиска уязвимостей и ошибок в программном обеспечении путем генерации различных наборов передаваемых параметров и передачи их на вход тестируемых функциональных объектов. Этот метод тестирования носит название фаззинг (*fuzzing, fuzz-testing*) [2].

Основными задачами при анализе программ данным способом, являются:

– определение функционального объекта, в отношении которого будет производиться тестирование;

– определение сигнатуры функционального объекта (список и типы передаваемых параметров, тип возвращаемого значения;

– генерация передаваемых параметров;

– передача параметров на вход тестируемого объекта;

– отслеживание возникающих уязвимостей.

Для реализации DBI существует специальные средства, такие как Frida, Valgrind, DynInst, DynamoRIO и многие другие [1]. Каждое средство имеет свои плюсы и минусы, но наиболее востребованным является DynamoRIO.

DynamoRIO – это система динамической инструментации, работающая на Windows, Linux и Android на архитектурах x86 и x86_64, а также ARM. DynamoRIO, возникшее из Dynamo (динамический анализатор, созданный HP *Laboratory*), объединяет работу между Dynamo и группой по изучению и оптимизации среды выполнения (RIO) из MIT [3].

Цель DynamoRIO - наблюдать и потенциально манипулировать каждой инструкцией до её выполнения. DynamoRIO создает базовые блоки из целевой программы. Часто выполняемые базовые блоки в последовательности сшиваются, чтобы стать трассой. Базовые блоки и трассировки помещаются в кэш базовых блоков и кэш трасс, соответственно. Коды, запущенные из этих кэшей, ведут себя так, как будто они работают в исходном формате. DynamoRIO рассматривает последовательность команд, заканчивающуюся одной инструкцией передачи управления, как базовый блок. Базовый блок DynamoRIO отличается от традиционного базового блока, его точки входа и выхода являются либо вызовом подпрограммы, либо возвратом или ответвлением команды.

Но одной из ключевых особенностей является то, что DynamoRIO предоставляет пользователю богатый интерфейс прикладного программирования (API) для создания своего собственного пользовательского клиента DynamoRIO. Клиент DynamoRIO, написанный на C или C ++ используется для выполнения манипуляций с кодом во время его выполнения. Клиент может изменить код приложения и поместить соответствующие инструкции в кэш кода. Это также гарантирует прозрачность в отношении приложения и DynamoRIO, так что приложение может работать, не зная о присутствии DynamoRIO. Клиент создается как динамическая библиотека, которая загружается DynamoRIO, как только она захватывает целевую программу. Клиент взаимодействует с DynamoRIO через хуки, которые клиент экспортирует. Он работает совместно с DynamoRIO для работы с целевой программой. Когда клиент запускается, он обрабатывает целевую программу. Целевая программа уже скомпилирована, и является бинарной по-

следовательностью. Следовательно, нет никакого беспокойства, что вставленные инструкции будут удалены компилятором. Процесс инструментации представлен на рис.

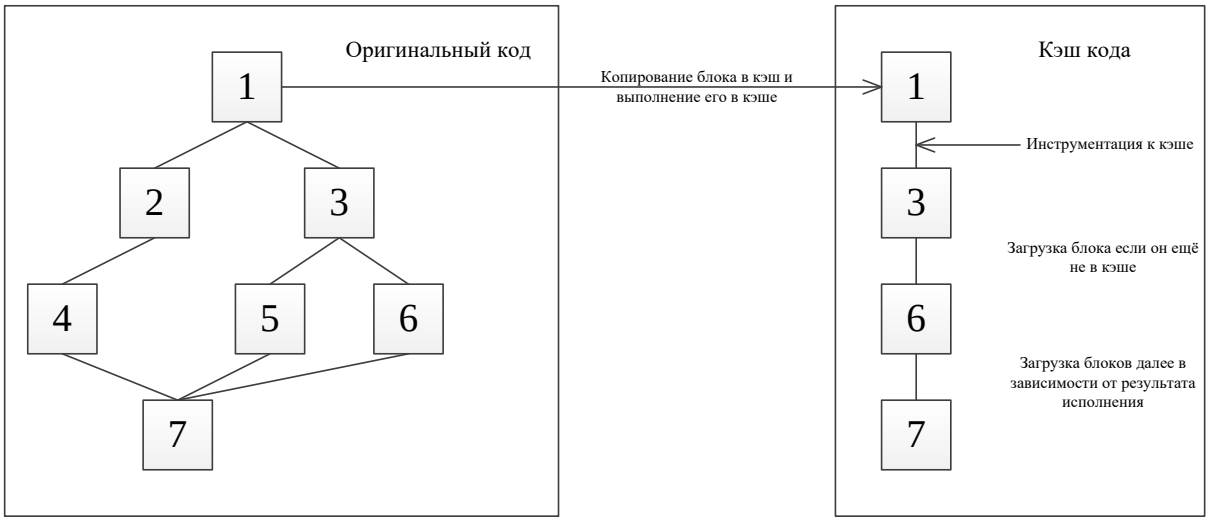


Рис. Процесс инструментации

Клиент DynamoRIO детектирует базовый блок в целевой программе и помещает его в свой кэш, где далее он выполняет с ним необходимые действия. Далее в процессе исполнения программы в кэш помещаются остальные базовые блоки. При необходимости в них вставляются необходимые инструментирующие функции.

Суть сбора информации о маршрутах выполнения приложения в том, что собирается и анализируется информация о приложении в момент его выполнения, осуществляется запись потока по адресу базового блока. Иными словами, записываются все вызываемые функции, включая функции из системных DLL-библиотек.

Список используемых источников

1. Инструментация – эволюция анализа [Электронный ресурс]. URL: https://xakep.ru/2013/09/11/61232/ (дата обращения: 15.11.2019).

2. Майкл Дж.Д. Саттон. Fuzzing. Исследование уязвимостей методом грубой силы : пер. с англ. СПб. : Символ-Плюс, 2009. 560 с. ISBN: 978-5-93286-147-9.

3. The DynamoRIO API [Электронный ресурс]. URL: http://dynamorio.org/docs/ (дата обращения: 25.09.2019).

УДК 004.056
ГРНТИ 81.96

АВТОМАТИЗИРОВАННЫЙ ДИНАМИЧЕСКИЙ АНАЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СРЕДСТВАМИ ДИНАМИЧЕСКОЙ БИНАРНОЙ ИНСТРУМЕНТАЦИИ DYNAMORIO

А. А. Колесников, А. С. Хилько

Академия ФСО России

В данной статье описан метод автоматизации динамического анализа API-функциями DynamoRio. Изложены основные достоинства и недостатки автоматизации данным способом. Приведен пример автоматизации анализа программного обеспечения. Целью данной работы является повышение безопасности приложений путём выявления в них недекларированных возможностей.

динамический анализ, динамическая бинарная инструментация, автоматизированный анализ, инструкции процессора.

В процессе тестирования программного обеспечения (ПО) специалисты данной области часто используют ручные методы анализа. Кроме того, происходит усложнение алгоритмов, используемых в приложениях, вследствие чего увеличивается объем исходных текстов и полученных из них машинных инструкций. Следовательно, автоматизация некоторых процессов позволит существенно повысить производительность и избавить пользователя от ошибок, вызванных человеческим фактором.

Существуют множество методов анализа ПО. По уровню знаний о структуре ПО методы анализа можно разделить на функциональное тестирование (по принципу «черного ящика») и структурное тестирование (по принципу «белого ящика»). Также существует метод тестирования по принципу «серого ящика», который подразумевает наличие некоторой информации о структуре исследуемого ПО. В зависимости от исследуемой структуры следует выбирать соответствующие методы автоматизации. Например, при исследовании приложения с исходными кодами процедура автоматизации является несложной задачей, достаточно сравнивать полученные инструкции с имеющимися исходными текстами, что нельзя сделать при функциональном тестировании.

Динамический анализ ПО – анализ приложения в процессе его работы. Это существенно усложняет процедуру автоматизации. Если для автомати-

зации статического анализа достаточно просто искать машинные инструкции в критических участках кода, то для динамического анализа процедура поиска усложняется необходимостью анализа инструкций, которые приложение передает процессору для выполнения.

Для анализа приложения можно использовать отладчик, который будет выполнять исследуемую программу по шагам, но современные приложения имеют большой объем и вручную просмотреть все выполняемые команды становится невозможно. Кроме того, в некоторых приложениях может содержаться защита от отладки, затрудняющая процедуру исследования путем выполнения специально сформированных, может быть вредоносных, команд.

Для решения данной проблемы можно использовать средства динамической бинарной инструментации (ДБИ). Под ДБИ следует понимать процесс трансляции бинарного кода в промежуточный язык с его последующим исполнением [1]. Для проведения инструментации существует большое количество средств, такие как:

– EEL;
– ERESI;
– TAU;
– Vulcan;
– Aslan;
– PIN;
– DynamoRIO;
– Dynist.

Для решения задач автоматизации будем использовать DynamoRIO.

DynamoRIO – свободно распространяемое ПО для операционных систем Windows и Linux, предназначенное для изменения машинных инструкций в процессе функционирования исследуемого ПО [2]. DynamoRIO позволяет программисту вставлять произвольный код (написанный на C или C++) в произвольных местах исполняемого файла.

При запуске приложения с использованием DynamoRIO, она перехватывает выполнение команды исполняемого файла и передает управления на специально сформированный код, написанный программистом для проведения анализа. После выполнения этого кода, DynamoRIO обратно передает управление тестируемому приложению. Следовательно, факт выполнения дополнительных инструкций для тестируемого приложения остается незамеченным, что позволяет защитить средство анализа от обнаружения.

Схема анализа ПО с помощью DynamoRIO представлена на рис.

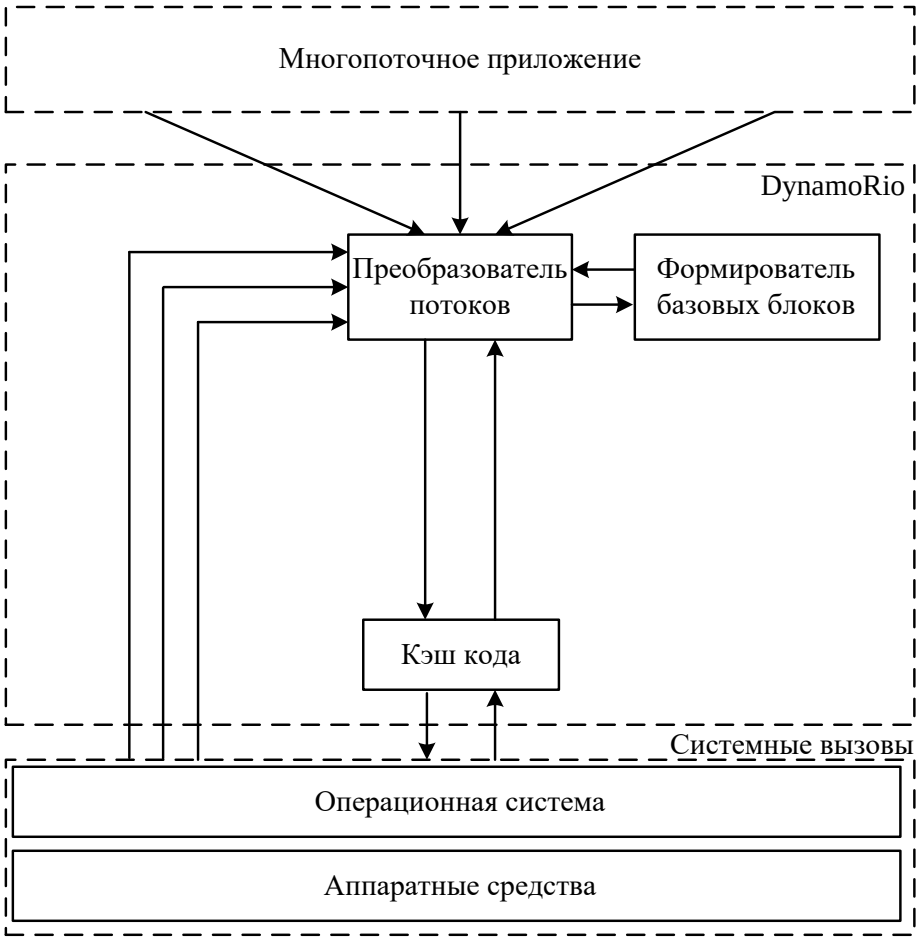


Рис. Схема анализа ПО API-функциями DynamoRIO

На данной схеме показано, что при проведении тестирования средствами ДБИ DynamoRIO данное средство анализа является промежуточным звеном между исследуемым приложением и операционной системой.

Данный метод анализа предоставляет множество способов тестирования, так как существует большое количество вариантов кода, написанного программистом с помощью API-функций DynamoRIO. Примером автоматизации такого тестирование является поиск участков кода, в которых содержатся ветвления, переходы в функцию и другие потенциально возможные уязвимости в ПО. После обнаружения данных участков необходимо записывать адреса, в которых хранятся данные инструкции.

Таким образом, программисту необходимо написать код, который будет осуществлять поиск потенциально опасных команд, и записывать адреса данных команд, например, в текстовый файл. Объем написанного программистом кода не будет большим, так как содержит в себе всего две процедуры: поиск и запись. Данный метод позволяет существенно повысить скорость проведения тестирования объемных приложений, так как ручной просмотр машинных инструкций с помощью отладчика занимает очень много времени. Но в то же время, данный метод не позволит найти участки

кода, в которых данные ветвления защищены от обнаружения путем применения экзотических способов ветвления.

Кроме того, недостатком такой автоматизации является невозможность найти все возможные потенциально опасные участки приложения, так как данных вариантов большое количество и перебрать все варианты невозможно. Но для простых программ данный способ позволяет сэкономить большое количество времени.

Уже на простом примере можно убедится в преимуществах автоматизированного анализа над ручным, при этом рассматривался наиболее примитивный способ автоматизации. При усложнении данного метода можно устранить ряд недостатков, тем самым еще повысив эффективность анализа.

В результате, можно утверждать, что автоматизация тестирования приложений при проведении динамического анализа позволяет программисту избавиться от рутинных операций, следовательно, ускорить проведение исследования, но и имеет ряд недостатков, описанных выше.

Список используемых источников

1. Казарин О. В. Безопасность программного обеспечения компьютерных систем: монография. М. : МГУЛ, 2003. 212 с.

2. Шудрак М. О. Методика и программный комплекс для динамического поиска уязвимостей в бинарном коде // Программные продукты и системы. 2014. № 4. С. 78–84.

УДК 004
ГРНТИ 20

РОЛЬ ПРОТОТИПИРОВАНИЯ В ПРОЕКТИРОВАНИИ ИНФОРМАЦИОННОГО РЕСУРСА

П. О. Кольцов, Е. С. Хайбрахманова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье описывается роль прототипирования в проектирование информационных систем, создание прототипов страниц информационного ресурса для сервис-агрегатора. Проведен сравнительный анализ англоязычных информационных платформ. В статье рассматривается подход к прототипированию информационных систем. Определены основные требования к прототипированию информационных систем.

прототип, прототипирование, юзабилити, пользовательский интерфейс, информационные системы.

Хороший пользовательский интерфейс обладает высокими показателями конверсии и прост в использовании. Другими словами, пользовательский интерфейс хорош как для бизнеса, а так и для людей, которые им пользуются.

Правильное размещение элементов интерфейса делает ресурс привлекательным для пользователей, повышает юзабилити [1]. В отдельных случаях, грамотная компоновка сайта склоняет посетителей к определенным действиям: купить билет, зарегистрироваться, приобрести товар и т. п.

С этой целью на этапе проектирования предварительно создают прототип – макет, выполненный в черно-белом варианте, представляющий упрощенную схему сайта. Макет содержит все основные элементы, представленные в упрощенном варианте. В таком виде клиенту проще оценить основную концепцию разрабатываемого проекта.

Также прототипирование помогает выяснить и сформировать основное направление будущего дизайна, при этом значительно сэкономив время. Дизайнеру нет необходимости тратить неделю на разработку абсолютно нового макета сайта. Это не единственная причина, по которой стоит уделить время созданию прототипа.

Прежде чем перечислить преимущества прототипирования, нужно четко определить, что есть прототип и процесс прототипирования.

Прототип – эскизный проект, предшествующий разработке оригинального дизайнерского макета. Прототип призван не только показать размещение основных элементов интерфейса и структуру разрабатываемого сайта, но и карту сайта, взаимосвязь его основных страниц.

Прототипирование – второй этап создания сайта. Во время создания прототипов закладывается функциональность, создаются ссылки, наглядно оценивается удобство сценариев, продуманных в карте сайта.

Среди главных причин использования прототипирования перед созданием макета можно выделить следующие:

– заказчик, глядя на прототип, имеет полноценное представление о том, как выглядит сайт в конечном результате;

– процесс прототипирования позволяет рационализировать процесс разработки визуальной составляющей сайта, концентрируя внимание на важных элементах интерфейса;

– эскиз – незаменимая вещь в процессе проектирования, если клиент еще не знает, какими функциями будет обладать та или иная страница. Тщательное планирование на этапе прототипирования позволяет избежать серьезных изменений в готовом макете;

– на этапе прототипирования выявляются ненужные элементы, от которых лучше всего отказаться, или же наоборот – дополнить интерфейс дополнительными деталями;

– данный процесс значительно снижает объем работы дизайнера по разработке проекта, а значит и экономит деньги заказчика;

– дизайнер и заказчик представляют конечный результат, когда имеют на руках прототип;

– разработка прототипа предполагает вовлечение заказчика, способствует продуктивной работе, согласованности процесса.

Прототип при этом создается достаточно легко. Уже при первой встрече с заказчиком можно набросать эскизы, уточняя определенные детали проектирования.

Существуют разные способы создания эскиза сайта. Один из самых быстрых – эскиз, нарисованный от руки. Бумажные модели пользуются большой популярностью среди дизайнеров, несмотря на развитие технологий. Преимуществом данного вида является скорость. Уже на этапе обсуждения создается набросок модели, вносятся поправки и замечания заказчика. Такой подход дает возможность лучше понять клиента, определить цели проекта. Бумажные прототипы чаще всего используются на этапе проработки идеи и возможных вариантов, так как нарисовать несколько возможных прототипов гораздо проще, чем создавать их с помощью соответствующих программных продуктов.

Бумажное прототипирование относится к статичным моделям, которые отличаются содержанием статичных изображений. Помимо концептов, нарисованных от руки, к статичным прототипам относятся эскизы, созданные в графических редакторах, нарисованные на планшете или маркерной доске. Эскизы отображают исключительно проект дизайна сайта.

Интерактивные прототипы, в отличие от статических, представляют собой проектирование взаимодействия всех составляющих ресурса. Это упрощенные макеты всех страниц веб-сайта с высокой детализацией. При этом все элементы находятся в зоне восприятия клика мышью: присутствует возможность перейти на другие страницы прототипа, развернуть различные меню и т. п. Интерактивный прототип раскрывает механизм работы проекта, помогает осуществить поставленные проектные решения, выявить целесообразность их реализации в готовом макете.

Современные инструменты позволяют создавать интерактивные макеты легко и достаточно быстро. Для этого не требуется глубоких знаний верстки.

Каждый инструмент обладает своими особыми возможностями и преимуществами. Необходимо оценить поставленные задачи и цели проектирования, совместимость с установленной операционной системой, оценить простоту использования, возможность совместной работы, внести правки или полностью изменить исходный вариант. Программа должна содержать

шаблоны, иметь возможность адаптировать свой макет под различные разрешения, будь то смартфон, персональный компьютер или планшет, поскольку такая программа призвана упростить процесс моделирования.

При разработке системы обязательным документом является техническое задание. Техническое задание – это документ, содержащий требования заказчика к объекту закупки, определяющие условия и порядок ее проведения для обеспечения государственных или муниципальных нужд, в соответствии с которым осуществляются поставка товара, выполнение работ, оказание услуг и их приемка [2]. Техническое задание является юридическим документом – как приложение включается в договор между заказчиком и исполнителем на проведение проектных работ и является его основой: определяет порядок и условия работ, в том числе цель, задачи, принципы, ожидаемые результаты и сроки выполнения.

Чтобы начать разработку информационной системы, необходимо определиться с областью. Затем проводится поиск и анализ аналогичных информационных систем: отбираются несколько систем, приводится краткое описание каждой, составляются критерии оценки, которые, в свою очередь, позволяют выявить преимущества и недостатки выбранных для анализа систем. Выявленные преимущества и недостатки позволяют внести корректировки в разработку, позволяют добиться максимально возможного качества.

Например, для информационных систем в сфере продажи билетов важно, чтобы пользователь мог достигнуть поставленных перед собой целей – найти мероприятие и купить на него билет. Однако, каждая информационная система предоставляет пользователю отличные от друг друга варианты достижения этих целей.

Яндекс Афиша – сервис, предоставляющий свои услуги на территории Российской Федерации и обладающий дружелюбным интерфейсом. На сайте присутствует окно поиска и различные фильтры, понятная навигация, практически отсутствует перегруженность. Оформление главной страницы приведено на рис. 1. Сервис позволяет приобретать билеты на мероприятия только в двух городах России – Москве и Санкт-Петербурге, физических точек продаж билетов не имеет.

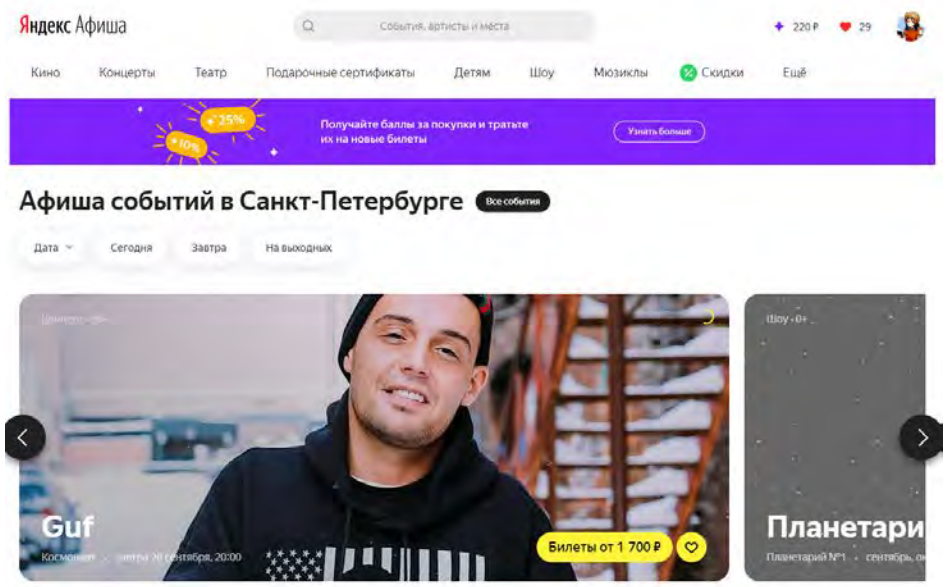


Рис. 1. Главная страница Яндекс Афиша

Ponominalu – сервис, предоставляющий пользователю возможность быстро найти и приобрести билет на выбранное им мероприятие: на главной странице располагается поле поиска, ниже – популярные теги, которые пользователи используют для поиска мероприятий чаще всего. Оформление главной страницы приведено на рис. 2. Надпись выше – «Быстрый поиск и покупка билетов» – слоган, который отражает преимущества и возможности сервиса. Помимо этого, у сервиса отсутствует комиссионный сбор при покупке. Распространяет свои услуги на территории Российской Федерации.

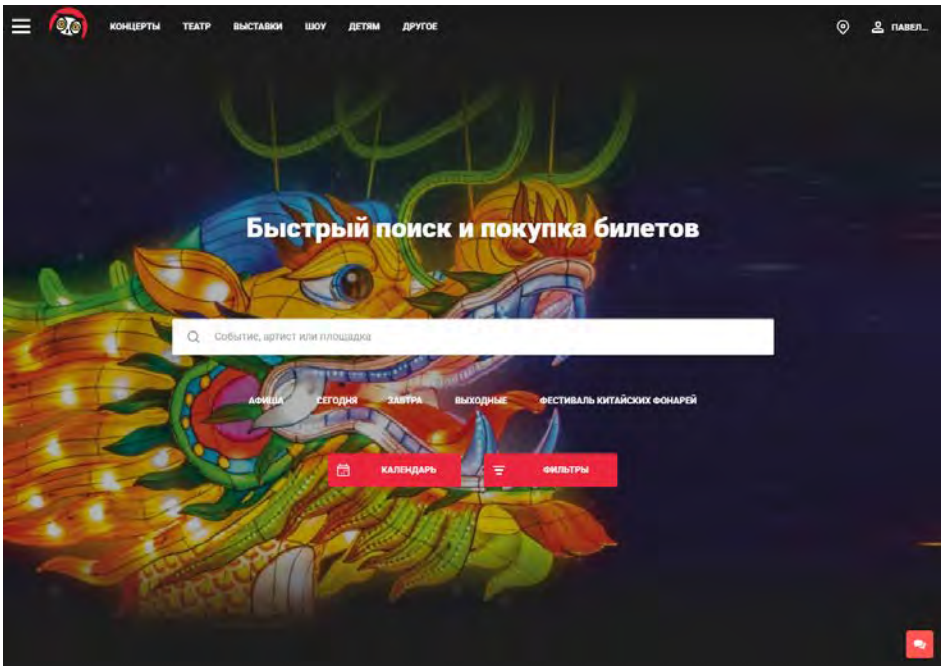


Рис. 2. Главная страница Ponominalu.ru

Таким образом, проектирование информационного ресурса включает в себя множество различных составляющих – процесс прототипирования, формирование технического задания, анализ аналогичных информационных систем. Успех проектирования во многом зависит также от навыков разработчика и от того, какие инструменты он использует в ходе разработки.

Список используемых источников

1. Сергеев С. Ф. Юзабилити информационных систем в образовании: основные этапы юзабилити в тестировании // Образовательные технологии. 2013. № 2. С. 57–63.

2. ГОСТ 25123-82. Машины вычислительные и системы обработки данных. Техническое задание. Порядок построения, изложения и оформления.

Статья представлена заведующим кафедрой ИКД СПбГУТ доктором технических наук, профессором Д. В. Волошиновым.

УДК 658.8.012.12
ГРНТИ 28.29.15

РЕШЕНИЕ ЗАДАЧИ ОПТИМИЗАЦИИ ВЫБОРА АССОРТИМЕНТА, ОБЪЕМОВ ПРОДАЖ, СЕГМЕНТОВ РЫНКА И ЦЕН НА УСЛУГИ ПРЕДПРИЯТИЯ СВЯЗИ

Г. О. Комлев, Э. Б. Песиков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается реализация одного из возможных подходов к формированию маркетинговой стратегии предприятия связи, основанного на применении методов исследования операций и позволяющего оптимизировать выбор ассортимента, объемов предложения, сегментов рынка и цен на услуги связи. Приводятся результаты решения задачи нелинейного частично-целочисленного программирования с помощью предлагаемого эвристического метода, основанного на итерационном увеличении цен на услуги связи и решении на каждом шаге изменения цен задачи линейного частично-целочисленного программирования методом Лэнда и Дойга.

предприятие, управление маркетингом, оптимизационная модель, услуга связи, целевой сегмент, объем продаж, цена, метод анализа иерархий.

В данной статье, являющейся продолжением работы [1], рассматривается реализация подхода к формированию маркетинговой стратегии предприятия связи, основанного на применении эвристических методов и моделей математического программирования и позволяющего оптимизировать товарную, ценовую и сбытовую стратегии.

В основу используемого аналитического инструментария положены представленные в работе [1] оптимизационная модель задачи выбора ассортимента, объемов продаж, сегментов рынка и цен на услуги и эвристический метод поиска приближенного решения исследуемой задачи.

Достоинством применения такой модели является то, что все расчеты по оптимизации выбора указанных объектов проводятся одновременно. Кроме того, отличительной особенностью предлагаемой оптимизационной модели является возможность планировать предложение как ранее реализуемых («старых»), так и новых видов услуг связи.

Постановка задачи

Пусть предприятие связи оказывает свои услуги на определенных сегментах рынка. В товарном портфеле предприятия имеются также виды услуг, с которыми предприятие еще не выходило на рынок и по которым необходимо принимать решение о целесообразности их вывода на рынок. Проведенные маркетинговые исследования позволили оценить емкости рынков сегментов, на которых предприятие уже работает или предполагает выходить со своими услугами. Маркетологи определили также по каждому сегменту рынка предельные значения цен, по которым потребитель согласен приобрести услуги. Руководство предприятия ставит перед собой задачу достичь в планируемом периоде определенных значений прибыли от реализации услуг. Ожидаемые уровни наличных производственных ресурсов в планируемом периоде определены и используются при планировании в качестве ограничивающих факторов. Предполагаются заданными нормы расхода ресурсов на каждый вид услуги, затраты на реализацию одной услуги для каждого сегмента рынка, а также цены на единицу каждого вида ресурса. Требуется определить на какие сегменты рынка, с какими услугами, объемами предложения и ценами следует выходить предприятию при условии, что будут реализованы цели предприятия, учтены ограничения по ресурсам и спросу и при этом ожидаемая прибыль от реализации услуг достигнет своего максимального значения.

Как показано в работе [1], математическая модель поставленной задачи сводится к модели нелинейного частично-целочисленного программирования с переменными непрерывного и булевого типа, применение которой позволяет планировать производство как ранее выпускаемой, так и новой продукции. Для анализа модели предлагается использовать эвристический алгоритм, основанный на итерационном увеличении цен на продукцию

и решении на каждом шаге изменения цен задачи линейного частично-целочисленного программирования методом Лэнда и Дойга [2].

Решение поставленной задачи на ПК применительно к отрасли связи

Исходные данные

Распределение уже освоенных и альтернативных видов услуг по сегментам рынка представлено в табл. 1. Символ «*» означает возможность работы с данной услугой на сегменте рынка, а символ «**» – новую (альтернативную) услугу.

ТАБЛИЦА 1. Распределение видов услуг по сегментам рынка

Код услуги	Услуга	Код сегмента				
		S1	*S2*	*S3*	*S4*	*S5*
U1	Внедрение IP АТС	*	*			*
U2	Установка и переустановка абонентских устройств	*		*		*
U3	Объединение устройств и компьютеров в сеть	*	*			*
U4	Монтаж волоконно-оптических линий связи			*	*	
U5	Ремонт волоконно-оптических линий связи			*	*	*
U6	Аренда каналов связи				**	
U7	Аренда сервера	**		**		

В табл. 2 приведены значения нижних и верхних границ платёжеспособного спроса в плановом периоде (год) на все виды услуг, имеющихся в товарном портфеле предприятия.

ТАБЛИЦА 2. Нижние (Н) и верхние (В) границы спроса на услуги (количество обращений в год)

Код услуги	Сегменты									
	S1		*S2*		*S3*		*S4*		*S5*	
	Н	В	Н	В	Н	В	Н	В	Н	В
U1	500	2 000	1 000	3 000	-	-	-	-	700	2 600
U2	300	1000	-	-	200	1 500	-	-	100	1 600
U3	40	700	60	500	-	-	-	-	160	1 000
U4	-	-	-	-	200	1 200	350	1 500	-	-
U5	-	-	-	-	300	2 000	140	1 400	30	800
U6	-	-	-	-	-	-	100	500	-	-
U7	150	800	-	-	45	400	-	-	-	-

В табл. 3 приведены начальные, предельные значения цен и приращения цен на каждый вид услуги *j* для каждого сегмента *f*.

ТАБЛИЦА 3. Начальные, предельные цены и приращения цен на услугу

Услуга (*j*)	Сегмент (*f*)	Начальная цена услуги *j* на сегменте *f* (руб.)	Предельная цена услуги *j* на сегменте *f* (руб.)	Приращение цены на услугу *j* на сегменте *f* (руб.)
U1	*S1*	10 000	115 000	13 200
U1	*S2*		105 000	
U1	*S5*		142 000	
U2	*S1*	250	4 000	375
U2	*S3*		5 000	
U2	*S5*		3 000	
U3	*S1*	400	6 000	710
U3	*S2*		8 800	
U3	*S5*		7 500	
U4	*S3*	7000	64 000	5700
U4	*S4*		58 000	
U5	*S3*	2000	12 400	1180
U5	*S4*		14 300	
U5	*S5*		13 800	
U6	*S4*	12500	35 000	2 250
U7	*S1*	900	8 600	770
U7	*S3*		6 300	

Виды наличных ресурсов, необходимых для оказания услуг, а также нормы расхода на одну услугу представлены в табл. 4. В табл. 5 представлены данные о затратах на реализацию единицы каждой услуги через стоимость одного часа работы. В табл. 6 приведена стоимость единицы ресурсов, необходимых для предоставления первых пяти услуг.

ТАБЛИЦА 4. Нормы расхода ресурсов на одну услугу

Код услуги	Наименование ресурса				
	Фонд времени работы сотрудников (час.)	Оптический кабель (км.)	Патч-корд (км.)	Время работы серверов (час.)	Время работы канала связи (час.)
U1	70	-	0,2	-	-
U2	8	-	0,02	-	-
U3	6	-	0,1	-	-
U4	10	0,9	-	-	-
U5	10	0,07	-	-	-
U6	4	-	-	-	720
U7	1	-	-	720	-

Код услуги	Наименование ресурса				
	Фонд времени работы сотрудников (час.)	Оптический кабель (км.)	Патч-корд (км.)	Время работы серверов (час.)	Время работы канала связи (час.)
Всего ресурса в наличии:	347 200	700	2 000	172 800	259 200

В табл. 5 представлены данные о затратах на реализацию каждой услуги через стоимость одного часа работы. В табл. 6 приведена стоимость единицы ресурсов, необходимых для предоставления первых пяти услуг.

ТАБЛИЦА 5. Данные о стоимости реализации одной услуги

Код услуги	Норма расхода времени на одну услугу (час)	Стоимость часа работы сотрудника (руб.)	Затраты на реализацию одной услуги (руб.)
U1	70	250	17 500
U2	8	200	1 600
U3	6	200	1 200
U4	10	250	2 500
U5	10	250	2 500
U6	4	250	1 000
U7	1	250	250

ТАБЛИЦА 6. Стоимость единицы ресурсов

Наименование ресурса	Единица измерения ресурса	Цена единицы ресурса (руб.)
Оптический кабель	км	40 000
Патч-корд	км	30 000

Расчеты проводились с использованием программы «Lindo», предназначенной для решения задач линейного и частично-целочисленного программирования. Используя результаты решения последовательности задач, получаемых в процессе итерационного увеличения цен на услуги связи, строится график изменения прибыли от предоставления услуг в зависимости от номера итерации изменения цен (см. рис.).

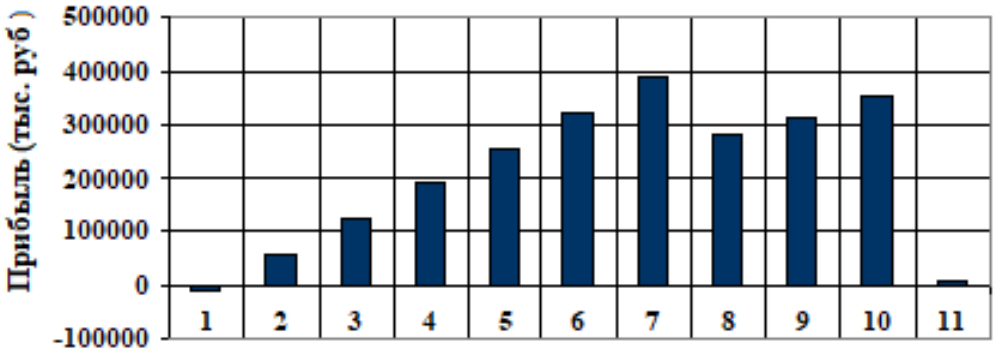


Рис. График зависимости прибыли от номера шага изменения цен

Значения объемов предложения(V) и цен на услуги связи (P), а также множество сегментов на седьмом шаге итерационного процесса изменения цен, на котором достигается максимальная прибыль предприятия, будут соответствовать оптимальному решению исходной задачи (см. табл.7).

ТАБЛИЦА 7. Оптимальные значения объёмов предложения услуг (обращений в год)

Код услуги	Код сегмента									
	S1		*S2*		*S3*		*S4*		*S5*	
	V	*P*	*V*	*P*	*V*	*P*	*V*	*P*	*V*	*P*
U1	2 000	102 400	2 009	102 400					700	102 400
U2	300	2875			200	2 875			100	2 875
U3	40	5370	60	5370					160	5 370
U4					200	46 900	350	46 900		
U5					300	10 260	140	10 260	30	10 260
U6							360	28 250		
U7	-	-			240	6290				

Представляется целесообразным оказывать альтернативные услуги, при этом услугу *U7* необходимо реализовывать только на сегменте *S3* (без выхода на *S1*). Максимальное значение прибыли от реализации рассматриваемого набора услуг составило 390 516,448 тыс. руб.

В дальнейшем для сокращения размерности решаемой задачи и выбора подходящих к работе сегментов рынка предлагается использовать метод анализа иерархий (метод Т. Саати) [3].

Список используемых источников

1. Песиков Э. Б. Оптимизация управления маркетингом предприятия на основе применения методов исследования операций // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 2. С. 491–497.

2. Зайченко Ю. П. Исследование операций. Учебник. 6-е изд. Киев : Слово, 2003. 668 с.

3. Саати Т., Кернс К. Аналитическое планирование. Организация систем. М. : Радио и связь, 1991. 224 с.

УДК 004.9
ГРНТИ 47.63.29

СПЕЦИФИКА ВОСПРИЯТИЯ ОПТИЧЕСКИХ ИЛЛЮЗИЙ КОМПЬЮТЕРНЫМ ЗРЕНИЕМ

П. В. Косов, А. А. Шиян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются особенности и отличия компьютерного зрения от человеческого. Рассмотрены особенности оптических иллюзий.

оптические иллюзии, компьютерное зрение, системы восприятия.

Компьютерное зрение (КЗ) является одним из самых востребованных направлений в современном мире ИТ. Это автоматическая фиксация и обработка изображений, как неподвижных, так и движущихся объектов при помощи компьютерных средств.

Задачи КЗ:

1) распознавание;
2) оценка движения;
3) восстановление сцены;
4) восстановление изображения.

КЗ уже активно используется в таких отраслях, как сельское хозяйство, медицина, автомобилестроение и т. д. Также КЗ и искусственный интеллект (ИИ) способны помочь в исследованиях тех областей науки, которые до сих пор плохо изучены. Одной из таких областей является изучение оптических иллюзий.

Иллюзия – обман органов чувств, нечто искажённое восприятием реально существующего объекта или явления. Их возникновение зависит от формы изображения и его содержания. Механизмы восприятия мозгом оптических иллюзий до сих пор плохо изучены, однако считается, что они возникают из-за несоответствия между считыванием информации (глазами) и обрабатывающим эту информацию отделом мозга (зрительной корой).

Чтобы научить компьютер видеть и распознавать оптические иллюзии, необходимо определить причину, по которой мы способны их видеть.

Из всех человеческих ощущений зрений считается самым сложным инструментом. Зрительная система включает в себя многоступенчатый процесс обработки информации.

Любая зрительная информация начинается со зрительного стимула – света. Отраженный от объектов он фокусируется хрусталиком, пройдя через его линзу, лучи образуют изображение на сетчатке глаза. Такое изображение мало напоминает то, что мы привыкли видеть. Изображение получается перевернутым, содержащим в себе различные аберрации, ошибки формирования изображения на сетчатке в неидеальных оптических системах (ОС), вызванные отклонениями лучей света от направления, по которым они должны были быть направлены в идеальной ОС. Связано это с неоднородностью хрусталика и с особенностью хрусталика по-разному преломляет лучи разного цвета [1].

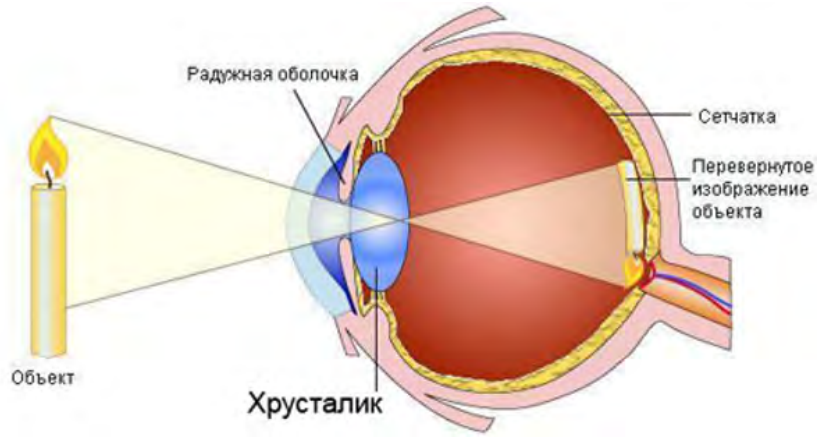


Рис. Оптическая система человеческого глаза

Примерно 17 раз в минуту изображение на сетчатке пропадает из-за мигания. Мигания подавляются в моменты напряженной работы, а после ее завершения их количество резко увеличивается. Также наши зрачки непрерывно находятся в движении. Даже если кажется, что мы смотрим на неподвижный объект, наши глаза совершают незаметные микродвижения – микросаккады. Не замечаем мы их, так как наш мозг научился сглаживать изображение. Именно благодаря этим колебаниям человек может видеть неподвижные объекты. Наше зрение устроено так, что видит исключительно динамику в любых ее проявлениях: перемещение в пространстве, изменение яркости, размеров и т. п. Без микросаккад мы бы не смогли видеть объекты, которые не меняют своих свойств. Такие объекты становились бы для нас невидимыми [3].

В условиях дефицита информации мозг включает еще один уникальный процесс – домысливание. Домысливание словно достраивает картинку, используя данные о миллионах объектах, которые человек видел с рожде-

ния. Когда мозг обрабатывает информацию, полученную от глаз, ему приходится делать об увиденном выводы, чтобы на их основе построить осмысленные изображения. Изображение, которые мы видим, строится после анализа и обработки. Когда наш мозг делает неверные выводы и строит ложные изображения, возникают оптические иллюзии [1].

В зрительной системе компьютера имеются критические отличия от зрительной системы человека. Изначально компьютер получает цифровые изображения от одного или нескольких источников, которые могут включать в себя не только светочувствительные камеры, но и датчики расстояния, ультразвуковые камеры, радары и другое. Получаемые данные могут являться плоским изображением, объемным пространством или последовательностью изображений. Пиксельные значения, как правило, соответствуют световой интенсивности в спектральных полосах, однако могут быть связаны с разными физическими величинами. Например, поглощение или отражение электромагнитных волн.

Полученные данные должны пройти предварительную обработку, чтобы к ним могли быть применены методы компьютерного зрения и можно было извлечь определенную информацию. В зависимости от используемых методов, данные проходят различные виды обработки, чтобы привести исходную информацию к необходимым требованиям, которые индивидуальны для каждой отрасли. К видам таких обработок можно отнести удаление шума для уменьшения искажения, вносимых источником, повышение контрастности изображения, чтобы было проще обнаружить необходимую информацию, масштабирование для лучшего различия объектов. Также во время обработки некоторые детали могут быть выделены. Например, при помощи границ или линий.

На определенных этапах обработки изображений используются детектирование и сегментация, во время которых изображения разделяют на интересующие сектора для последующей обработки и ненужные сектора, которые система впоследствии будет игнорировать. Это может быть сегментация участков изображения с характерным объектом или выделение конкретного набора интересующих точек

С отобранными сегментами производится высокоуровневая обработка, в которой проводится проверка того, что данные удовлетворяют определенным условиям, и классификация по категориям обнаруженного объекта. Исходные данные на этом этапе, как правило, представляют из себя набор точек или небольшой участок изображения, на котором предположительно размещается объект [6].

Ученые Луисвилльского университета Роман Ямпольский и Роберт Уильямс попытались создать ИИ, способный самостоятельно распознавать и строить оптические иллюзии. Оценив результаты работы ИИ, строящих изображения несуществующих людей на основе базы данных, они решили

действовать таким же способом. Им удалось собрать базу данных из 6 725 изображений различных оптических иллюзий и создать генеративно-состязательную сеть, которая должна была самостоятельно создавать оптические иллюзии.

Результаты оказались разочаровывающими. «После семи часов тренировок не было сгенерировано ничего ценного», – говорят исследователи. Ученые утверждают, что люди способны видеть оптические иллюзии, а системы компьютерного зрения – еще нет [5].

На данный момент невозможно научить компьютер видеть подобно человеку из-за серьезных отличий в восприятии изображения. Возможно, для решения этой проблемы необходимо лучше изучить поведение оптических иллюзий при изменении их характеристик и вывести закономерности, чтобы передать эти знания компьютеру.

Список используемых источников

1. Меньшикова Г. Я. Зрительные иллюзии: психологические механизмы и модели : автореф. дис. … докт. псих. наук: 19.00.02 / Меньшикова Галина Яковлевна. М., 2014. 46 с.

2. Arthur G. Shapiro, Dejan Todorovic, The Oxford compendium of visual illusions, Oxford, Oxford University Press. 2017. 833 p.

3. Adam Hadhazy, What are the limits of human vision? 2015. [Электронный ресурс]. URL: https://www.bbc.com/future/article/20150727-what-are-the-limits-of-human-vision (дата обращения: 11.11.2019).

4. Time-Traveling Illusion Tricks the Brain. 2018. [Электронный ресурс]. URL: https://www.caltech.edu/about/news/time-traveling-illusion-tricks-brain-84009 (дата обращения: 23.11.2019).

5. Neural networks don’t understand what optical illusions are. 2018. [Электронный ресурс]. URL: https://www.technologyreview.com/s/612261/neural-networks-dont-understand-what-optical-illusions-are/ (дата обращения: 15.10.2019).

6. Компьютерное зрение: технологии, рынок, перспективы. 2019. [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/%D0%A1%D1% 82%D0%B0% D1%82%D1%8C%D1%8F:%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B5_%D0%B7%D1%80%D0%B5%D0%BD%D0%B8%D0%B5:_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8,_%D1%80%D1%8B%D0%BD%D0%BE%D0%BA,_%D0%BF%D0%B5%D1%80%D1%81%D0%BF%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D1%8B.

УДК 004.056
ГРНТИ 81.93.29

СПОСОБ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ НА ОСНОВЕ АНАЛИЗА СЛУЖЕБНОГО ТРАФИКА

В. С. Косолапов, В. А. Липатников, А. А. Шевченко

Военная академия связи

Рассматривается возможность повышения защищенности информационно-вычислительной сети за счет внедрения способа управления кибербезопастностью информационно-вычислительной сети на основе анализа служебного трафика, с прогнозированием событий безопасности. Предлагается способ сетевого контроля служебного трафика. Введены процедуры распознавания нелегитимного пользователя, пытающегося получить доступ к защищаемым ресурсам информационно-вычислительной сети. Разработан алгоритм выявления последовательности действий нарушителя, определения вектора и стратегии кибернетического вторжения. Учитываются ситуационные параметры во взаимной противоборствующей обстановке с достоверным прогнозом вектора атаки.

информационно-вычислительные сети, сетевой контроль, защита информации, кибербезопасность.

Актуальность

Кибербезопасность (КБ) являет собой набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей. КБ подразумевает достижение и сохранение свойств безопасности у ресурсов организации или пользователей, направленных против соответствующих киберугроз [1, 2].

Стандарт ISO/IEC 27032:2012 (*Information technology–Security techniques – Guidelines for cybersecurity*) дает четкое понимание связи термина КБ (*cybersecurity*) с сетевой безопасностью, прикладной безопасностью, интернет-безопасностью и безопасностью критичных информационных инфраструктур с точки зрения западных специалистов.

Перспективным направлением является управление кибернетической безопасностью интегрированной организации с прогнозированием на основе интеллектуальных методов [3, 4]. КБ ставит своей целью обеспечение безопасности киберсреды – системы относящейся ко многим интегрированным организациям, со множеством составных компонентов и подходов к обеспечению безопасности. Существует множество различных классов

средств обеспечения кибербезопасности, в том числе интеллектуальных, недостатком большинства средств является реактивность используемых методов, с недостаточным вниманием к анализу динамики действий нарушителя при подготовке и реализации сценариев внешних, а также внутренних вторжений [5, 4]. За счет этого возникает противоречие между развивающимися средствами кибернетического вторжения и существующими способами защиты, что делает направление актуальным.

Релевантные работы

В работе [6] рассматривается подход к разработке и использованию систем КБ, основанный на выделении интеллектуальной составляющей над традиционными способами защиты и построении единой унифицированной среды для создания и поддержки функционирования систем защиты. Однако, не рассмотрены вопросы сетевого контроля служебной информации и выявления нарушений КБ.

В работе [7] недостаточно внимания уделено сетевому контролю служебной информации и анализу динамики действий нарушителя. В работах анализируются частные показатели и не учитываются особенности вторжений и воздействие нарушителей на служебный трафик. В действительности, не стоит пренебрегать тем фактом, что злоумышленники ежедневно находят новые способы обхода СЗИ, обнаруживают новые уязвимости в программах и протоколах.

Следовательно, совершенствование способа сетевого контроля позволит выполнить обнаружение и анализ нарушений КБ, детектировать большинство известных атак, обнаружить ошибки в конфигурировании и функционировании оборудования и ПО.

Определено противоречие, заключающееся в том, что с одной стороны оперативность нарушителя до формирования и реализации компьютерной атаки (КА) на основе учета данных служебной информации значительно увеличились, а, с другой стороны, современные методы КБ оказываются не эффективными из-за недостаточной информированности о воздействиях на служебный трафик.

Цель исследования – совершенствование управления КБ за счет повышения оперативности анализа сетевого контроля.

Постановка задачи – разработать способ управления КБ на основе повышения оперативности анализа служебного трафика при требуемой достоверности.

Основная часть. Управление КБ организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией [3], происходит за счет добавления в демилитаризованную зону ИВС выделенного сервера, на котором с помощью технологии контейнерной виртуализации развёртывается виртуальная копия реальной сети, включающая сетевые

сервисы. Злоумышленник, производящий подготовку компьютерной атаки на сеть, работая с данным сервером, предполагает, что взаимодействует с реальной сетью. В процессе анализа действий злоумышленника в реальном времени, администратор сети получает информацию о приоритетных целях злоумышленника, используемых им средствах и уязвимостях различных элементов сети, что даёт ему возможность оперативно принять меры по повышению защищённости сети и избежать её компрометации.

Определение легитимного и нелегитимного пользователя реализуется за счет сетевого контроля, распознавания последовательности действий нарушителя, определения вектора и стратегии кибернетического вторжения, определение ситуационных параметров во взаимной противоборствующей обстановке с достоверным прогнозом вектора атаки.

Для передачи пользовательских данных в информационно-вычислительную сеть (ИВС) используются различные протоколы, использование которых сопровождается служебной информацией.

Анализ цифровых потоков в ИВС позволяет сделать вывод о том, что служебная информация может являться источником информации как о самой сети и её элементах, так и о характере её функционирования.

При осуществлении сетевого контроля особое внимание уделяется анализу служебного трафика, так как при анализе служебной информации потенциальный нарушитель может получить сведения о потенциальных объектах вторжения. Следовательно, при сетевом контроле необходимо выявлять уязвимости служебной информации.

В процессе организации КБ при сетевом контроле необходимо распознать подготовку и реализацию КА в процессах сбора хранения, обработки и передачи информации при попытках нарушителя воздействовать на инфраструктуру организации, выводя её из строя или снижая её эффективность.

Разделение трафика на пользовательский и служебный происходит на этапе его первичной обработки на выделенном сервисе из PCAP файлов. В качестве критерия используется информация из полей EtherType, SSAP, DSAP в зависимости от типа Ethernet-кадра и поля «Protocol» заголовков IP-пакетов [8, 9]. Происходит детектирование аномального пользовательского и служебного трафика. Сгенерированные IDS/IPS системой Snort журналы уведомлений обнаружения аномального трафика отправляются в агент прогнозирования вторжений. В случае отсутствия сетевых аномалий, происходит объединение трафика. Разработанная ранее общая структурная схема процесса анализа служебного трафика при сетевом контроле [10, 11].

Процесс управления КБ ИВС должен получать информацию о текущем состоянии путем анализа ЦП соединения [12] Для обеспечения требуемой достоверности целесообразно учитывать свойства структуры ЦП, передаваемого в канале связи.

Благодаря новой совокупности существенных признаков в заявленном способе, за счёт отслеживания поведения нелегитимного пользователя на выделенном сервере в демилитаризованной зоне, что позволяет заблаговременно перенастроить средства защиты информации и сетевые службы ИВС, заранее предотвращая вторжение в ИВС, что указывает на достижение технического результата – повышение структурной надёжности, обеспечивающей устойчивую работу ИВС [13].

Анализ существующих источников в данной предметной области показывает, что традиционный подход к построению средств защиты информации (СЗИ) подразумевает так называемую реактивную модель поведения: действия по нейтрализации разрушающего воздействия КА принимаются после их обнаружения [14, 15]. Также существенным недостатком большинства СЗИ является то, что они используют множество угроз, заложенное разработчиками на этапе разработки и расширяемое только путём обновления со стороны разработчиков. При этом, множество угроз для ИВС постоянно меняется: злоумышленники находят новые способы обхода СЗИ, обнаруживают новые уязвимости в программах и протоколах. Поэтому «традиционные» СЗИ, такие как антивирусное программное обеспечение, межсетевые экраны и системы обнаружения вторжений не могут гарантировать соответствия защищённости ИВС требуемому уровню.

Практическая значимость

Настоящее решение позволит своевременно среагировать на события, требующие внимания со стороны персонала, занимающегося вопросами обеспечения информационной безопасности ИВС, и как результат предотвращение попыток вторжения на сеть. При этом способ позволяет поддерживать защищённость ИВС выше требуемого значения $P_{ЗТ}$ в пределах каждой итерации цикла управления ИБ.

Выводы

Предложенный подход позволяет обеспечить КБ защищаемой инфраструктуры ИО на основе использования модели прогнозирования событий.

Данные о событиях безопасности формируются на уровне инфраструктуры, подлежат предварительной обработке на уровне данных, распространяются с помощью уровня событий к требуемым элементам прикладного уровня и, в конечном итоге, окончательно обрабатываются элементами этого последнего уровня.

Список используемых источников

1. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности. Учебное пособие. СПб. : СПбГУТ, 2012. 396 с. ISBN: 978-5-91891-092-4.

2. Липатников В. А., Царик О. В.Методы радиоконтроля. Теория и практика: монография. Сер. «Система технической защиты информации в Российской Федерации» СПб., 2018. 607 с.

3. Липатников В. А., Чепелев К. В. Шевченко А. А. Способ защиты информационно-вычислительной сети от вторжений. Пат. Российской Федерации. № 2 705 773. Опубликовано: 11.11.2019. Бюл. № 32.

4. Липатников В. А., Кащенко М. А., Лобашев А. И. Алгоритм ассиметричного шифрования на основе решения задачи целочисленного программирования при взаимодействии информационных сетей // Информационные системы и технологии. 2019. № 1 (111). С. 113–123.

5. Липатников В. А., Тихонов В. А., Шевченко А. А. Метод управления кибернетической безопасностью в системах критических инфраструктур, основывающийся на интеллектуальных сервисах защиты информации // Технологии построения когнитивных транспортных систем. Материалы всероссийской научно-практической конференции с международным участием. 2019. С. 207–214.

6. Korshunov G. I., Lipatnikov V. A., Shevchenko A. A. Decision support systems for information protection in the management of the information network. Fuzzy Technologies in the Industry. FTI 2018. 23–25 October, 2018. Ulyanovsk (Russia). PP. 418–426.

7. Липатников В. А., Шевченко А. А. Способ контроля уязвимостей при масштабировании автоматизированной системы менеджмента предприятия интегрированной структуры // Информационные системы и технологии. 2016. № 2 (94). С. 128–140.

8. Kavanagh K. M., Rochford O., Bussa T. Magic Quadrant for Security Information and Event Management. Gartner. August 2016.

9. Kavanagh K. M., Bussa T. Magic Quadrant for Security Information and Event Management. Gartner. December 2017.

10. Batina Ivo. Model predictive control for stochastic systems by randomized algorithms. Eindhoven: Technische Universiteit Eindhoven, 2004.

11. Byres E., Lowe J. The myths and facts behind cyber security risk for industrial control systems // In ISA Process Control Conference, 2003.

12. Sheth H., Shah B., Yagnik S. A survey on RBF Neural Network for Intrusion Detection System // Int. Journal of Engineering Research and Applications. 2014. vol. 4. PP. 17–22.

13. Ryan J., Lin M.-J. Intrusion Detection with Neural Networks // Advances in Neural Information Processing Systems. 1998. PP. 943–949.

14. Tan K. The Application of Neural Networks to UNIX Computer Security // Proceedings of the IEEE International Conference on Neural Networks. 1995. Vol. 1. PP. 476–481.

15. Ярушева С. А., Аверкина А. Н., Федотова А. В. Модулярная модель прогнозирования временных рядов на основе нейро-нечетких сетей и когнитивного моделирования // Нечеткие системы и мягкие вычисления. 2017. Т. 12, № 2. С. 159–168. https://doi.org/10.26456/fssc31.

УДК 004.7
ГРНТИ 20.51.23

АНАЛИЗ ВЛИЯНИЯ СТРУКТУРНОЙ КОМПОЗИЦИИ НА СТАТИСТИЧЕСКИЙ ПРОФИЛЬ ПЛАНИРОВЩИКОВ ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОРМАЦИОННЫХ АГЕНТОВ

М. С. Коткина, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Описаны преимущества введения вычислительного интеллекта в информационные инфраструктуры. Рассмотрены архитектурные разнообразия носителей вычислительного интеллекта в виде интеллектуальных информационных агентов. Определены актуальные направления расширения знаний о качестве функционирования интеллектуальных информационных агентов. Выделены альтернативы в структурной композиции планировщиков интеллектуальных информационных агентов. Описаны элементы статистического профиля планировщиков. Представлены компоненты моделей планировщиков. Сформирована методика анализа влияния структурной композиции на статистический профиль планировщиков.

архитектура, интеллектуальный агент, структурная композиция, статистический профиль, модель планировщика.

Вычислительный интеллект является составной частью современного искусственного интеллекта. В информационной инфраструктуре вычислительный интеллект представляет собой совокупность методов, моделей, программных средств и технологий для решения неформальных задач с использованием представлений, в определённой степени отражающих мыслительную деятельность в виде нечеткости рассуждений, интуитивного и качественного подхода, самообучения, логического вывода и иных подходов.

Введение вычислительного интеллекта в информационную структуру позволяет:

1) снизить уровень ошибок;

2) увеличить скорость функционирования инфраструктуры;

3) повысить вычислительную адаптивность;

4) обеспечить устойчивость к внешним воздействиям.

Классификация архитектур интеллектуальных информационных агентов, как носителей вычислительного интеллекта, разделяет их на следующие группы:

1) архитектуры, в основе которых лежат принципы и методы искусственного интеллекта;

2) реактивные архитектуры, анализирующие поведение окружающих объектов и субъектов, с последующей реакцией на появляющиеся события внешнего мира;

3) гибридные многоуровневые архитектуры, объединяющие в себе достоинства предыдущих двух групп.

Наличие подсистемы моделирования является основным требованием к архитектуре информационного агента. Данная подсистема необходима для определения процессов собственного развития, на основании которых агент формирует своё поведение в настоящем и будущем [1, 2].

Преимущество организации агентов на принципах искусственного интеллекта заключается в предоставлении возможности использовать методы и средства символьного представления знаний, разработанные в рамках искусственного интеллекта. В то же время, становится достаточно трудно создать точную и полную модель представления мира, процессов и механизмов рассуждения в нём.

Альтернативным подходом к архитектуре интеллектуальных агентов являются принципы реактивной архитектуры. К реактивной относятся архитектуры, не имеющие детального представления модели окружающей среды, а функционирование отдельных агентов и всей системы в целом осуществляется по правилам типа ситуация – действие.

Гибридные архитектуры объединили в себе все преимущества архитектур, основанных на знаниях, и реактивных архитектур агентов.

При постоянном расширении технологических базисов информационных инфраструктур появляются новые востребованные приложения, базирующиеся на основе интеллектуальных информационных агентов. Данные приложения могут позволить пользователю управлять информацией, управлять контентом, извлекать знания, генерировать знания.

В контексте расширения областей применения интеллектуальных информационных агентов подвергается ревизии содержание основных этапов их жизненного цикла: актуализация, проектирование, создание, внедрение и сопровождение. В каждом из перечисленных приложений появляются новые аспекты, требующие внесения изменений в основные этапы их жизненного цикла.

Известные методологические исследования эффективности интеллектуальных информационных агентов ориентируются на анализ выполняемой интеллектуальным агентом деятельности, спланированной в их соответствующей подсистеме [3, 4, 5, 6]. При этом собственно процесс планирования не подвергается анализу. В связи с этим актуализируется исследование динамических характеристик процесса планирования действий интеллектуальных информационных агентов.

Планировщики действий интеллектуальных информационных агентов структурно описываются различными композициями процедур, относящихся к обобщённому алгоритму планирования [7].

Структурная композиция планировщиков интеллектуальных информационных агентов состоит из процедур, соответствующих компонентам обобщённого алгоритма планирования. Такими компонентами являются процедуры выбора подцели, используемой стратегии консервации и стратегии снижения вычислительной сложности.

При описании конструктора решений и выборе подцели, опираясь на результаты анализа функциональных спецификаций планировщиков, предусматриваются следующие варианты:

1) на основе модального критерия истинности проверяется условие завершения и выбор подцели (MTC);

2) на основе пустоты текущего множества подцелей проверяется условие завершения и произвольный выбор подцели из текущего множества подцелей (ARB).

При описании консервации используются следующие варианты:

1) консервация не проводится (NC);

2) осуществление консервации посредством односторонней защиты каузальных связей (SGL);

3) выполнение консервации через двустороннюю защиту каузальных связей (DBL).

Для снижения вычислительной сложности необходимо воспользоваться следующими стратегиями:

1) снижение вычислительной сложности не используется (NO);

2) снижение вычислительной сложности осуществляется посредством разрешения конфликтов (CFT);

3) упорядочивание шагов с целью снижения вычислительной сложности (ORD).

В предлагаемом подходе к анализу процесса планирования действий интеллектуальных информационных агентов предусматривается расширение его объектно-ориентированной модели, с последующим преобразованием данной модели по модифицированному методу свертки и определением динамических характеристик планировщика.

Представленные ниже характеристики, функции и параметры применяются для описания расширенных объектно-ориентированных моделей любого планировщика:

– размерность множества действий описывается размерностью выполняемых при планировании действий и обозначается I;

– $u_i(k_i)$, $k_i = 1,2, ..., K_i$ – плотность распределения вероятностей k_i дискретного времени выполнения i-го действия планировщика, K_i – верхняя

граница дискретного времени выполнения *i*-го действия, *I* – общее число действий, для каждого из которых соблюдается следующее условие:

$$\sum_{k_i}^{K_i} u_i\,(k_i) = 1, i = 0, 1, 2, \dots, I;$$

– $p_{i,l}$, i = 1,2, ..., J; l = 1,2, ..., L_j вероятности выбора альтернативных вариантов поведения в ходе деятельности планировщика, которые удовлетворяют условию полной группы несовместных событий:

$$\sum_{l=1}^{L_j} p_{j,l} = 1, j = 1,2, \dots, J,$$

где *j* – номер узла решения; L_j – число альтернативных вариантов поведения после решения *j*, *J* – число узлов решения;

– матрица инциденций для узлов разъединения и узлов соединения *A* размера (*n*x*n*), где *n* – общее число узлов разъединения и узлов соединения; $a_{i,j}$ = 0, если узлы не связаны через узлы действий; $a_{i,j}$ = 1, если *j*-му узлу предшествуют узлы действий, следующие в последовательности узлов после *i*-го узла; $a_{i,j}$ = –1, если узлы действий, предшествующие *i*-му узлу, следуют после *j*-го узла;

– спецификации всех узлов соединений, характеризующих взаимодействие действий в деятельности.

В предлагаемую методику анализа влияния структурной композиции на статистический профиль планировщиков включаются следующие этапы:

1. Формирование множества структурных композиций планировщиков.

2. Выбор исходной структурной композиции планировщика.

3. Построение расширенной объектно-ориентированной модели структурной композиции планировщика.

4. Преобразование расширенной объектно-ориентированной модели структурной композиции планировщика с помощью модифицированного метода свертки.

5. Определение динамических характеристик планировщика с выбранной структурной композицией по результатам преобразования его расширенной объектно-ориентированной модели.

6. Смена структурной композиции и переход к п. 3, если не проанализировано сформированное множество структурных композиций планировщиков.

7. Сравнительный анализ динамических характеристик сформированного множества структурных композиций планировщиков.

8. Выявление ключевых особенностей влияния структурной композиции на статистический профиль планировщиков.

При формировании расширенных объектно-ориентированных моделей планировщиков соблюдаются следующие принципы:

1) каждая модель ставится некоторому методу нелинейного планирования;

2) каждая модель описывается в контексте использования процедур обобщённого алгоритма планирования.

Благодаря предлагаемой методике создаются объективные предпосылки для развития методологических аспектов определения эффективности планировщиков интеллектуальных информационных агентов.

Список используемых источников

1. Системный анализ и принятие решений: Словарь-справочник. Учеб. пособие для вузов / Под ред. В. Н. Волковой, В. Н. Козлова. М. : Высш. шк. 2004. 616 с.

2. Птицына Л. К., Шестаков С. М. Информационные сети. Интеллектуальные информационные агенты : учеб. пособие. СПб. : Политехн. ун-т, 2008. 210 с. ISBN 5-7422-1728-5.

3. Птицына Л. К., Лебедева А. А. Модельно-аналитическое обеспечение информационных интеллектуальных агентов с динамической синхронизацией их действий // Наукоемкие технологии в космических исследованиях Земли. 2014. № 6. С. 68–71.

4. Птицына Л. К., Лебедева А. А. Аналитические компоненты информационной технологии формирования динамических характеристик запросов интеллектуальных агентов с подтверждением // Наукоемкие технологии в космических исследованиях Земли. 2015. № 1. С. 32–36.

5. Птицын А. В. Методологический базис агентных технологий для обеспечения информационной защищённости // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 1. С. 50–55.

6. Птицына Л. К., Лебедева А. А., Белов М. П. Формирование модельно-аналитического интеллекта для реактивных инфокоммуникационных сред // Международная конференция по мягким вычислениям и измерениям. 2016. Т. 1. № секции 1–3. С. 324–326.

7. Птицына Л. К. Интеллектуальные системы и технологии : учебное пособие. СПб. : СПбГУТ, 2019. 231 с.

УДК 02.026 (681.3)
ГРНТИ 20.53.01

АНАЛИЗ ЗАДАЧ, ФУНКЦИЙ И ПРИЗНАКОВ СОВРЕМЕННЫХ ЭЛЕКТРОННЫХ БИБЛИОТЕК

Е. С. Крюкова, И. Б. Паращук, А. В. Чернявский

Военная академия связи

Рассматриваются вопросы анализа признаков, свойств и особенностей современных электронных (цифровых) библиотек. Анализируются этапы их развития, достоинства, функции и задачи. Исследование проводилось с целью выявления и анализа существенных свойств данных объектов IT-инфраструктуры в интересах достоверного и многокритериального оценивания их качества и эффективности функционирования.

электронная библиотека, признак, документ, классификация, информационный ресурс, доступ.

Упоминания о первом, не всегда позитивном, опыте в создании и применении электронных библиотек (ЭБ) встречаются в отечественной и зарубежной литературе на рубеже конца 80-х – начала 90-х годов прошлого столетия. Первопроходцами в этой области можно по праву считать редколлегии научных журналов США и Великобритании, которые впервые, в рамках проектов своего эволюционного развития и конкурентной борьбы, создали цифровые платформы для размещения научный статей с открытым доступом к ним по каналам передачи данных. Это проекты носили названия «CORE», «Tulip» «Mercury», (1987–1993 гг.), проект «High Wire Press» (1995 г.), проект JSTORE (1995 г.) и другие. Создание этих цифровых платформ сыграло свою роль не только в науке, но и в финансово-экономической сфере – свободный онлайн-доступ к электронному фонду ключевых научных журналов позволил сократить расходы библиотек за счет исключения дублирования фондов (коллекций, контента). Положительный опыт создания электронных (цифровых) библиотек привел к тому, что многие научные журналы с середины 90-х годов прошлого века стали издаваться исключительно в электронной форме. К этому же времени относится и зарождение ЭБ в России, где появились проекты как для научных журналов, так и для других изданий. В частности, началась оцифровка коллекций Эрмитажа, редких рукописей в Российской Государственной Библиотеке, в Российской Национальной Библиотеке, Президентской библиотеке им. Б. Н. Ельцина и т. д.) [1].

Важность этого научно-технического направления возрастает и выходит на уровень государственной политики наряду и во взаимосвязи с расширением современного информационного пространства, расширением границ и ростом запросов информационного общества. Электронные библиотеки создаются не только в отдельных вузах и организациях, но и в учебных и научно-исследовательских организациях различных министерств и ведомств Российской Федерации [2, 3]. Электронные библиотеки на сегодняшний день занимают такое же важное место в ряду современных и перспективных информационных систем, развертываемых в интересах силовых ведомств, как и информационные системы управления войсками и оружием. Так, благодаря неоспоримым достоинствам этих систем, осуществляется и находится под постоянным контролем Министра обороны проект по созданию единой ЭБ образовательных и научно-исследовательских организаций Вооруженных сил РФ в рамках проекта «Электронный ВУЗ» [4]. Электронная библиотека – это распределенная, взаимоувязанную по целям и задачам, емкая и мощная информационная система, предназначенная для организации и хранения систематизированного фонда электронных объектов, а также организации и обеспечения доступа к ним с помощью единых для всех средств навигации и поиска. Она призвана, через общие и ведомственные (иногда закрытые) сети передачи данных, в удобном для конечного клиента (читателя) виде, надежно сохранять и рационально использовать многообразные и разноплановые коллекции электронных документов, базы данных, справочные и поисковые платформы, а также иные информационные ресурсы [2, 3]. Более того, ЭБ сама по себе уже представляет собой систематизированную совокупность электронных информационных ресурсов. Эти ресурсы организованы и упорядочены по «библиотечному принципу» на основе современных автоматизированных библиотечных технологий и программ, имея целью повышение эффективности и качества библиотечно-информационного обслуживания зарегистрированных пользователей. Показателями качества могут служить: уровень книгообеспеченности образовательного процесса в ВУЗе, степень внедрения современных информационных технологий в практику библиотечно-информационного обслуживании, своевременность (оперативность) доступа зарегистрированных пользователей к электронному библиотечному фонду (контенту), количество качественно новых способов работы с большими объемами информации, уровень доступности книг и других электронных документов, а также интервал (длительность по времени, срок) хранения электронных документов.

Задачи ЭБ определяются целями ее функционирования, направлены на интеграцию информационных ресурсов, эффективную навигацию в них и заключаются в обеспечении безусловных и своевременных: сбора (комплектования фонда), формирования, обработки, систематизации, хранения

и доступа зарегистрированных пользователей к электронным документам и базам данных [2, 5].

К достоинствам ЭБ можно отнести работу с электронными объектами фонда не только в режиме просмотра изображений или чтения документов, но и в режиме полноценного редактирования контента. Помимо этого, легальный (авторизированный) пользователь получает оперативный доступ к разнообразным электронным объектам фонда ЭБ, невзирая на время суток и местонахождение. Расширяется диапазон предоставления библиотечно-информационного обслуживания, поскольку издания, которые есть в наличии в библиотеках в небольшом количестве, иногда в единственном экземпляре, могут быть доступны большему числу пользователей [2, 5].

Важным достоинством ЭБ также является тот факт, что их создание (развертывание) не потребует больших затрат времени и средств. Но даже вложенные затраты быстро окупаются, благодаря широкому внедрению в ЭБ новейших технологий, обеспечивающих оперативный доступ к огромному объему информационных ресурсов на качественно новом уровне.

Сегодня не существует канонической признаковой типологии и систематизации электронных библиотек, адекватно учитывающих их особенности и разнообразие их параметров, нет общепринятой классификации ЭБ. Нами предлагается вариант формулировки классификационных признаков. При этом под «признаком» понимается достаточное условие для принадлежности объекта некоторому классу, а под понятием «свойство» понимается атрибут объекта (предмета, процесса).

Основные классификационные признаки ЭБ, на наш взгляд, должны быть тесно связаны с опциями (функционалом), реализуемыми ими. При этом, в рамках формирования классов ЭБ, предполагается, что эти объекты подразделяются на ЭБ, реализующие научно-исследовательские, образовательные, информационные, просветительные, справочные опции а также опции (функционал) сохранения творческого наследия [2, 3, 5].

Предлагаемый вариант формулировки существенных свойств и признаковой классификации ЭБ сделан с учетом объективно сформулированных свойств и признаков этих систем, их современной специфики и ситуаций, в которых они функционируют, а также аспектов, связанных с процедурами автоматизации управления их ресурсами.

Так, по признаку состава хранимых документов, различают библиотеки, чей фонд организован из однотипных электронных документов (монодокументные ЭБ), и библиотеки, чей фонд – комплексное собрание мультимедийных электронных объектов (полидокументные ЭБ).

Базовым признаком электронных библиотек является цель их создания и функционирования. С точки зрения этих целей, ЭБ бывают: мемориальные – здесь создается фонд документов, посвященных конкретному лицу или событию; учебные или учебно-методические – создан фонд документов,

нацеленных на поддержку образовательного процесса; справочные – фонд документов имеет энциклопедическую направленность и универсальный состав для получения необходимой краткой информации по максимальному количеству отраслей знаний; художественные – фонд документов состоит, в основном, из художественных литературных произведений; просветительские – здесь создается фонд научно-популярных документов, которые способны осветить изучаемый предмет на популярном общеобразовательном уровне, не требующем академических знаний; научные – создан фонд документов, ориентированных на глубокое изучения предмета (темы) профессионалами, научными работниками и иными специалистами; смешанные – фондом такой электронной библиотеки могут быть общие информационные ресурсы, не ориентированные на какое-либо конкретное предназначение (предмет, тему).

Электронные библиотеки организовываются, в основном, несколькими способами: электронные документы создаются держателями фонда этой библиотеки (генерируемые ЭБ), электронные документы собираются из уже существующих, готовых электронных публикаций или коллекций документов (агрегируемые ЭБ), а также, так называемые, смешанные ЭБ, состоящие частично заимствованных изданий, частично из созданными своими авторами (держателями фонда).

С точки зрения организации и архитектуры, электронные библиотеки бывают или независимыми, или «вмонтированными» в тотальный, всеобщий ресурс, например, в систему дистанционного обучения или научно-образовательный комплекс, или интегрированными, как, например, в большей части виртуальных библиотек – фонды объединены общей тематикой и единым интерфейсом, но электронные документы находятся на различных электронных порталах.

В современных условиях признаки, характеризующие источники финансирования процессов создания и функционирования ЭБ, а также материально-финансовые аспекты доступа к их ресурсу, являются, порою, ключевыми. Различают библиотеки, традиционно финансируемые за счет бюджета (государственные ЭБ) и финансируемые, для удовлетворения своих потребностей, за счет частных лиц или коммерческих компаний (негосударственные ЭБ). При этом бывает, что с пользователей взимается оплата за доступ к фонду библиотек (платные ЭБ) или доступ предоставляется на безвозмездной основе (бесплатные ЭБ).

По признаку языковой принадлежности различают одноязычные и многоязычные библиотеки, первые из них используют в интерфейсах ЭБ поддержку одного языка, другие – нескольких языков.

Анализ признаков защищенности ресурса ЭБ позволяет говорить о разделении их на два класса – защищенные и незащищенные (открытые).

К первым относят ЭБ, приспособленные противодействовать несанкционированному доступу к их ресурсам, их уничтожению, нарушению целостности, копированию и модификации. Незащищенные (отрытые) ЭБ обеспечивают открытый доступ к своим ресурсам.

Признаки ЭБ, указывающие на способ их использования, дают основания разделить их на частные ЭБ, в которых их фонд доступен для ограниченного круга лиц в пределах ограниченной территории и объединенные – фонды (электронные ресурсы) различных ЭБ, как правило, территориально распределенных, объединены в общий единый фонд и используются определенным кругом лиц.

С точки зрения организации доступа важно рассмотреть два аспекта: есть ЭБ, где требуется регистрация пользователей (оф-лайн ЭБ) и те, где регистрация не нужна (он-лайн ЭБ). Признаки, определяющие механизм распределения доступа к фондам ЭБ позволяют говорить о существовании ЭБ ограниченного доступа – ресурс библиотек предоставляется ограниченному кругу лиц и ЭБ общего доступа – доступ к ресурсам библиотек имеют все пользователи в равной степени [2, 5].

Способ наполняемости информационного ресурса ЭБ является одним из существенных их признаков, значит можно предположить, что существуют следующие классы: ЭБ без возможности добавления новых ресурсов – пользователь не имеет права добавлять новые электронные объекты, пополнять фонд библиотеки; ЭБ с ограничением добавления новых ресурсов – добавлять новые электронные объекты и пополнять фонд имеет право ограниченный круг лиц; ЭБ без ограничения добавления новых ресурсов – добавлять новые электронные объекты и пополнять фонд имеет право любой легальный (авторизированный) пользователь.

Таким образом, проведен анализ задач, функций и свойств ЭБ, однако предложенная их признаковая классификация не является полной и открыта для дополнений. Вместе с тем, результаты анализа и формулировки признаков уже на этом этапе исследований облегчают принятие решения по выбору необходимой системы показателей качества ЭБ.

Проведенный обзор и анализ классификационных признаков позволяет выявить и формализовать существенные свойства электронных библиотек, как важных элементов IT-инфраструктуры, что, в свою очередь позволит повысить достоверность оценивания их качества и эффективности функционирования.

Список используемых источников

1. Антопольский А. Б., Маркарова Т. С., Крюкова О. П., Харламов А. А. Электронные библиотеки в образовании / Под редакцией О. П. Крюковой, А. А. Харламова. М. : 2009. 94 с.

2. Национальный стандарт Российской Федерации ГОСТ Р 7.0.96 - 2016. Электронные библиотеки. Основные виды. Структура. Технология формирования. М. : Стандартинформ, 2016. 13 с.

3. Зуйкина К. Л., Соколова Д. В., Скалабан А. В. Электронные библиотеки в России. Текущий статус и перспективы развития. М. : Ваш формат, 2017. 120 с.

4. Электронная библиотека Министерства обороны РФ (2019) [Электронный ресурс]. URL: http://mil.ru/departament_informashion_system/activity/ellib.htm (дата обращения: 30.10.2019).

5. Крюкова Е. С., Паращук И. Б. Особенности развития современных электронных библиотек и анализ подходов к оцениванию их качества. // Современные технологии: актуальные вопросы, достижения и инновации: Сборник статей XXXI Международной научно-практической конференции. Пенза: МЦНС «Наука и Просвещение». 2019. 54 с., С. 34–36.

УДК 004.75
ГРНТИ 81.93.29

АКТУАЛЬНЫЕ УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

А. А. Кузькин, М. А. Куцакин, В. В. Рябоконь

Академия ФСО России

В статье представлен пример актуальных уязвимостей и ошибок в программном обеспечении, базирующихся на метриках и классификации уязвимостей OWASP. При этом учитываются множество различных путей использования уязвимостей, которые могут различаться по сложности поиска и эксплуатации уязвимостей, а также по степени риска. Приведены актуальные данные по наиболее опасным дефектам программного обеспечения и обозначены наиболее общие подходы к повышению защищенности программ от перечисленных уязвимостей.

информационная безопасность, программное обеспечение, уязвимости.

Объективные причины появления уязвимостей в программных продуктах заключаются в чрезвычайно высокой структурной сложности программного кода, динамичности развития версий и легкости модификации кода. Несмотря на усилия ведущих мировых разработчиков программного обеспечения, задача снижения числа уязвимостей в программных системах не получила реального решения.

Помимо человеческого фактора, который по-прежнему составляет большую долю в успешно реализованных компьютерных преступлениях,

уязвимости и дефекты программного обеспечения прочно удерживают позиции второго по значимости фактора. Актуальность проблемы наличия уязвимостей обуславливается:

– ростом числа хакерских атак, эксплуатирующих открытые уязвимости операционных систем и сервисов;

– значительным усложнением самого программного обеспечения;

– развитием средств защиты информации, что усложняет метод взлома системы «в лоб»;

– возрастанием значимости и ценности информации различной степени конфиденциальности.

В российской нормативной базе имеется ряд определений отдельных классов уязвимостей, а именно: программной закладки (ГОСТ Р 50.1.053-2002), скрытого канала (ГОСТ Р 53113.2-2009), бреши/уязвимости (ГОСТ Р 50922-2006) и недекларированных возможностей (НДВ) (руководящий документ ФСТЭК России). В частности, в РД ФСТЭК России недекларированные возможности трактуются как функциональные возможности ПО, не описанные в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации. Программные закладки являются реализацией недекларированных возможностей, т. е. преднамеренными уязвимостями инициируемого типа [1]. Одна из возможных классификаций уязвимостей представлена на рис. 1.

Вопросами выявления уязвимостей и сертификационных испытаний программного обеспечения занимаются испытательные лаборатории Минобороны, ФСБ и ФСТЭК России, однако существующая нормативная, методическая и инструментальная база выявления недекларированных возможностей в программном обеспечении не позволяет эффективно обеспечивать безопасность программ. Например, в отличие от средств антивирусного контроля, отсутствуют средства гарантированного выявления программных закладок в структурно сложном программном обеспечении. Отсутствуют разработки математического аппарата для оценки степени безопасности программного обеспечения, основанного на сертификационных испытаниях с целью подтверждения отсутствия программных закладок. К этому можно добавить проблему достоверной идентификации преднамеренно созданных программных закладок, несовершенство нормативно-методической базы и отставание инструментальной базы сертификационных испытаний.

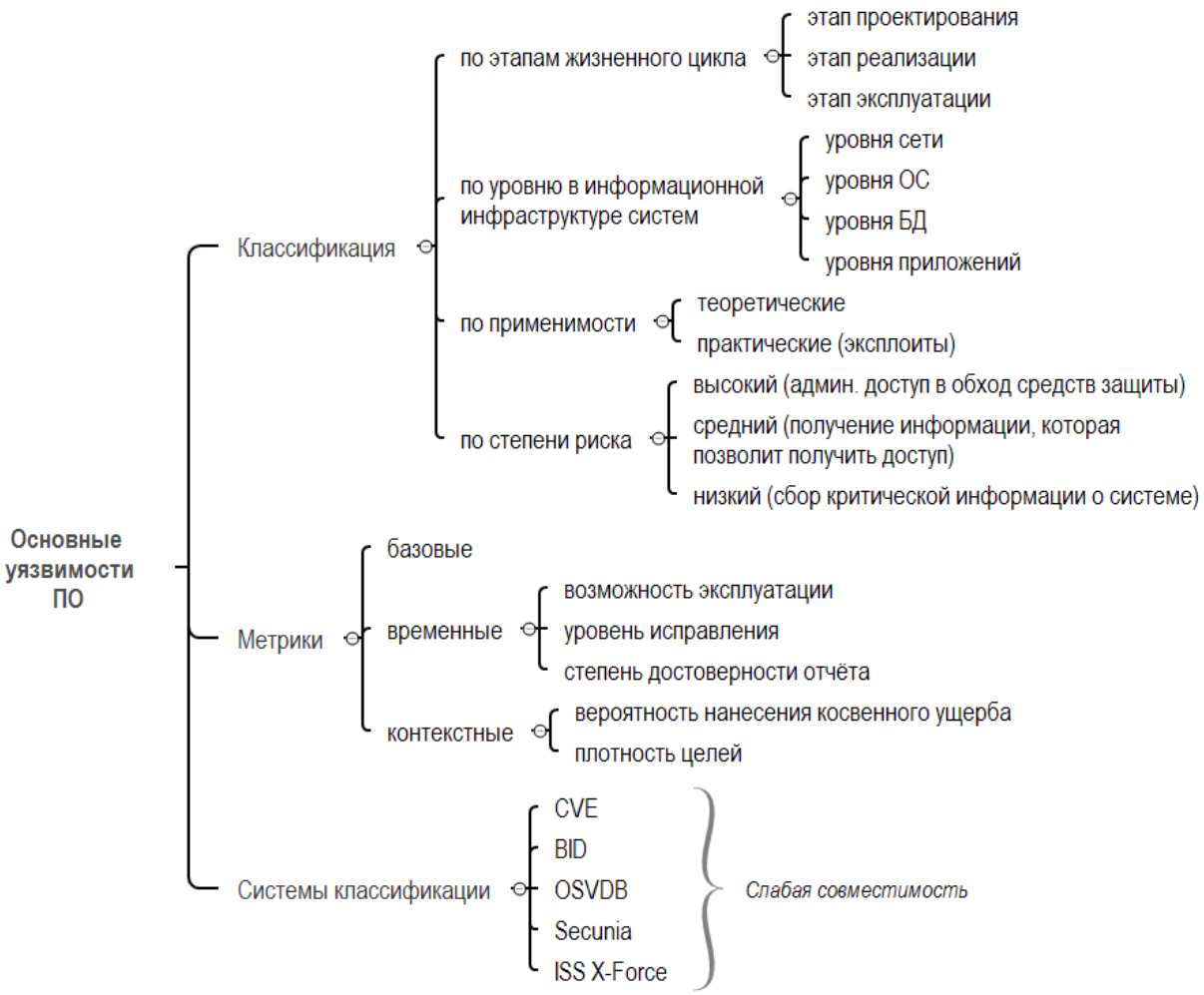


Рис. 1. Классификация и метрики уязвимостей ПО

В настоящее время популярен ряд международных классификаций и таксономий, ориентированных на категории угроз ИБ, наиболее известной из которых является OWASP [2]. Классификация OWASP определяет множество классов критических уязвимостей веб-проектов, например: инъекции, межсайтовый скриптинг, нарушения аутентификации и управления сессиями, незащищенная прямая ссылка на объект, подделка межсайтовых запросов, некорректная конфигурация настроек безопасности, незащищенное хранилище криптографических объектов, ошибки ограничения доступа, недостаточная защита транспортного уровня, некорректные перенаправления и пересылки.

Обычно уязвимость позволяет атакующему «обмануть» приложение – заставить его совершить действие, на которое у того не должно быть прав. Это делается путем внедрения каким-либо образом в программу данных или кода в такие места, что программа воспримет их как «свои». Некоторые уязвимости появляются из-за недостаточной проверки данных, вводимых поль-

зователем, и позволяют вставить в интерпретируемый код произвольные команды. Другие уязвимости появляются из-за более сложных проблем, таких как запись данных в буфер без проверки его границ (переполнение буфера).

При этом нарушители потенциально могут использовать множество различных путей посредством приложений, которые приводят к различным рискам (рис. 2).

Рис. 2. Риски безопасности ПО

Такие пути могут различаться по сложности поиска и эксплуатации уязвимостей, а также по степени риска [3].

Актуальный список самых опасных ошибок OWASP с кратким описанием представлен в таблице. Распределение мест в списке из года в год изменяется по причине своевременного обнаружения и исправления некоторых типовых уязвимостей ПО. Например, в 2013 году XSS-уязвимости (межсайтовый скриптинг) в списке занимали 3-е место, а уже на 2017 год уязвимости типа XSS составляли 26 % и занимают первое место среди остальных уязвимостей по статистическим данным. Причиной этого являлось то, что некоторое время программисты и разработчики ПО не уделяли им должного внимания, считая их неопасными. Однако это мнение оказалось ошибочным: на веб-странице или в HTTP-Cookie могут быть весьма уязвимые данные (например, идентификатор сессии администратора или номера платёжных документов).

ТАБЛИЦА. Список наиболее опасных уязвимостей по классификации OWASP

Название	Описание
Инъекция	SQL инъекция может дать возможность атакующему выполнить произвольный запрос к базе данных, получить возможность чтения и/или записи локальных файлов и выполнения произвольных команд.
Нарушение аутентификации	Реализованная подсистема авторизации пользователей не выполняет или выполняет некорректно проверки, связанные с доступом к ресурсам.

Название	Описание
Разглашение важных данных	Утечка сведений о системе или личных данных пользователей (некорректная защита финансовых или личных данных).
Внешние сущности XML (XXE)	Устаревшие или плохо сконфигурированные обработчики (процессоры) XML могут некорректно обрабатывать внешние по отношению к XML-документу объекты.
Нарушение контроля доступа	При неверной реализации контроля доступа аутентифицированные пользователи могут получить незапланированный доступ к данным, возможности по модификации данных и изменения прав доступа.
Неверная конфигурация безопасности	Неверные с точки зрения безопасности конфигурации по умолчанию, своевременное обновление программного обеспечения, применение патчей и обновлений безопасности.
XSS – Cross Site Scripting	Внедрение выполняемых на клиентском компьютере вредоносных скриптов в выдаваемую системой страницу, для атаки на сервер используется авторизованный на этом сервере клиент.
Небезопасная десериализация	Десериализация вредоносных или поддельных объектов, предоставленных злоумышленником, что может привести к удаленному выполнению кода.
Использование компонентов с известными уязвимостями	При использовании устаревших версий ПО, его компонентов или библиотек без своевременных обновлений безопасности возникает риск существования готовых к распространению и использованию эксплоитов, эксплуатирующих обнаруженные в этом ПО уязвимости.
Недостаточный мониторинг и аудит безопасности	Отсутствие журналов о попытках аутентификации, о предупреждениях и ошибках, выдаваемых приложениями, или недостаточность информации в них, а также отсутствие отслеживания подозрительной активности и своевременного уведомления администраторов об инцидентах безопасности.

Базовыми методами контроля, определенными в [1] являются статический и динамический анализ исходных текстов программ. В общем случае для реализации совокупности методов статического и динамического анализа аккредитованные сертификационные центры и лаборатории применяют варианты инструментария верификации и валидации (V&V), принцип организации которого представлен на рис. 3 (см. ниже).

При этом наиболее общими подходами к повышению защищенности ПО от перечисленных уязвимостей являются:

– формирование требований к безопасности приложений по стандартам верификации безопасности приложений (ASVS);

– формирование архитектуры безопасности приложений, позволяющей внедрять средства безопасности с самого начала разработки;

– стандарты безопасности, позволяющие контролировать разработку приложений;

– цикл безопасной разработки приложений, обеспечивающий контроль безопасности на всех этапах жизненного цикла ПО.

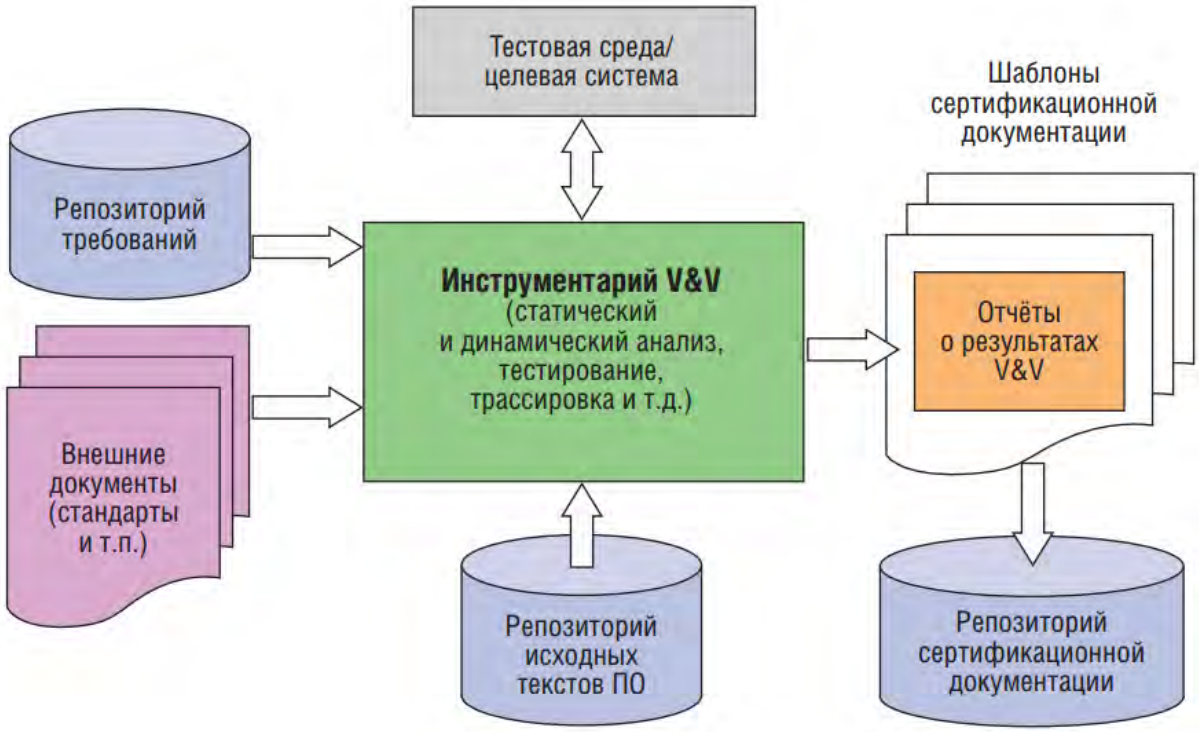


Рис. 3. Обобщенная схема организации инструментария верификации и валидации программного обеспечения

Список используемых источников

1. Руководящий документ ФСТЭК России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.

2. Проект OWASP Top 10 [Электронный ресурс]. URL: https://www.owasp.org/ (дата обращения: 26.11.2019).

3. Методология оценки рисков OWASP [Электронный ресурс], URL: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology (дата обращения: 26.11.2019).

УДК 004
ГРНТИ 81.01.07

ОБЛАЧНЫЕ ТЕХНОЛОГИИ. ДОСТОИНСТВА И НЕДОСТАТКИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Д. С. Кукунин, Е. А. Маслова, С. С. Шумилов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрено внедрение весьма занимательной и перспективной технологии – cloud technologies или в простонародье – «облако» в IT-инфраструктуру бизнес-организаций. В статье раскрыто само понятие облачных технологий. Приведены основные три модели обслуживания облачных технологий, собственно, разобрана их классификация. В статье также представлены основные достоинства и недостатки облачных технологий. Тема достаточно важная и актуальная в наше время, так как большинство сервисов и бизнес-процессов уже работают или уходят на удаленные сервера и облачные хранилища.

cloud technologies, «облако».

В наш век информационных технологий, вместе со стремительным развитием средств связи, в частности глобальной сети Интернет, в геометрической прогрессии растёт количество передаваемой информации. В сегодняшних реалиях, структура хранения и передачи данных претерпевает серьёзные изменения, так, всё больше информации хранится не в огромных датацентрах, а, как правило, в облаке. Интересно, что на общепринятых схемах компьютерных сетей Интернет изображён именно в виде облака, основной задачей которого является передача данных от одного компьютера к другому вне зависимости от их расстояния (рис.).

Рис. Схема компьютерной сети

Увеличение количества и скорости информационных потоков, непрерывное совершенствование электронных гаджетов, а также стремительно растущие потребности пользователей – всё это, несомненно, приводит к развитию сети Интернет. К примеру, уже не первый год при решении производственных задач используются технологии виртуализации данных. Следовательно, появилась возможность передать облаку решение более

сложных задач, например, таких как перенос части бизнес-процессов организации на удалённые серверы или использование вычислительной мощности больших дата-центров несколькими предприятиями. Таким образом, появилось новое понятие облачных технологий или облачных вычислений.

Облачные вычисления (англ. *cloud computing*) – модель обеспечения удобного сетевого доступа по требованию к некоторому общему фонду конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам – как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру [1]. Возможности реализации правил облачных вычислений в производственной среде объединяют понятием «облачные технологии». Здесь нам предстоит рассмотреть возможности реализации принципов облачных технологий.

По уровням облачных вычислений различают 3 модели обслуживания облачных технологий [1, 2, 3, 4, 5, 6]:

- Инфраструктура как услуга (англ. *Infrastructure as a service,* IaaS) предлагается как возможность пользователя самостоятельно управлять базовыми вычислительными ресурсами (обработка и хранение данных, управление сетевыми сервисами, операционными системами и приложениями) на облачной инфраструктуре провайдера.
- Платформа как услуга (англ. *Platformasaservice,* PaaS) предполагает предоставление пользователю возможности использования облачной инфраструктуры провайдера с предустановленной операционной системой для последующего развертывания на нем приложений.
- Программное обеспечение как услуга (англ. *Softwareasaservice,* SaaS) предлагает потребителю использовать прикладное программное обеспечение провайдера, реализованное в облачной инфраструктуре провайдера (физическая среда, развернутые операционные системы).

В системе облачных структур по степени виртуализации IaaS считают низшим уровнем, здесь виртуальной для пользователя является только физическая среда организации вычислений. Средним уровнем является PaaS, к виртуальной физической среде добавляется среда развёртывания операционной системы. Высшим уровнем облачных вычислений принято считать *SaaS*, в котором физическая среда, операционная система, а также приложения являются полностью виртуальными для пользователя.

Достоинства и недостатки облачных технологий

Достоинствами облачных технологий являются [2]:

•Доступность. Она обусловлена возможностью получения доступа к информации или приложениям, хранящимся в облаке, пользователю, имеющему электронное вычислительное устройство (компьютер, телефон, планшет и т. д.), подключённому к сети Интернет.

•Экономичность. Пользователю теперь нет необходимости покупать и эксплуатировать большие по вычислительной мощности системы и сопутствующее программное обеспечение для них. Так же отпадает потребность в специалистах для их обслуживания. Всё это приводит к существенному сокращению затрат и, соответственно, экономию средств.

•Мобильность. В любом месте, где есть точка доступа к Интернету, пользователь, посредством имеющегося в его распоряжении гаджета, может организовывать рабочий процесс. Следовательно, в разы возрастает удобство производства, так как больше нет строгой привязки к определённому рабочему месту.

•Высокая технологичность. Огромный пласт вычислительных мощностей, используемых для обработки, анализа и хранения данных находится под контролем пользователя.

•Масштабируемость. Пользователь получает подходящий пакет услуг под решение задач, определённых им самим. По сути, оплата производится только за необходимые функции.

•Надёжность. Сегодня, безусловно, облачные сервисы имеют более надёжную и безопасную инфраструктуру, чем компьютерная сеть организации. В облаке реализован достаточный уровень резервирования, при этом на создание резервной копии и восстановление по запросу выделяются необходимые ресурсы.

Основные недостатки облачных технологий [6]:

•Монополия провайдера. Весомую роль в определении направления деятельности бизнес-организации занимает выбор и внедрение конкретного IT-решения. Как правило, это весьма трудоёмкая, поэтапная операция, требующая существенного вложения средств. Неправильный выбор IT-решения с высокой долей вероятности подвергнет организацию огромному риску и стрессу, посредством существенного увеличения финансовых расходов, что может привести к краху организации в условиях малого бизнеса.

•Неконтролируемые изменения. На сегодняшний день, скорость внедрения обновлений определяет качество программных продуктов. IT-инфраструктура представляет собой динамично развивающуюся систему, следовательно, тот набор функций, с которым работает пользователь, претерпевает множество доработок и изменений. На этой почве между пользо-

вателем и провайдером могут возникнуть разногласия, так как не всегда существует общее представление между ними о том, какие именно обновления необходимы на определённый момент времени.

•Увеличение стоимости. Как было отмечено ранее, экономичность является одним из достоинств использования облачных технологий. Действительно, на этапе запуска так и есть, в особенности, если необходимо приступить к работе в сжатые сроки. Но, как правило, на начальном этапе становления организации сложно спрогнозировать темпы и объёмы её развития. Следовательно, параллельно будут увеличиваться и требования к облаку, в частности, его «объёму». Зачастую, расширение облачного сервиса провайдером обходится пользователю в немалую сумму.

•Негарантированный доступ. Для того чтобы использовать функционал облака, пользователю необходим доступ к сети Интернет. Как показывает практика, и провайдер и пользователь не застрахованы на 100 процентов от аварийных ситуаций, периодически возникающих от программных сбоев сетевых маршрутизаторов, на устранение которых необходимо несколько часов, до обрывов оптико-волоконных линий, на восстановление которых может потребоваться несколько суток. Использование облачных сервисов, в данных условиях, не представляется возможным.

•Стандартный набор функций. Разработчики облачных сервисов предлагают определённый набор функций, ориентированный на некоторые «средние» бизнес-проекты. Для начинающих организаций внедрение необходимых ей функций может оказаться для них весьма дорогим, а для крупных компаний с богатой историей и опытом предложенного функционала, наоборот, будет недостаточно для его внедрения и ведения бизнеса.

•Конфиденциальность. Провайдеры облачных сервисов хранят огромное количество данных своих пользователей, заметно превышающее объём локальных сетей небольших организаций, тем самым привлекая большее количество атак злоумышленников. Следовательно, наиболее остро встаёт вопрос кибербезопасности – одной из самых основных задач, которая должна совершенствоваться Интернет-сообществом.

•Сохранность. Архитектура ЦОД, словно другим зданиям и сооружениям, подвержена риску стихийных бедствий. Так, известен случай, когда в августе 2015 года молния 4 раза ударила по дата-центру Google в Бельгии. Часть данных пользователей была безвозвратно утеряна, несмотря на систему резервного копирования и высокую энергозащищенность.

Таким образом, сегодняшняя технологическая парадигма полностью оправдывает внедрение облачных систем в обиход организаций совершенно разного уровня. Существует ряд инструментов и возможностей, которые позволяют использовать облачные технологии на максимальную мощность, принося огромную пользу как бизнесу, так и обычным пользователям, не-

смотря на существующие недостатки и возможные угрозы. В наиболее выгодной ситуации находятся организации “среднего” уровня, имеющих стандартную структуру, для которых эффективно работать помогут облачные сервисы модели SaaS. В случае, если бизнес-предприятие представляет собой широкую сеть, обладающей большим оборотом данных - облачные сервисы модели IaaS объединят деятельность отдельных подразделений в общем информационном пространстве, тем самым делая её более удобной и прозрачной.

Список используемых источников

1. Облачные вычисления // Википедия. Свободная энциклопедия: сайт. URL: ru.wikipedia.org/wiki/Облачные_вычисления

2. Глазунов Сергей. Бизнес в облаках. Чем полезны облачные технологии для предпринимателя. // Журнал СКБ Контур. URL: https://kontur.ru/articles/225, URL: https://www.cta.ru/cms/f/448405.pdf

3. Черняк Леонид. Интеграция – основа облака // Журнал Открытые системы. СУБД. URL: https://www.osp.ru/os/2011/07/13010473

4. Обзор: Облачные сервисы 2017 // Журнал в сфере высоких технологий Cnews. URL: http://www.cnews.ru/reviews/cloud2017

5. Соловьев Сергей. Десять рисков «облачных» IT-решений // Журнал Executive.ru. URL: www.e-xecutive.ru/management/itforbusiness/1984811-desyat-riskovoblachnyh-it-reshenii

6. Браггер Ева. Собираетесь в облака? Возьмите с собой парашют! // Журнал Executive.ru. URL: www.e-xecutive.ru/management/itforbusiness/1986007-sobiraetes-v-oblakavozmite-s-soboi-parashut

УДК 621.391
ГРНТИ 49.13.01

ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ СИГНАЛИЗАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

В. И. Курносов, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются способы управления комплексами аппаратно-программных средств телекоммуникационной системы на основе ресурсосберегающих технологий и особенности функционирования ее системы управления. Предложена обобщенная модель информационно-логических трактов взаимодействующей в системе подсистем сигнализации и управления. Представлена модель сетевой службы по обеспечению взаимодействия подсистем. Приведены результаты исследований организации построения

сети обмена данными системы управления телекоммуникационной системой и вероятностно-временных характеристик информационного обмена.

телекоммуникационная система, система сигнализации, сеть обмена данными, вероятностно-временные характеристики.

Исследования способов управления комплексами аппаратно-программных средств телекоммуникационной системы (ТКС) на основе ресурсосберегающих технологий, основные результаты которых представлены в [1], показывают, что качество формируемого сетевого ресурса транспортной сети ТКС во многом определяется возможностями и характером функционирования ее системы управления (системы управления связью, СУС). В [2, 3, 4, 5] обосновано, что эффективность функционирования СУС определяется порядком построения и эксплуатацией ее подсистем (рис. 1), среди которых особое значение отводится системам сигнализации (СС).

В интересах СУС посредством ее СС в ТКС осуществляется обмен сигнально-управляющими сообщениями, которые содержат информацию о состоянии коммутационных центров, объемах выполненных сетевых услуг, ориентированных и неориентированных на соединения, которые поддерживают процессы взаимосвязи между сетями доступа ТКС с различными технологиями функционирования [4]. Особенностью СС в мультисервисных сетях ТКС является реализация пакетного обмена сигнально-управляющей информацией сигнальными единицами (СЕ). К передаче и доставке СЕ предъявляются жесткие требования, что, с учетом развитой архитектуры общеканальной сигнализации (ОКС), позволяет применять ее в СУС ТКС в качестве единой сети обмена данными (СОД). Это налагает дополнительные требования к процедурам проектирования СУС ТКС, которые должны учитываться в [5], поэтому достаточно актуальным является решение подобной задачи.

Рассмотрим модель образования сетевой службы для обеспечения взаимодействия элементов ТКС при использовании различных телекоммуникационных технологий, в которых доставка сигнально-управляющей информации в интересах СУС осуществляется посредством коммутируемых сигнальных единиц (КИЕс). Так как в мультисервисной ТКС коммутационные узлы пунктов сигнализации (ПС) могут устанавливаться на всех СУ, центрах коммутации (ЦК) то, это позволяет для динамической маршрутизации КИЕс использовать третий уровень подсистемы передачи информационных сообщений (ИС) (MTP) или подсистему управления сквозными соединениями (SCCP) [3, 6]. В этом случае возможно использование всех четырех классов протоколов SCCP, включая контроль последовательности и управлением потоком КИЕс. Следовательно, на основе СС в интересах СУС можно построить унифицированную сеть обмена данными (СОД) в транспортной сети ТКС.

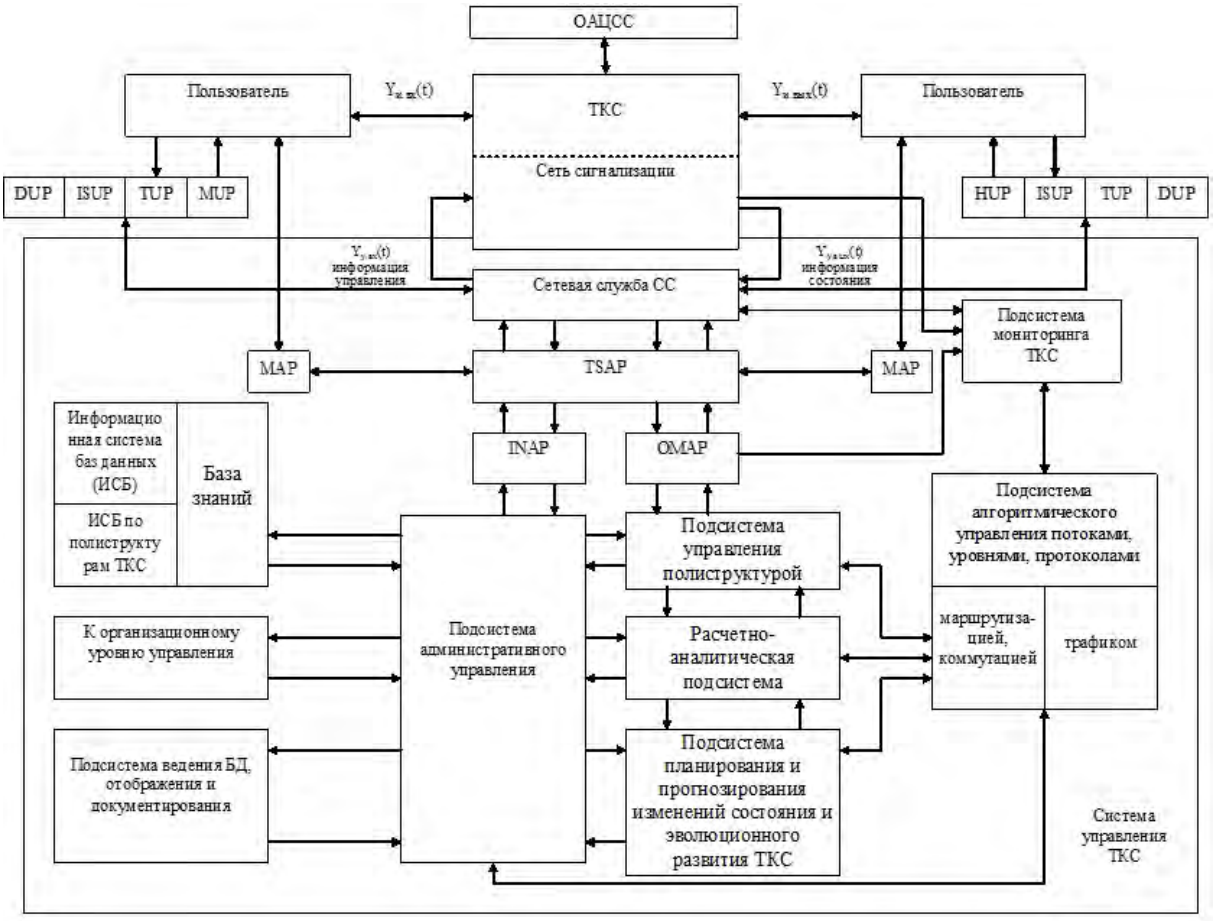


Рис. 1. Обобщенная функциональная схема взаимодействия подсистем сигнализации и управления ТКС

Одним из основных принципов организации построения СОД является квазисвязанный режим. При его использовании для каждого передаваемого между пользователями сигнального потока формируется отдельное физическое или логическое соединение в сетевой службе и обеспечивается возможность разграничения пользовательского доступа, что позволяет реализовать выполнение неоднородных требований к качеству услуг, поддерживаемых СУС ТКС.

Для повышения надежности доставки КИЕс в СОД используют альтернативную маршрутизацию, которая автоматически переключает поток сигнально-управляющих сообщений на резервное соединение при отказе основного. Резервное и основное соединения проходят по разным физическим линиям ТКС, которые заблаговременно сформированы на стадии проектирования ТКС по результатам синтеза топологической и потоковой структуры ТКС (выражения (2.74) и (2.75) в [4]).

Управление потоками сигнально-управляющих сообщений в СОД основано на задании для каждого сигнально-управляющего соединения согласованной скорости передачи сообщений (CIR) [3, 7]. Параметры CIR определяются двумя характеристиками: согласованным объемом КИЕс (Bc),

необходимым для передаваемой информации, и избыточным объемом КИЕс (Ве), который соответствует максимальному числу битов, превышающих значение Вс, которые могут быть переданы по сигнальному соединению без обеспечения гарантии их передачи. Это позволит передавать неоднородный поток сообщений различной важности, срочности и длины. Ряд вопросов для комбинированной СОД требует дополнительных исследований с оценкой вероятностно-временных характеристик (ВВХ).

Характер функционирования СС и СУС показывает, что поток сигнально-управляющих сообщений будет неоднородным и для его описания необходимо задавать как ВВХ (функции распределения длин интервалов между моментами поступления сигнально-управляющих сообщений и параметров этого распределения), так и характеристики важности, срочности и длины сигнально-управляющих сообщений.

В общем случае среднее время передачи сообщений $T_{\text{су}}$ посредством КИЕс между двумя оконечными пунктами сигнализации может быть определено из выражения:

$$\overline{T_{\text{су}}} = \overline{T_{\text{су}_a}} + \sum_{i=1}^{n+1}(\overline{Q_t} + \overline{Q_a}), \quad (1)$$

где $T\text{су}_a$ – среднее время передачи сообщения при отсутствии искажения в КИЕс, которое зависит от среднего времени передачи сообщений в исходящем, транзитном и оконечном пункте СС (СУС), а также от среднего времени распространения КИЕс по звену сигнализации; n – количество транзитных пунктов сигнализации (ТПС); Q_t и Q_a – средняя задержка, за счет очередей сигнально-управляющих сообщений с искажениями и без искажений в КИЕс соответственно.

Параметры составляющих в (1) зависят от качества цифрового канала для КИЕс, длины КИЕс и от сложности протоколов, реализующих обмен КИЕс в звене сигнализации.

Вероятность своевременной доставки сигнальных сообщений можно оценить с применением многофазной модели массового обслуживания. Выражение для оценки вероятности своевременной доставки сообщений СС и СУС ТКС в СОД, для типового варианта сигнального соединения, можно представить в виде:

$$P\left(t \le t_{\text{a}_{ij}}\right) = P_f^2 \prod_{i=1}^{n} P_i, \quad (2)$$

где P_f – вероятность своевременной обработки сообщения на устройстве сигнально-управляющего доступа; P_i – вероятность своевременной обработки сообщения на i-м коммутационном устройстве ПС или ТПС, которые зависят от интенсивностей входного потока и обслуживания КИЕс, произ-

водительности устройства доступа, коэффициентов оперативной готовности, оперативного простоя и интенсивности восстановления элементов СС и СУС.

Зависимость длины СЕ от качества канала связи определяется как:

$$L(P_{\text{ош}}) = M[\tau_0]v/(1 + M[\tau_0]P_{\text{ош}}v\ , \quad (3)$$

где v – скорость передачи КИЕс; $M[\tau_0]$ – математическое ожидание КИЕс в СОД, которое рассчитывается как:

$$M[\tau_0] = \tau_u/(1-\rho)(1-Q), \quad (4)$$

где Q – вероятность ошибки в КИЕс; τ_u – длительность КИЕс; $\rho = d/\eta$ – приведенная плотность потока сигнально-управляющих сообщений.

Вероятность появления в КИЕс длиной из n элементов j и более ошибок для канала с независимыми ошибками определяется как в [6, 7]:

$$Q(j \le n) = \sum_{i=j}^{n}(nP_{\text{э}})^i \exp(-nP_{\text{э}})/i!, \quad (5)$$

где $P_{\text{э}}$ – вероятность битовой ошибки в цифровом канале.

Верхняя граница вероятности появления j ошибок в КИЕс длиной из n элементов (например, для СС с ОКС от 1 до 274 байт) выражается как [9]:

$$Q = P_{\text{верх}}(j \in n) = \mathrm{C}_{\mathrm{n}}^{\mathrm{j}}\,\mathrm{P}_{\text{э}}(1-P_{\text{э}})^{n-j}, \quad (6)$$

где $\mathrm{C}_n^j = n!/(n-j)!\,j!$.

Тогда, среднее время доставки данных, в зависимости от приведенной плотности потока заявок можно представить в виде:

$$M[\tau_0] = (\tau_u + \Delta\tau_u)R/(1-\rho)(1-Q), \quad (7)$$

где $\Delta\tau_{\text{u}}$ – время передачи сигнально-управляющей информации; R – количество КИЕс, передаваемых достоверно в одном сеансе.

На основании (5)–(7) построены зависимости возможной длины КИЕс от качества канала связи в СОД ТКС для СС СУС, а также средней длительности сеанса совместной передачи КИЕс речи и данных СУС ТКС от приведенной плотности потока заявок, которые представлены на рис. 2 и 3.

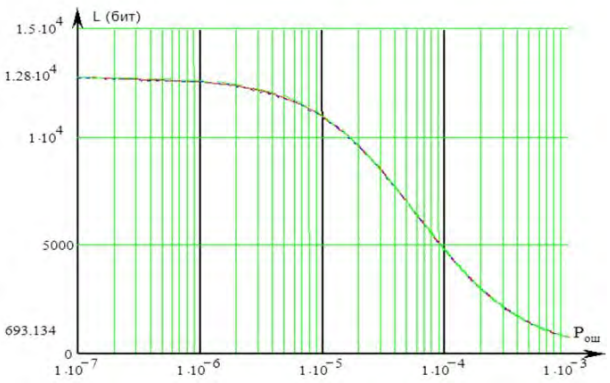


Рис. 2. Зависимость длины КИЕс от качества цифрового канала

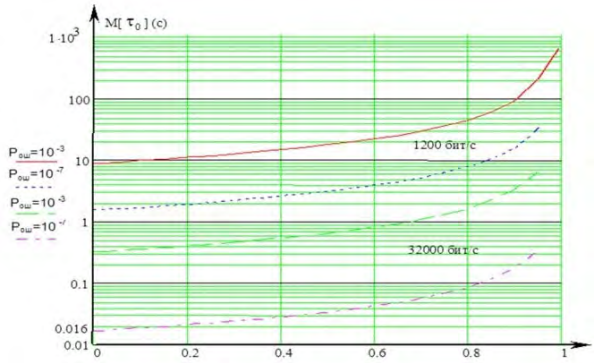


Рис. 3. Зависимость средней длительности сеанса совместной передачи КИЕс речи и данных СУС ТКС от приведенной плотности потока заявок

Анализ полученных зависимостей показывает, что при вероятности битовой ошибки $P_{ош} = 10^{-3}$ загрузка канала связи в сетевой службе ТКС не должна превышать 0,2 от максимально возможной. Это объясняется возрастающей интенсивностью перезапросов КИЕс, что снижает производительность сети в целом.

Список используемых источников

1. Курносов В. И., Шестаков А. В. Методика построения комплексов аппаратно-программных средств на основе ресурсосберегающих технологий // Радиолокация, навигация, связь : материалы XXV Междунар. науч.-технич. конф. (RLNC*2019), Воронеж, 14–16 апр. 2019 г. Воронеж : ВГУ, 2019. Т. 2. С. 281–292.

2. Буренин А. Н., Давыдов А. Е., Курносов В. И., Ефимов В. В. Основы управления и обеспечения безопасности связи и информации в инфокоммуникационных сетях / Энциклопедия «Инфокоммуникационные сети». Кн. 2. М. : Наука, 2015. 623 с.

3. Буренин А. Н., Курносов В. И. Теоретические основы управления современными телекоммуникационными сетями: монография / под общ. ред. проф. В. И. Курносова. М. : Наука, 2011. 464 с.

4. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб. : ГУАП, 2016. 325 с.

5. Исагалиева А. С., Шестаков А. В. Процедуры проектирования автоматизированной системы управления телекоммуникационной инфраструктурой // World science: problems and innovations: материалы XXXI Междунар. науч.-практич. конф., в 2 ч., ч. 1, Пенза : МЦНС «Наука и Просвещение», 2019. С. 43–47.

6. Воробьев С. П., Давыдов А. Е., Курносов В. И., Миньдюков Н. Н. Инфокоммуникационные сети: классификация, структура, архитектура, жизненный цикл, технологии / Энциклопедия "Инфокоммуникационные сети". Кн. 1. М. : Наука, 2015. 742 с.

7. Гольдштейн Б. С. Сигнализация в сетях связи. М. : Радио и связь, 1997. 263 с.

8. Лоу А. М., Кельтон В. Д. Имитационное моделирование. 3-е изд. СПб. : Питер, 2004. 848 с.

9. Рыжиков Ю. И. Имитационное моделирование. Теория и технологии. М. : Альтекс-А, 2004. 384 с.

УДК 004.657
ГРНТИ 20.23.17

МЕТОДИКА ПРОВЕРКИ ПРАВИЛЬНОСТИ СОСТАВЛЕНИЯ SQL-ЗАПРОСОВ

М. А. Куцакин, А. Н. Лапко

Академия ФСО России

Статья посвящена разработке методики проверки правильности составления SQL-запросов. Общая идея проверки заключается в сравнении результирующих наборов данных, возвращаемых проверяемым запросом и запросом-образцом. Фиксация идентичности результирующих наборов данных осуществляется с использованием тестирующих SQL-инструкций. Представлен состав тестирующих инструкций для различных SQL-запросов. Приведены исходные данные и ограничения методики. Пошагово описана методика проверки правильности составления SQL-запросов.

база данных, SQL-запрос, проверка правильности составления SQL-запросов, запрос-образец, тестирующая инструкция.

В настоящее время распространенной концепцией хранения данных в информационных автоматизированных системах является концепция баз данных (БД). Основным инструментом взаимодействия с БД является структурированный язык запросов SQL. Интерфейсы, основанные на языке SQL, поддерживаются подавляющим большинством современных коммерческих СУБД. Таким образом, одним из ключевых аспектов разработки информационных систем является знание языка SQL и умение его использования в практических целях.

В процессе подготовки специалистов в области разработки информационных систем возникает необходимость организации контроля практических умений в составлении SQL-запросов, что требует существенных временных затрат не только на составление набора практических заданий, но и на их проверку, в ходе которой не исключена вероятность возникновения ошибок, допущенных проверяющим.

В связи с этим возникает противоречие между необходимостью безошибочной и своевременной проверки практических умений в составлении SQL-запросов и ограниченным временным ресурсом, выделяемым на ее проведение. Одним из путей разрешения сложившегося противоречия является применение автоматизированных средств проверки правильности составления SQL-запросов.

Одной из особенностей языка SQL является то, что один и тот же запрос к БД может быть реализован различными способами с помощью команд (инструкций), которые могут отличаться друг от друга используемыми

операторами и синтаксическими конструкциями. Другими особенностями языка SQL являются нечувствительность к регистру, возможность написания инструкции SQL как на одной, так и на нескольких строках, возможность использования комментариев внутри SQL-команды.

Представленные особенности языка SQL свидетельствуют о том, что для реализации одного и того же действия над объектами БД существует несколько различных инструкций, гарантирующих достижение заданного результата. Этот факт обуславливает нецелесообразность использования известных систем автоматизированного тестирования общего назначения, таких как Moodle, АСТ-тест, My Test и др., для проверки правильности составлении запросов к БД, поскольку имеющиеся в этих системах типы заданий предполагают наличие только одного правильного ответа.

Известные специализированные автоматизированного средства, предусматривающие проверку правильности составления SQL-запросов, такие как SQL-EX, Vertabelo Academy, SQL Zoo и др., представляют собой Internet ресурсы, реализующие on-line тестирование. Они как правило являются англоязычными и не подразумевают коррекцию заданий, структуры и содержания объектов БД под цели конкретной образовательной программы, что крайне затрудняет, а в некоторых случаях не позволяет их использовать для оценки практических умений в составлении SQL-запросов.

В связи с этим актуальной является задача разработки методики проверки правильности составления SQL-запроса.

Общая идея проверки правильности составления SQL-запросов заключается в том, что хранить все SQL-запросы, обеспечивающие правильный результат для некоторого задания, не является целесообразным. Во-первых, количество таких запросов может быть достаточно большим, и во-вторых, не все запросы, обеспечивающие правильный результат, могут быть учтены при формировании ответа на задание, что может привести к возникновению ошибки второго рода, когда правильный ответ будет принят за неправильный. В связи с этим для проверки правильности составления SQL-запроса предлагается [1]:

– использовать только один SQL-запрос – запрос-образец, гарантированно обеспечивающий правильный результат;

– сравнивать не синтаксис проверяемого запроса с запросом-образцом, а состояния экземпляров БД, в которые их привели запрос-образец и проверяемый запрос;

– состояние экземпляров БД оценивать по результирующему набору данных, возвращаемому запросом на выборку данных из анализируемых объектов БД.

Предлагаемый способ проверки основывается на предположении: если одинаковое действие, заложенное в SQL-запросе, выполняется над двумя

одинаковыми наборами данными, то состояния двух результирующих наборов данных тоже будет одинаковым. Фиксация идентичности результирующих наборов данных осуществляется с использованием:

– запроса-образца, если рассматриваются задания, связанные с выборкой данных из таблиц БД;

– заранее подготовленных тестирующих SQL-инструкций, если рассматриваются задания создания (изменения) таблиц БД, модификации данных в таблицах БД или создания программируемых объектов БД (представлений, хранимых процедур и функций).

Тестирующие инструкции для проверки SQL-запросов создания и изменения таблиц БД, включают SQL-команды вставки (изменения) и выборки данных. SQL-команды вставки (изменения) данных позволяют протестировать структуру создаваемой или изменяемой таблицы БД, а также наличие и правильное функционирование заданных ограничений таблиц. SQL-команды выборки данных позволяют определить успешность произведенной вставки (изменения) данных.

Тестирующие инструкции для проверки SQL-запросов модификации данных в таблицах БД включают SQL-команды выборки данных, которые позволяют определить правильность произведенных операций модификации данных в анализируемых таблицах БД. Причем для каждого SQL-запроса модификации данных достаточно одной SQL-команды выборки всех данных из анализируемой таблицы БД, что позволит определить новое состояние набора данных.

Тестирующие инструкции для проверки SQL-запросов создания программируемых объектов БД включают фрагменты SQL-кода вызова этих объектов с различными значениями входных параметров и другие тестирующие инструкции, рассмотренные ранее, в зависимости от содержания (функционального наполнения) анализируемого программируемого объекта. В этом случае создание программируемого объекта БД считается правильно выполненным, если все тестирующие инструкции дадут положительный результат, т. е. для различных исходных данных будет получен ожидаемый результат.

Исходными данными методики проверки правильности составления SQL-запроса являются:

– проверяемый запрос или проверяемый фрагмент SQL-кода;

– запрос-образец или в общем случае фрагмент-образец SQL-кода;

– набор тестирующих SQL-инструкций;

– резервная копия БД, позволяющая привести набор данных в исходное состояние.

В качестве ограничений решаемой задачи выступают:

– последовательность столбцов в инструкциях создания таблиц БД и выборки данных должна строго соответствовать условию задания;

– дополнительные манипуляции с результирующим набором данных в инструкциях выборки данных, которые могут привести к изменению последовательности строк или содержимого ячеек (например, сортировка, округление значений и др.), не допустимы.

Результатом проверки правильности составления SQL-запроса является значение переменной answer булева типа данных: answer = 1, если задание решено верно, answer = 0 в противном случае.

Во избежание возникновения конфликтов между объектами БД, созданными проверяемыми запросами и запросами-образцами предлагается эти запросы выполнять в разных экземплярах БД. В этих целях создаются два экземпляра БД: exem_check – для выполнения проверяемых запросов и exem_example – для запросов-образцов.

Методика проверки правильности составления SQL-запросов заключается в последовательном выполнении шагов:

1. Инициализация используемых переменных и массивов; answer = 0.

2. Экземпляры БД exem_check и exem_example приводятся в одинаковое состояние, заданное в файле резервной копии БД.

3. В экземпляре exem_check выполняется проверяемый SQL-запрос или фрагмент проверяемого SQL-кода.

4. В случае возникновения ошибки при выполнении проверяемого SQL-запроса принимается решение о том, что задание не выполнено. Проверка завершается.

5. В противном случае в экземпляре exem_example выполняется запрос-образец или фрагмент-образец SQL-кода.

6. При проверке SQL-кода, включающего создание (изменение) таблиц БД, в обоих экземплярах БД выполняется один и тот же набор тестирующих инструкций вставки (изменения) данных.

7. При проверке SQL-кода, включающего модификацию данных в таблицах БД, в обоих экземплярах выполняется один и тот же набор тестирующих инструкций выборки данных из анализируемых объектов БД.

8. Проверяется идентичность результирующих наборов данных, полученных в двух экземплярах БД. Последовательность проверки:

8.1. Определяется размерность результирующих наборов данных в двух экземплярах, т. е. вычисляется количество строк и столбцов.

8.2. В случае если размерность результирующих наборов данных различна в двух экземплярах, то результирующие наборы данных считаются неидентичными. Принимается решение о том, что задание выполнено неправильно. Проверка завершается.

8.3. В случае если размерность результирующих наборов данных в двух экземплярах одинакова, осуществляется сравнение значений в соответствующих ячейках результирующих наборов данных двух экземпляров.

8.4. В случае совпадения значений во всех ячейках результирующих наборов данных двух экземпляров, принимается решение об их идентичности.

8.5. В противном случае результирующие наборы данных считаются неидентичными. Принимается решение о том, что задание выполнено неправильно. Проверка завершается.

9. В случае идентичности результирующих наборов данных в двух экземплярах принимается решение о том, что задание выполнено правильно; answer = 1.

Проверка адекватности представленной методики проверки правильности составления SQL-запросов показала ее пригодность к использованию по назначению. Представленная методика, реализованная в виде прикладной программы [2], позволяет существенно облегчить деятельность проверки заданий по составлению SQL-запросов, сократить время проверки, снизить вероятность возникновения ошибок первого и второго рода.

Среди направлений дальнейших исследований по данному направлению можно отметить:

– разработку механизма проверки SQL-запросов, при котором наборы данных, отличающиеся только последовательностью строк или столбцов, считались бы идентичными, что позволит снять одно из ограничений представленной методики;

– внедрение механизма частичного выполнения сложных заданий, который позволит ввести обратную связь с обучающимся с целью указания пунктов задания, которые ему не удалось выполнить, и учесть их при проверке правильности составления SQL-запросов;

– создание заданий, адаптированных к различным диалектам языка SQL (Transact-SQL, PL-SQL, PL-pgSQL) и пригодными к использованию в различных СУБД.

Список используемых источников

1. Лапко А. Н., Вихарев А. Н., Зверев Д. А., Парамонов И. С. Подход к автоматизации процесса проверки правильности составления SQL-запросов // Информационные технологии моделирования и управления. 2019. № 2 (116). С. 141–148.

2. Лапко А. Н., Сентяков А. М. Модуль проверки корректности составления SQL-запросов. Свидетельство о государственной регистрации программы для ЭВМ № 2018663299 Российская Федерация; заявл. 25.09.2018; зарег. 24.10.2018.

УДК 004.93'12
ГРНТИ 85.29.05

РАЗРАБОТКА МЕТОДА ПОИСКА РЕЛЕВАНТНЫХ ПАТЕНТНЫХ ИЗОБРАЖЕНИЙ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ

Н. С. Лебедев, Ю. Н. Островский, Д. О. Федосеев

Военная академия связи

Разработка методов поиска, использующих изображения патентов, позволяет сделать патентную экспертизу более качественной, международной. Отсутствие изображений в патентной заявке может указывать на неполное описание изобретения и влечет за собой отказ и другие проблемы. Классификация патентных изображений является сложной задачей. Так как патентные изображения, даже если рассматривать изображения одного типа, класса и т.п., являются уникальными, отличающимися друг от друга.

патентные изображения, нейронные сети, формирование набора данных, качество обучающего набора данных, глубокое обучение, метод поиска.

Количество патентных заявок стабильно увеличивается из года в год. В 2016 году было подано больше чем 3 миллиона заявок на получение патента. Это рекордное число, которое выше на 8,3 % чем в 2015 году [1]. С увеличением количества патентов растет и время рассмотрения заявки на регистрацию патента [2, 3]. Эксперту патентного бюро необходимо установить уникальность патентуемого изобретения. Для этого он должен провести сравнение с похожими патентами и удостовериться в отсутствии аналогов изобретения. В ходе такой работы эксперт может проверить тысячи патентов, пользуясь как текстовыми поисковыми запросами, так и анализом содержащихся в существующих патентах изображений [4]. Поэтому изучение изображений может оказаться очень важным при установлении релевантности патентов поданной заявке [5, 6]. Еще одним подтверждением важности поиска патентных изображений является тот факт, что изображения, по самой своей сути, не зависят от языка заявителя и не испытывают воздействия происходящих со временем изменений в научной терминологии, воздействующих на качество поиска. К тому же использование при поиске патентных изображений облегчало бы выявление релевантных документов, опубликованных на разных языках, не прибегая к недостаточно качественному машинному переводу. В настоящее время существует проблема недостаточной точности традиционных методов поиска релевантных

изображений, что не позволяет автоматизировать анализ рисунков, содержащихся в патентных документах.

Многообещающий подход для улучшения поиска изображений в патентах – это адаптировать анализ релевантности к каждому классу изображения патентов, например, сравнивать блок-схемы друг с другом, то есть для поиска патентных изображений нужно сначала произвести предварительный анализ изображения. Например, классифицировать изображения.

Оценка точности нейронной сети (табл. 1), обученной на основе IPC (*International Patent Classification*) [7], показывает неудовлетворительные результаты [8].

ТАБЛИЦА 1. Точность нейронной сети, обученной на основе существующей классификации IPC, в зависимости от размера изображения и количества эпох

Размер изображения	Кол-во эпох	Время обучения	Точность на обучаемых данных, %	Точность на тестовых данных, %
100x100	8	12 мин	26,46	20,15
100x100	16	20 мин	35	22,88
200x200	8	35 мин	28	21,25
200x200	16	1 ч 19 мин	38	25
200x200	32	2 ч 44 мин	50	28
400x400	16	4 ч	37	19
400x400	40	8 ч 52 мин	51	30

Было принято решение об улучшении качества выборки и получении новой классификации патентных изображений. С помощью веб-парсинга были получены патентные изображения. В результате (таб. 2) осталось 45 168 изображений, 86,25 % изображений с веб-сайта Freepatent [9] не подходят для обучающей выборки.

ТАБЛИЦА 2. Улучшенная выборка изображений после обработки

Категория	Количество скачанных изображений	Количество оставшихся изображений после удаления
Удовлетворение жизненных потребностей человека	66 421	8 348
Различные технологические процессы; транспортирование	44 506	8 506
Химия; металлургия	105 174	8 222
Текстиль; бумага	4 976	1 192
Строительство; горное дело	14 222	2 872
Машиностроение; освещение; отопление; двигатели и насосы;	36 501	7 174

Категория	Количество скачанных изображений	Количество оставшихся изображений после удаления
оружие и боеприпасы; взрывные работы		
Физика	45 540	6 742
Электричество	11 222	2 112

Была разработана новая классификация патентных изображений (рис. 1), в отличие от существующих, основанная не на субъективных мнениях экспертов, а на выделения графических объектов на основании результатов вычислительных экспериментов. Полученные изображения (табл. 2) были распределены по 6 классам изображений: технический рисунок, химическая структура, диаграмма, последовательность гена, блок-схема, таблица.

На основе оставшихся изображений была сформирована обучающая, проверочная и тестирующая выборки по выделенным классам патентных изображений. Для создания обучающей выборки брались по 1 000 изображений на каждый класс. 600 изображений обучающая выборка, 200 проверочная и 200 тестирующая.

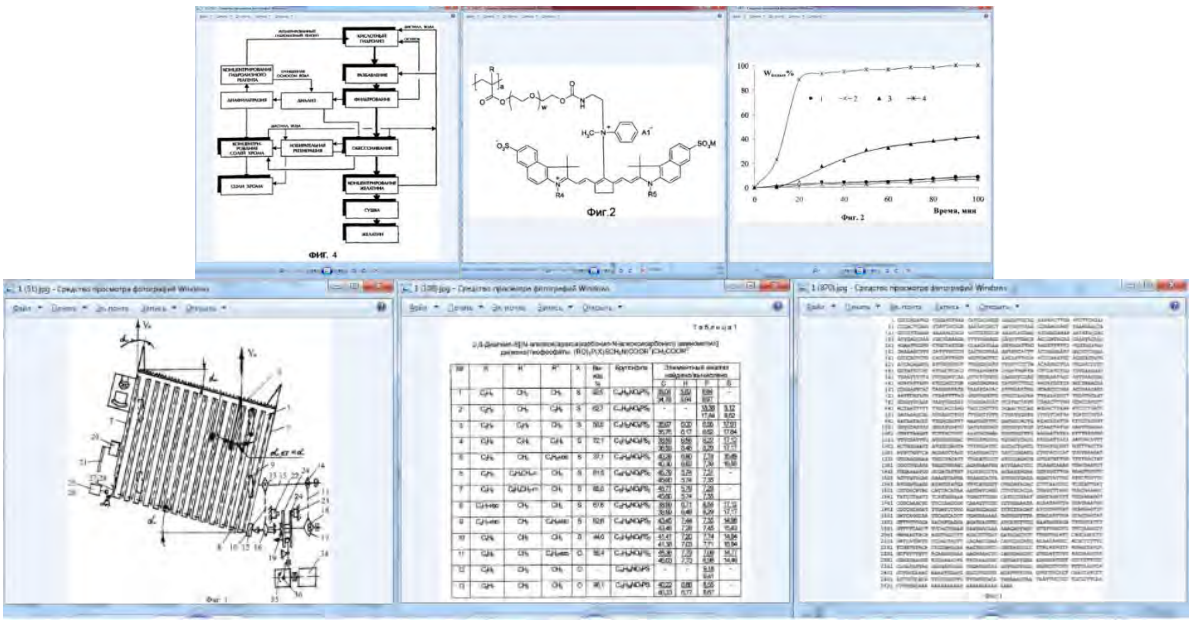


Рис. 1. Классификация патентных изображений, полученная на основе вычислительных экспериментов

Для классификации патентного изображения использовалась архитектура глубокой сверточной нейронной сети (рис. 2), состоящая из трех повторяющихся слоев свертки и под-выборки для выделения признаков изображений и полносвязного классификатора из 64 нейронов и выходного слоя из 6 нейронов. Использование функции активации ReLU, обусловлено тем,

что она показывает хорошие результаты при обучении нейронных сетей и отвечает за отсечение ненужных деталей в канале (при отрицательном выходе). Для оптимизации используется метод градиентного спуска с размером мини-выборки 32, то есть берутся первые 32 изображений, определяется направление градиента и в соответствии с этим направлением выполняем изменение весов и т. д.

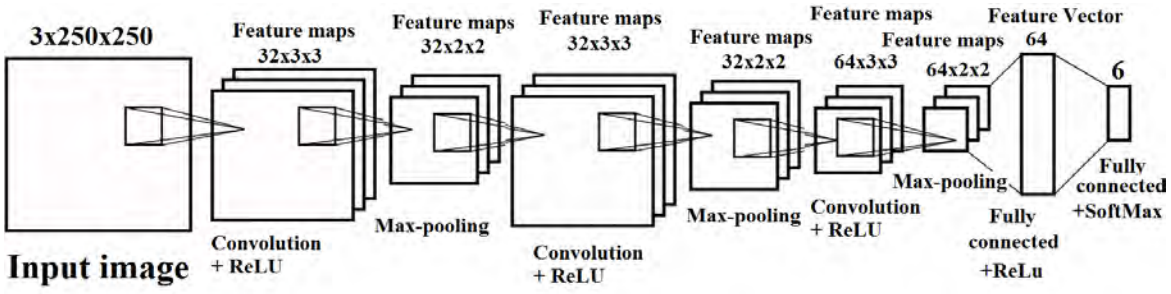


Рис. 2. Архитектура СНС

Разработан метод (рис. 3, слева) поиска релевантных патентных изображений, который сравнивает соответствующие классы патентных изображений, определяемых на основе глубокой сверточной нейронной сети, с помощью перцептивного хэша и расстояния Хэмминга.

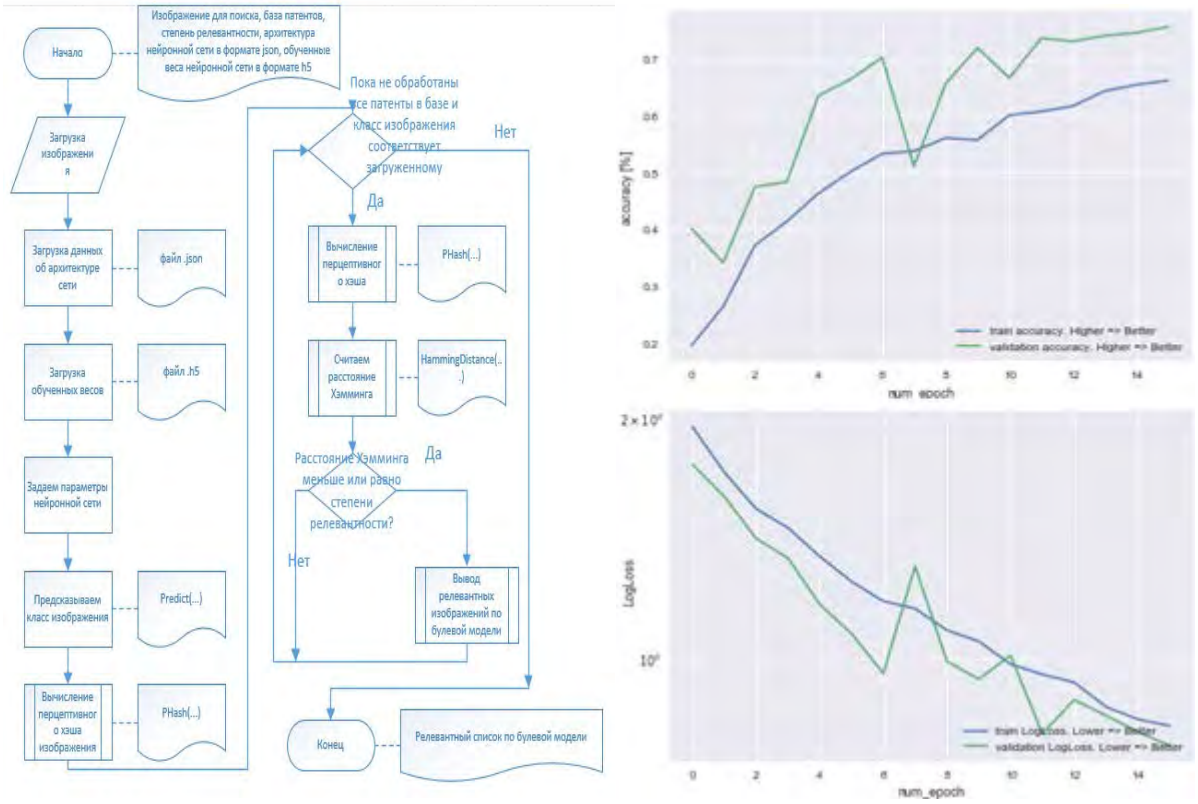


Рис. 3. Алгоритм работы метода (слева). Графики зависимости точности и функции ошибки от количества эпох. Количество эпох 16. Dropout 0.7. (справа)

Также был обеспечен контроль над обучением нейронной сети с помощью проверочной выборки.

Количество эпох 16. Средство регуляризации Dropout 0.7. Результаты эксперимента показывают (рис. 3, справа), что нейронная сеть не дообучилась и точность модели можно повысить, увеличив количество эпох. Также нужно следить за тем, чтобы нейронная сеть не переобучилсась, используя средства регуляризации, например Dropout, проверочную и тестирующую выборку. На графиках точность на проверочных данных должна быть больше, чем на обучающих, так как на обучающих данных использовано средство регуляризации Dropout. Как видно из графиков (рис. 3, справа) переобучения не произошло.

Практическая значимость

Разработана автоматизированная система для скачивания патентных изображений, удаления некорректных изображений, перемещения изображений на заданный уровень вложенности, определения класса патентного изображения и поиска релевантных патентных изображений.

Заключение

В результате исследования был разработан новый метод поиска релевантных изображений, основанный на глубокой сверточной нейронной сети и алгоритме перцептивного хэша.

Программно реализован разработанный метод и модуль по формированию набора данных для обучения в виде автоматизированной системы (рис. 4).

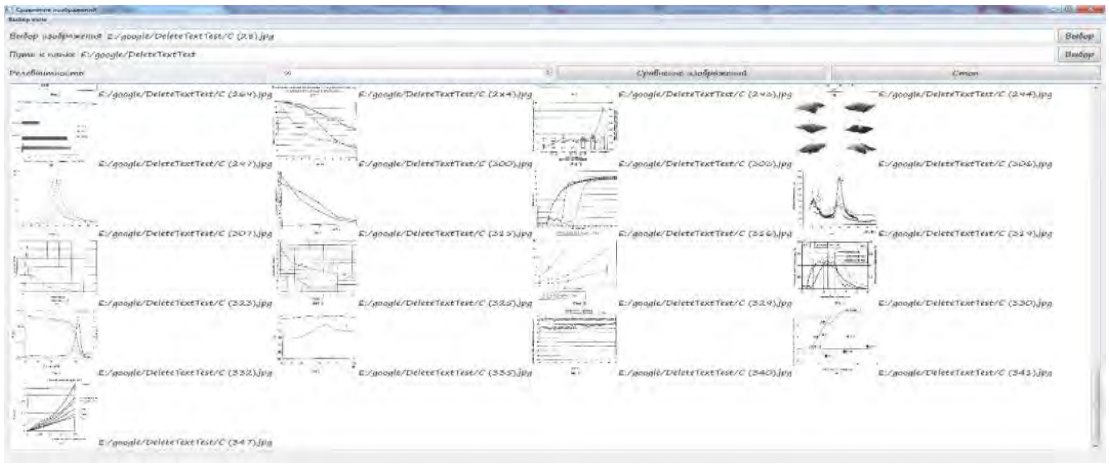


Рис. 4. Поиск релевантных изображений

Была предложена новая классификация патентных изображений, основанная на машинной обработке большого патентного массива и выделения

графических объектов на основании результатов вычислительных экспериментов.

Список используемых источников

1. WIPO [Электронный ресурс] // International patent classification. URL: http://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2017-chapter2.pdf

2. Korobkin, D., Fomenkov, S., Kravets, A., Kolesnikov, S. Methods of statistical and semantic patent analysis // Communications in Computer and Information Science. 2017. N 754. pp. 48–61.

3. Kravets, A., Shumeiko, N., Lempert, B., Salnikova, N., Shcherbakova, N. "Smart Queue" Approach for new technical solutions discovery in patent applications // Communications in Computer and Information Science. 2017. N 754, pp. 37–47.

4. Дыков М. А., Кравец А. Г., Коробкин Д. М., Укустов С. М., Сальников М. Ю. Автоматизированная система принятия решений при патентной экспертизе // Известия ВолгГТУ. Серия «Актуальные проблемы управления, вычислительной техники и информатики в технических системах». Вып. 20. 2014. № 6 (133). С. 35–41.

5. Kravets, A., Kozunova, S. The risk management model of design department's PDM information system // Communications in Computer and Information Science. 2017. N 754. PP. 490–500.

6. Kravets, A. G., Mironenko, A. G., Nazarov, S. S., Kravets, A. D. Patent application text pre-processing for patent examination procedure // Communications in Computer and Information Science. 2015. N 535. pp. 105–114.

7. WIPO [Электронный ресурс] // International patent classification. URL: http://www.wipo.int/classifications/ipc/en/

8. Kravets Alla, Lebedev Nikita and Legenchenko Maxim Patents Images Retrieval and Convolutional Neural Network Training Dataset Quality Improvement // in ITSMSSM. 2017. vol. 72. pp. 287–293.

9. Freepatent [Электронный ресурс] // Библиотека патентов на изобретения. URL: http://www.freepatent.ru/

УДК 004.056.57
ГРНТИ 81.93.29

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

А. И. Ликарь

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Информация, обрабатываемая на персональных компьютерах пользователей в домашних условиях, а также на предприятиях, разнообразна. Незаконное использование информации наносит серьёзный удар по репутации, банальное воровство денег с бан-

ковских карт. Если информация хранится на компьютере и автоматизировано обрабатывается, риск ее потери возрастает. Любая информация, которая содержит сведения, как частного характера, так и закрытой (конфиденциальной) информации различных организаций, является важной и чрезвычайно ценной.

Целью анализа методов защиты информации от вредоносного программного обеспечения, является анализ и выработка доступных и эффективных мер по защите от получения незаконного доступа к информации и обеспечение ее сохранности. В результате выполнения предложенных мер внедрение вредоносного программного обеспечения в информационную систему извне снижается и сводится к минимуму.

вредоносное программное обеспечение, анализ методов защиты информации.

С развитием информационно-коммуникационных средств, а следовательно, и возможности повреждения информации, которая хранится и передается с их помощью, появилась информационная безопасность.

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудования, предназначенные для использования, сбережения и передачи этой информации. Иными словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты информационной безопасности.

Компьютерная программа или код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе, либо для скрытого неправомерного использования системных ресурсов или иного вмешательства в функционирование компьютерной системы, называется вредоносным ПО.

Вредоносное программное обеспечение включает в себя сетевые черви, классические компьютерные вирусы, рекламные программы (*advare*), троянские кони, шпионские программы, хакерские утилиты и другие программы, которые наносят вред компьютеру, на котором они запущены, или другим компьютерам в сети. В независимости от типа, вредоносное ПО может нанести значительные потери. Для информации возникают угрозы нарушения ее целостности, конфиденциальности или доступности.

Вирусы, вирусные программы, но прежде всего вирусы, представляют серьезную угрозу для информации. Недооценка этого риска может оказать серьезные последствия для информации пользователей и организаций. Знание механизмов действия вирусов, методов и средств борьбы с ними, позволяет эффективно организовать противодействие вирусам, минимизировать вероятность заражения и потери от их воздействия [1].

Проанализировав методы защиты информации от вредоносного ПО, можно утверждать, что полной защиты от вредоносных программ не существует. Для снижения угроз от воздействия вредоносного ПО, рекомендуется использовать следующие методы защиты:

1. Использовать современные лицензионные операционные системы, которые имеют защиту от вредоносных программ. Регулярно устанавливать обновления для операционной системы. Включить режим автоматического обновления операционной системы, при его наличии.

2. При работе на персональном компьютере пользоваться правами пользователя. Для повседневной работы, правами администратора не пользоваться. Это уменьшит вероятность установки вредоносного ПО на компьютере.

3. Антивирусные программы, используемые для работы, применять надежных производителей. Устанавливать автоматическое обновление, программ и антивирусных баз. Использовать, программы, которые используют эвристические анализаторы, для противодействия вредоносному ПО.

4. При работе с выходом в интернет, не забываем об угрозах, которые там есть, также необходимо использовать персональный Firewall. Правила работы которого, устанавливает сам пользователь либо работодатель.

5. Ограничить физический доступ к компьютеру других лиц. Для входа в компьютер, применять пароль.

6. Используйте внешние носители информации, только из проверенных источников. Проверяйте съемные диски на наличие вирусов перед их использованием. Все файлы, загружаемые из интернета проверять на вирусы.

7. Компьютерные файлы, полученные от ненадежных источников, не открывайте. На сменных носителях отключить автозапуск. Эта мера, без разрешения пользователя, не даст запускаться программам или кодам, которые находятся на них. При открытии документа, если сообщается об использовании макросов, запрещаем их загрузку.

Защита от различных видов вредоносных программ включает в себя множество программных компонентов и методов обнаружения «хороших» и «плохих» приложений. Сегодня производители антивирусных программ встраивают сканеры в свои программы для обнаружения «шпионов» и другого вредоносного кода, поэтому все делается для защиты конечного пользователя. Однако ни один из пакетов антишпионских программ не является совершенным. Один продукт может быть чрезмерно внимателен к программам, блокируя их при малейшем подозрении, в том числе удаляя полезные утилиты, которыми вы регулярно пользуетесь. Другой продукт более лоялен к программам, но может пропустить некоторые шпионские программы. Так что никакой панацеи нет. Эффективность обнаружения вредоносного программного обеспечения не является абсолютной и варьируется в зависимости от используемых угроз и антивирусного программного обеспечения [2].

Рекомендовано, одновременное использование, антивируса и антишпионской программы. Это наилучшим образом обеспечивает всестороннюю защиту системы от опасностей, которые могут возникнуть неожиданно.

Один пакет, следует использовать в качестве постоянного «блокатора», который загружается каждый раз при включении компьютера, в то время как другой пакет (или несколько) должен запускаться, по крайней мере, раз в несколько дней, для обеспечения дополнительного сканирования. Таким образом, то, что один пакет пропускает, другой сможет обнаружить.

Таким образом, комплексное и только, комплексное использование методов защиты информации от вредоносного программного обеспечения, позволит снизить риск потери информации, защитить компьютеры. Необходимо постоянно анализировать угрозы от злонамеренных действий, и постоянно совершенствовать комплексные средства защиты на шаг вперед.

Список используемых источников

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. М. : ИД «Форум», 2008. 416 с.

2. Степанов Е. А., Корнеев И. К. Информационная безопасность и защита информации. М. : Инфра-М. 2001. 304 с.

Статья представлена, заведующим кафедры БИС СПбГУТ, кандидатом технических наук, доцентом С. В. Хорошенко.

УДК 004.853
ГРНТИ 28.23.01

ИСТОРИЯ И ОСОБЕННОСТИ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В. А. Липатников, А. А. Матвеев, В. В. Флейснер

Военная академия связи

Рассматривается актуальная проблема В статье рассмотрена краткая история развития работ и проектов по искусственному интеллекту (ИИ), охарактеризованы направления, рассмотрены предпосылки по развитию ИИ, даётся общий обзор современного состояния исследований и разработок систем на основе ИИ. Рассмотрены возможности применения ИИ в системах специального назначения.

искусственный интеллект, история развития, языки программирования, машинное обучение.

На данный момент развитие искусственного интеллекта насчитывает уже более пятидесяти лет. На пути этого развития интерес к нему то угасал, то вновь разжигался с новой силой. Это было связано с теми или иными

предложениями по решению фундаментальных проблем, концепциями, научно-техническими решениями [1].

Первым этапом (волной) развития искусственного интеллекта стали работы по изучению теории искусственного интеллекта, относящиеся к 1950-м годам. Так они пытались решить три фундаментальные задачи [1, 2]:

1. Игра в шахматы

В 1954 году аналитики из корпорации REND написали программу для игры в шахматы. А. Ньюэлл, Дж. Шоу, Г. Саймон и другие аналитики написали программу для игры в шахматы против компьютера. Этим проектом заинтересовались уже тогда ставшие экспертами в этой области А. Тьюринг и К. Шеннон. Позже в этот проект были и привлечены группа голландских психологов. И к 1957 году данный проект был закончен, называлась эта программа NSS (*Newell, Shaw, and Simon*). В основе этой работы лежала эвристика, правила выбора решения в отсутствие теоретических оснований.

2. Машинный перевод

С 1954 года по 1957 год в СССР разрабатывались экспериментальные переводчики машинного перевода с английского и китайского на русский. Использовались такие ЭВМ как БЭСМ-2 М-20 в ИТМиВТ, гражданского назначения под руководством Королёва Л. Н. В военном же секторе так же велись подобные разработки на М-40, М-50, 5Э26 и других.

Однако в 1954 году был проведён «Джорджтаунский эксперимент» [3, 4]. Именно такое название получил эксперимент с машинным переводом. 7 января 1954 года в штаб квартире корпорации IBM в Нью-Йорке был продемонстрирован полностью автоматический перевод более 60 предложений с русского языка на английский, благодаря базе знаний состоящей из 60 русских фраз (основа словаря), 250 пар слов, и 6 грамматических правил. Этот эксперимент стал первым удавшимся таким опытом и послужил большим толчком в направлении развития искусственного интеллекта последующие 12 лет.

Хоть и результаты были многообещающие, но проблема оказалось много сложнее чем казалось ранее. Суть данного эксперимента была скрыта от окружающих. Однако по прошествии времени мы можем с уверенностью сказать, что долгоиграющей целью эксперимента было машинное обучение. Суть данного перевода заключалось в обучении компьютера создавать правила построения, создание исключений и общей логики перевода. На тот момент вычислительной мощности и технических средств, которые были доступны, оказалось недостаточно, чтобы выполнить полностью поставленную задачу. Однако стоит отметить, что данная попытка оказало огромное

влияние на направления развития искусственного интеллекта, а так же математической лингвистики.

3. Доказательство теорем

Автоматическое доказательство теорем стало одно из наиболее активно развивающихся тем, при развитии искусственного интеллекта [6]. В 1959 году усилиями Г. Саймоном, К. Шоу и А. Ньюэллом был создан «Универсальный решатель задач» [1, 3]. Данная программа была предназначена для универсального решения задач, ну соответствующим образом формализованная. Целью были решение задач евклидовой геометрии, логики предикатов, решение шахматных задач.

Вторым этапом развития считается логическое программирование. Первой работой в этом направлении является создание первого языка программирования (логического) Prolog, созданного 1971 году. Так же в связи с созданием этого языка был ажиотаж вокруг экспертных систем. Так экспертные системы пытались решить свои задачи путём искусственного интеллекта, а именно специалисты по управлению знаниями. Эти специалисты вручную опрашивая экспертов предметной области формировал базу знаний выдержками и фундаментальными принципами работы в данной области. Машина же делала вывод в рамках своего «понимания» вещей, однако поскольку эти знания заложил человек, соответственно это было пропущено через фильтр человека, потому оно (это решение) было заранее детерминировано. Так же главной проблемой этой работы было выбор правильных экспертов в данной области, поскольку знания, которое они давали были субъективными. Так же не стоит забывать, что создание таких систем отняло бы часть работы у тех же экспертов, осознавая это они понимали, что это приведёт к снижению их профессионального статуса. Так любой человек только выпустившийся с университета, с помощью этой системы мог оказать такую же экспертную оценку, как и специалист, проработавший в данной области не один год. Подытожив эти доводы, можем отметить что создание экспертных систем породило большой интерес к проблеме представления знаний в компьютерных системах. Эта проблема и породило семантические сети, системы фреймов, продукционные системы (системы, основанные на семантических правилах) и их комбинаций.

Так же стоит отметить успехи в машинном переводе текстов с одного языка на другой. Данное направление активно развивалось в противостоянии России и США во времена холодной войны. Так как в это время поступало большое количество информации на русском языке, а человеческие ресурсы были ограничены, была острая необходимость в машинном переводе текстов. Похожий опыт был у компании IBM Candide. Данная корпорация переводила стенограммы заседаний канадского парламента, которые были опубликованы на английском и французском языках. Общая база данных

данной системы составила более 3 миллионов предложений. В виду того что это были официальные документы, их переводы были выполнены на высочайшем уровне. По меркам 1990 года количество данных было огромным. Данная технология машинного перевода получило название «статический машинный перевод» [9]. Кривая повышения уровня машинного перевода на этом этапе остановила свой рост, в виду того что правительство посчитало что данная тема исчерпала себя и больше не нуждается в дальнейшем развитии и инвестировании в неё средств.

Вторым этапом (волне) развития искусственного интеллекта ознаменовано создание продвинутых программ, относительно ранее созданных, для игры в шахматы и шашки. Так же к этому периоду относятся и первые соревнования машин в ранее описанных дисциплинах. Так одной из ярких побед на соревнованиях между компьютерными программами для игры в шахматы можно смело считать матч августа 1974 года. На первом чемпионате мира по шахматам (*World Computer Chess Championship,* WCCC) советская программа, разработанная в середине 1960 годов завоевала первое место [12]. Успех «Каиссы» стал мировой сенсацией, поскольку все были уверены в успехе американской программы. По воспоминанием шахматистов, которые были на первом чемпиона мира, примерный уровень игры данной программы второй шахматный разряд.

Первая и вторая волна развития искусственного интеллекта стала называться «старый добрый ИИ». Формальная логика, которая легла в основу программ, применима для формализованных задач, но данный подход очень проигрывает системам реального времени.

Нынешнее развитие искусственного интеллекта принято считать третьей вехой (волной) развития искусственного мозга. Данная волна сразу поразила экспертов как охватом задач, так и амплитудой. На данный момент развитие IT технологий, технические средства, высокоскоростные пути передачи данных, интернет, беспроводные сети развились остаточно хорошо и повсеместно, это позволяет внедрять системы на основе искусственного интеллекта практически в каждый дом. Мы можем рассчитывать на значительный прорыв в данной области знаний человечества. Точкой отсчёта данной вехи принято считать знаменитую победу американской шахматной программы «Дип Блю» над чемпионом мира Гарри Каспаровым.

В отличие от первых двух этапов, третья волна ознаменовалась применением генетического программирования. Данная логика позволяет имитировать процесс мутаций, или адаптации, которая протекает в биологических видах, а развитие вычислительных мощностей позволяет провести миллионы лет эволюции в считаные дни. Такие алгоритмы идеально подходят в системах поиска решений, под которые можно постараться формализовать почти любую задачу.

Так же одним из бурно развивающихся направлений развития является технология искусственных нейронных сетей (ИНС). Данная технология имитирует работу биологических нейронов живых существ. Так простейшая ИНС состоит из 3 частей: входного слоя, скрытых слоёв (вычислительных слоёв) и выходного слоя. Схема работы простейшей (3-х слойной) нейронной сети продемонстрирован на рис. На первый слой поступают входные данные или сигналы из внешнего мира, во внутреннем слое они обрабатываются и передаются в выходной слой, который и выводит решение нейронной сети о том или ином объекте, или решении. Внутренний слой ограничивается лишь суммарной мощностью вычислительных средств, задействованный в данной нейронной сети.

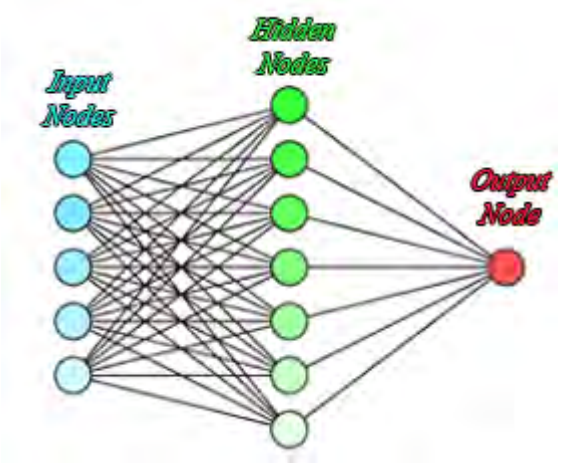


Рис. Схема простейшей нейронной сети

В Вооружённых силах Российской Федерации системы принятия решений на основе искусственного интеллекта так же получили большое развитие. Так данные системы уже активно работают на беспилотных летательных аппаратах, робототехнике, применяются в самолётостроении, а так же в управлении боевыми машинами в небе. В недрах Национального центра управления обороной Российской Федерации стоит не одна система помощи в принятии решения, основанная на искусственном интеллекте, а технология Big Data позволяет храниться тысячам эеттабайтов из всех уголков нашей страны, для принятия решения по тем или иным вопросам.

Главный вопрос, который сейчас нас интересует насколько масштабным будет развитие искусственного интеллекта в третьей вехе своего развития и на какой ноте оно закончится. Подводя итог вышенаписанного можно смело сказать, что мы уже перешли экватор третьего этапа развития. Накопленные знания, умения, навыки и подходы к разработке систем искусственного интеллекта позволяют сейчас сказать, что мы ограничены только широтой мысли человека, а это значит, что мы готовы к созданию систем, которые будут порождать другие системы. Это и будет четвёртым этапом развития искусственного интеллекта.

Список используемых источников

1. Баррат Дж. Последнее изобретение человечества. Искусственный интеллект и конец эры Homo sapiens. М. : Альпина нонфикшн, 2015. 304 с.

2. Бессмертный И. А. Искусственный интеллект. СПб. : СПбГУ ИТМО, 2010. 132 с.

3. Бринк Х., Ричардс Д., Феверолф М. Машинное обучение. СПб. : Питер, 2017. 336 с.

4. Брокман Д. Что мы думаем о машинах, которые думают: Ведущие мировые учёные об искусственном интеллекта. М. : Альпина нон-фикшн, 2017. 552 с.

5. Васильева Д. Тенденции в развитии искусственного интеллекта [Электронный ресурс]. URL: http://robotoved.ru/iskusstvennii_intellket_development/

6. Демченко Д. Карта применения технологий искусственного интеллекта: Медицина, образование, транспорт и другие сферы [Электронный ресурс]. URL: https://vc.ru/p/ai-map

7. Дерюгина О. Искусственный интеллект и современное искусство [Электронный ресурс]. URL: http://www.colta.ru/articles/art/14931

8. Достижения в глубоком обучении за последний год [Электронный ресурс]. URL: https://habrahabr.ru/company/mailru/blog/338248/

9. Жданов В. С. Современное состояние и перспективы развития искусственного интеллекта [Электронный ресурс]. URL: http://emag.iis.ru/arc/infosoc/emag.nsf /BPA/c1274a3671576d79c325766200406380

10. Искусственный интеллект (ИИ) как ключевой фактор цифровизации глобальной экономики [Электронный ресурс]. URL: https://www.crn.ru/ news/ detail.php?ID=117544

11. Как искусственный интеллект поможет спасти планету [Электронный ресурс]. URL: https://news.rambler.ru/other/39160318-kak-iskusstvennyy-intellekt-pomozhet-spasti-planetu/

12. Майер-Шенбергер В., Кукьер К. Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим / Пер. с англ. М. : Манн, Иванов и Фербер, 2014. 240 с.

13. Мунгалов Д. Власть над миром: Чем закончится гонка за искусственным интеллектом [Электронный ресурс]. URL: https://sk.ru/news/b/articles/archive/2017/08/23/vlast-nad-mirom-chem-zakonchitsya-gonka-za-iskusstvennym-intellektom.aspx

14. Опасности искусственного интеллекта [Электронный ресурс]. URL: http://senspeople.ru/opasnosti-iskusstvennogo-intellekta/

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ ЭФФЕКТИВНОСТИ РЕДУКЦИИ МЕНЕЗЕСА, ОКАМОТО И ВАНСТОУНА ПРИ РЕШЕНИИ ПРОБЛЕМЫ ДИСКРЕТНОГО ЛОГАРИФМА В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

В. А. Липатников, В. С. Ярмуш

Военная академия связи

Представлен анализ эффективности MOV-редукции для решения проблемы дискретного логарифма. Представлено математическое описание MOV-редукции. Выявлен

основной недостаток MOV-редукции. Предложен алгоритм реализации MOV-редукции в случае суперсингулярных кривых. Представлен результат работы алгоритма при различных множителях безопасности.

MOV-редукция, суперсингулярные кривые, решение проблемы дискретного логарифма.

Некоторые современные ассиметричные криптографические системы строятся на решении проблемы дискретного логарифма в конечных полях. Сегодня существуют субэкспоненциальные методы решения проблемы дискретного логарифма (DLog) в конечных полях, что вызывает интерес к группе точек эллиптической кривой (ЭК), поскольку эти субэкспонен-циальные методы не применимы для них. То есть мы можем рассматривать группы меньшего размера, благодаря чему можно использовать более короткие ключи при том же уровне безопасности.

Менезес, Окамото и Ванстоун (MOV), используя спаривание Вейля [1], сумели осуществить редукцию проблемы дискретного логарифмирования в группе точек кривой к проблеме дискретного логарифмирования в конечном поле. Известно, что в конечном поле существует довольно большое количество эффективных алгоритмов решения проблемы DLog по сравнению с ЭК. Цель работы: определить эффективность MOV-редукции при решении DLog задачи. Задача: выполнить данную редукцию и показать, является ли MOV-редукция эффективнее общих методов решения проблемы DLog в группе точек ЭК.

Опишем MOV-редукцию. Первоначально докажем взаимно однозначное соответствие между точками на эллиптической кривой и элементами конечного поля.

Теорема 1. Пусть E – эллиптическая кривая, определенная над конечным полем $\mathbb{F}_q$. Пусть P имеет порядок n и порождает подгруппу $\langle P\rangle$ в $E(\mathbb{F}_q)$. Пусть Q – точка в $E[n]$ такая, что $e_n(P,Q)$ является примитивным корнем n-й степени из единицы.

Пусть $\varphi: \langle P\rangle \to \mu_n$– функция, где

$$\varphi : R \to e_n(R,Q).$$

Тогда φ является изоморфизмом.

Пусть проблема дискретного логарифма на эллиптической кривой подгруппы $\langle P\rangle$ будет задана с помощью $R \in \langle P\rangle,\ Q \in E[n]$ и $R = l \cdot P$, для $0 < l < n-1$. Положим $\alpha = e_n(P,Q)$ и $\beta = e_n(R,Q)$. Тогда из взаимно однозначного соответствия f существует ровно одно значение l' такое, что $\alpha^{l'} = \beta$. Но

$$\alpha^{l'} = \beta = e_n(l \cdot P, Q) = e_n(P,Q)^l = \alpha^l,$$

таким образом, $l = l'$.

Данные рассуждения показывают, что мы можем редуцировать задачу нахождения дискретного логарифма в группе точек эллиптической кривой к задаче нахождения дискретного логарифма в группе n-х корней из единицы. Нам нужно будет определить линейно независимую точку $Q \in E[n]$ и наименьшее k такое, что $E[n] \subset E(\mathbb{F}_{q^k})$. Значение k должно быть мало на столько, на сколько это возможно, чтобы поле $\mathbb{F}_{q^k}$ не стало больше, чем это необходимо. Параметр k называется степенью вложения.

Степень вложения часто встречается в литературе как множитель безопасности [2]. Она определяет, насколько велико расширение поля $\mathbb{F}_{q^k}$, где выполняются вычисления для определения спаривания Вейля. Таким образом, для эффективного вычисления спаривания, k должно быть контролируемым. Произвольная кривая с высокой долей вероятности имеет большую степень вложения $k > (\log p)^2$ [3]. Таким образом, для более эффективного анализа MOV-редукции воспользуемся суперсингулярными кривыми со степенью вложения $k = 4$.

Вложение точек. Нам необходимо рассмотреть практическую проблему вложения точек из $E(\mathbb{F}_q)$ в $E(\mathbb{F}_{q^k})$, когда $q = p^e$. Пусть α порождает поле $\mathbb{F}_q$ и пусть $A(x)$ – минимальный многочлен элемента α. Пусть β порождает расширение поля $\mathbb{F}_{q^k}$ и пусть $B(x)$ является минимальным многочленом элемента β. Отметим, что $A(x)$ будет иметь корни (расщепляется) в $\mathbb{F}_{q^k}$. Теперь рассмотрим вложение

$$\Phi : \mathbb{F}_q \to \mathbb{F}_{q^k}, \qquad \alpha \to \bar{\alpha},$$

где $\bar{\alpha}$ – это корень $A(x)$ над $\mathbb{F}_{q^k}$. Таким образом, вложение точки (x, y) из $E(\mathbb{F}_q)$ в $E(\mathbb{F}_{q^k})$ является отображением $(x, y) \to (\Phi(x), \Phi(y))$.

Вложение сохраняет групповую структуру на точках и дает точку P, порождающую группу $\langle P \rangle$. Вложенная точка $\Phi(P)$ генерирует изоморфизм групп $\langle \Phi(P) \rangle \simeq \langle P \rangle$. Отметим, что если $e = 1$ в $q = p^e$, то Φ будет тождественным отображением.

Алгоритм редукции в случае суперсингулярной кривой. Для того, чтобы MOV-атака была эффективна, нам требуется знать параметры k, c и n_1 [4], поскольку нет быстрого способа вычисления этих параметров. В алгоритме 1 представлена MOV-редукции в случае суперсингулярной кривой.

АЛГОРИТМ 1. MOV-редукция для суперсингулярных кривых

Данные: суперсингулярная кривая $E/\mathbb{F}_q$, точки $P \in E(\mathbb{F}_q)$ и $R \in \langle P \rangle$
Результат: дискретный логарифм l точки R по основанию P

$t \leftarrow n$
пока $t > 0$ выполнять
$Q' \overset{R}{\leftarrow} E(F_{q^k})$;
$Q \leftarrow \frac{cn_1}{n} \cdot Q'$;
$\alpha \leftarrow e_n(P, Q)$
$\beta \leftarrow e_n(R, Q)$
$l' \leftarrow \log_\alpha \beta$
если $l' \cdot P = R$ то
вернуть: l'
$t \leftarrow 0$
$t \leftarrow t - 1$

Анализ редукции. Чтобы показать эффективность MOV-редукции, воспользуемся методом Копперсмита исчисления индексов, реализованным в системе компьютерной алгебры Magma [5]. Данный алгоритм, во-первых, вычисляет дискретный логарифм в группе точек суперсингулярной кривой над полем $\mathbb{F}_{2^m}$ характеристики 2; во-вторых, осуществляет MOV-редукцию; в-третьих, вычисляет дискретный логарифм в конечном расширении $\mathbb{F}_{2^{4m}}$. В качестве основного алгоритма воспользуемся методом ρ-Полларда.

Настройка оборудования. Испытания проводились на сервере DTUSunFireE6900 с четырьмя процессорами, каждый из которых имел тактовую частоту 1 ГГц. Magma не может запускать процессы в многопоточном режиме, поэтому замеры времени производились только для одного процессора с частотой 1 ГГц.

Скрипт был написан таким образом, чтобы мы могли менять расширение поля $\mathbb{F}_{2^m}$, для m = 1, …, 67. Для каждой кривой мы могли вычислить порядок группы точек и найти подгруппу наибольшего простого порядка. В тесте происходило следующее: вычислялись различные дискретные логарифмы n = 10 раз над группой точек кривой, осущест-влялась MOV-редукция в поле $\mathbb{F}_{2^{4m}}$ и затем в этом поле применялся алгоритм исчисления индексов. Скрипт был составлен таким образом, что вначале один раз запускался алгоритм исчисления индексов, причем предварительные вычисления выполнялись одновременно с основными. В последующих n вычислениях предварительные расчеты уже не проводились. Это не только повысило производительность, но и позволило лучше оценить работу программы, поскольку основные вычисления были отделены от предварительных. Результаты работы алгоритма можно видеть в табл.

ТАБЛИЦА. Время работы ЦП в секундах при вычислении MOV-редукции для кривой $E/\mathbb{F}_2$: $y^2 + y = x^3 + x + 1$.

m	Dlog в $\langle P \rangle$	Редукция	IC пред. выч.	IC основ. выч.
3	0.000	0.001	0.000	0.000
5	0.000	0.001	0.000	0.000
7	0.000	0.005	0.000	0.001
9	0.001	0.009	0.009	0.001
11	0.001	0.010	0.000	0.001
13	0.006	0.013	0.000	0.002
15	0.005	0.015	0.007	0.003
17	0.009	0.023	0.007	0.003
19	0.001	0.016	0.017	0.003
21	0.021	0.025	0.012	0.008
23	0.013	0.024	0.024	0.006
25	0.035	0.047	0.015	0.015
27	0.039	0.048	0.023	0.017
29	0.297	0.059	25.672	2.068
31	0.026	0.032	29.565	4.725
33	0.092	0.054	0.031	0.019
35	0.270	0.077	0.079	0.041
37	0.504	0.089	37.859	3.921
39	0.032	0.045	0.067	0.013
41	0.245	0.094	44.914	7.516
43	44.362	0.194	57.809	17.541
45	0.039	0.056	0.132	0.018
47	3.571	0.128	453.131	61.959
49	6.141	0.142	568.618	69.262
51	0.036	0.066	1460.873	97.877
53	1796.178	0.270	1456.450	128.200
55	79.714	0.248	1756.489	155.571
57	24.216	0.206	2017.111	227.679
59	0.052	0.103	2025.859	234.541
61	27.234	0.274	2896.387	281.013
63	10.452	0.260	3782.372	391.738
65	0.370	0.158	5989.431	450.829

Результаты. По полученным данным не удается однозначно определить эффективность MOV-редукции. В случае m = 33, 35, 39, 45, длительность основных и предварительных вычислений существенно отклонялась от планируемого времени, которое, как ожидалось, должно строго возрастать. Возможно, это объясняется тем, что в Magma присутствуют некие недокументированные механизмы, поскольку на основании имеющейся документации не ясно, почему эти методы работают быстрее, чем алгоритм исчисления индексов. Заметим, что в случае, когда m = 53, метод исчисления индексов работает быстрее, чем общий алгоритм дискретного логарифмирования для больших подгрупп. Это важное наблюдение наталкивает на мысль о том, что в данном случае MOV-редукция сработала эффективно

и метод исчисления индексов в данном случае гораздо быстрее общего алгоритма.

Список используемых источников

1. Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing // Журнал математической криптологии. Нью-Йорк, 2004. № 17 (4). PP. 297–319.

2. Степень расширения поля [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%81%D1%88%D0%B8%D1%80%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE%D0%BB%D1%8F

3. Balasubramanian R. and Koblitz Neil The impropability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm // J. Cryptol. 11(2):141–145, 1998.

4. David Møller Hansen. Pairing-based Cryptography. A short signature scheme using the Weil pairing. Магистерская диссертация, 2009.

5. Wieb Bosma, John Cannon, and Catherine Playoust. The magma algebra system i: the user language. J. Symb. Comput., 24 (3-4): 235-265, 1997.

УДК 681.5.017
ГРНТИ 50.43.19

ИССЛЕДОВАНИЕ ТЕХНОЛОГИЙ СОЗДАНИЯ «УМНОГО ДОМА»

В. Л. Литвинов, А. А. Макаров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире быстрыми темпами развиваются автоматические системы управления. Автоматизация в большей мере коснулась промышленности и производства, но с конца прошлого века стала появляться система «умный дом», которая позволяет сделать более комфортной жизнь ее пользователей. Система «умный дом» подразумевает автоматизацию обычных повседневных действий людей, производимых с бытовой техникой и системами жизнеобеспечения. С появлением интернета вещей системы «умного дома» стали гораздо продуктивнее, появилась возможность удалённо получать информацию о состоянии своего дома или управлять техникой в нем. В работе рассмотрено гибкое решение системы «умного дома» на базе платформы Arduino.

«умный дом», автоматизация, управление, интернет вещей, Arduino.

«Умный дом» – это система коммуникаций здания, объединённая при помощи различных устройств так, чтобы в нем было удобно его пользователям. Данная система подразумевает максимальную автоматизацию возможных жизненных процессов, например управление светом, системой

микроклимата дома, различными бытовыми приборами. Кроме автоматизации в «умном доме» предусматривается повышение безопасности жилища с использований различных сигнализаций, например пожарной сигнализации, системы обнаружения движения, системы сигнализации протечек воды или газа, а также системы видеонаблюдения. «Умный дом» настроит работу всех систем в соответствии с пожеланием человека, временем суток, его положением в доме, погодой, внешней освещённостью для обеспечения комфортного состояния дома внутри [1].

Для создания умного дома необходимо наличие ряда устройств:

1. Датчики окружающей среды (освещенности, температуры, влажности, движения и т. д.).

2. Контроллер «умного дома».

3. «Умные устройства».

Рассмотрим пример реализации системы управления микроклиматом комнаты. Структурная схема системы показана на рис. 1 (см. ниже). В систему входит контроллер (Кн), датчик температуры (ДТ), датчик влажности (ДВ), панель управления (ПУ), радиатор (Р) системы отопления с краном (Кр), инфракрасный обогреватель (ИКО), увлажнитель (У), кондиционер (К). Пользователь при помощи панели управления задаёт желаемую температуру воздуха и влажность внутри комнаты. Контроллер получает сведения с датчиков температуры и влажности и сравнивает полученные значения с заданными. Если температура ниже заданной, на кран подаётся команда открытия. Если необходимая температура не достигнута, включается ИК обогреватель. Если же измеренная температура выше заданной, то выключается обогреватель и закрывается кран. При невозможности снизить до нужного уровня, включается кондиционер. Так же происходит увлажнение воздуха. Кроме того, если в систему добавить датчик присутствия, то можно ее запрограммировать, чтобы в отсутствие в комнате людей не производилось увлажнение и излишний обогрев или кондиционирование, таким образом, данная система позволит не только повысить комфорт, но и значительно снизить потребление тепловой и электрической энергии, что приведёт в свою очередь к экономии средств.

Это далеко не единственная функция «умного дома». Полный набор возможностей данной системы будет зависеть от добавленных в неё «умных устройств».

«Умным устройством» считается такое устройство, которое выполняет свои функции без вмешательства пользователя. Есть несколько вариантов того, как устройство становится «умным».

Первый вариант – за счёт изменения своей конструкции: эта конструкция может быть таковой, что поведение системы будет выглядеть разумным (например, увлажнитель со встроенным датчиком влажности). Такие устройства имеют высокую стоимость и не всегда приводят к корректным

результатам из-за того, что все датчики расположены в одном корпусе с исполнительным устройством, в результате собирают некорректные сведения.

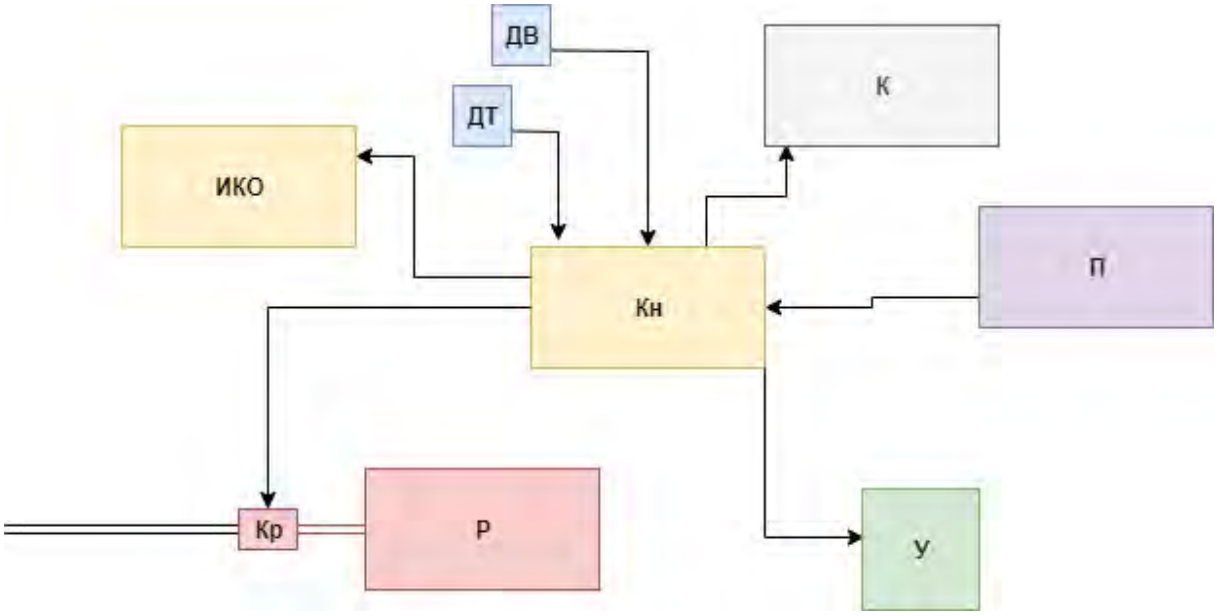


Рис. 1. Структурная схема системы климат-контроля «умного дома»

Второй вариант – за счёт «интеллектуализации» (оснащения системы сбора информации, её обработки и принятия решений). Такой подход позволяет обеспечить достаточно сложное и «разумное» поведение гораздо более простыми способами, чем за счёт создания соответствующей конструкции. При этом придётся для каждого устройства добавлять контроллер и набор датчиков.

Третий способ – поведение системы становится «разумным» за счёт того, что она взаимодействует с другими системами. Технология IoT (интернет вещей) как раз и предоставляет возможность каждому элементу «умного дома» объединиться в общую сеть и обмениваться информацией с другими системами. Таким образом, один и тот же датчик может давать сведения для работы нескольких устройств, и сами устройства будут работать в зависимости друг от друга под управлением общего контроллера. Кроме того, с появлением интернета вещей системы «умного дома» вышли на новый уровень, контроллер может присылать уведомления пользователю и получать от него команды для новых заданий удалённо.

На сегодняшний день на рынке существует большое количество предложений по созданию «умного дома». Некоторые из них подразумевают полное проектирование системы на этапе строительства или ремонта дома или квартиры, а некоторые являются готовыми решениями и предлагают внедрить систему без особых вмешательств в состояние здания. В нашей стране чаще встречаются вторые, так как с первым вариантом стоимость

«умного дома» близка к средней стоимости самого дома. Как правило, готовые решения умного дома состоят из следующих компонентов:

– контроллер;
– модули для увеличения количества выходов;
– контрольный блок;
– аккумулятор к блоку;
– реле;
– предохранители;
– видеокамеры;
– термостаты;
– микрофоны;
– датчики;
– GSM модем или Wi-Fi роутер;
– схема сборки.

На рынке готовых решений наиболее распространены:

– Xiaomi Smart Home Suite;
– Ростелеком;
– Redmond Smart Home.

Все они имеют как ряд преимуществ, так и ряд недостатков. Так «умный дом» от Xiaomi имеет большое число различных датчиков, невысокую стоимость, возможность удалённого управления всеми устройствами, но при этом имеет крепления датчиков невысокого качества и для российского рынка придётся использовать переходники под электрические розетки. Система от российского производителя Ростелеком стандартизирована под рынок нашей страны, но пока имеет очень малый спектр выбора устройств. В умном доме от Redmond самый широкий выбор устройств, так как данный производитель предлагает не только выключатели, видеокамеры и розетки, но и свою бытовую технику, оснащённую модулями для включения их в общую сеть «умного дома», но из-за этого техника сразу поднимается в цене в сравнении с аналогичными моделями.

Основным недостатком всех имеющихся на рынке систем является то, что каждая работает по своему протоколу, таким образом отсутствует возможность создать комбинированную систему с устройствами разных производителей. Кроме того, почти все из предложенных устройств используют облачный сервер, что в свою очередь может негативно сказаться на безопасности [2], так как в случае взлома учётной записи злоумышленник получит доступ не только к информации, а возможность управления всеми технологическими процессами дома или квартиры.

Наиболее эффективным было бы создание такой системы с использованием программируемых контроллеров. Они имеют низкую стоимость, просты в управлении и будут работать по гибкому алгоритму, который заложит программист. Таким образом, можно путём небольшого изменения

инженерных сетей дома создать полноценный «умный дом». К выключателям света добавить реле для управления светом с помощью контроллеров. С их помощью можно управлять любым устройством, которое имеет пульт дистанционного управления, так как бытовые пульты дистанционного управления работают с открытыми кодами, которые может выдавать контроллер при помощи передатчика. Контроллеры можно объединить между собой в сеть и, добавив в данную сеть локальный сервер, управлять всеми системами через смартфон или единую панель управления, находящуюся в той же сети. Функциональная схема предлагаемого решения представлена на рис. 2.

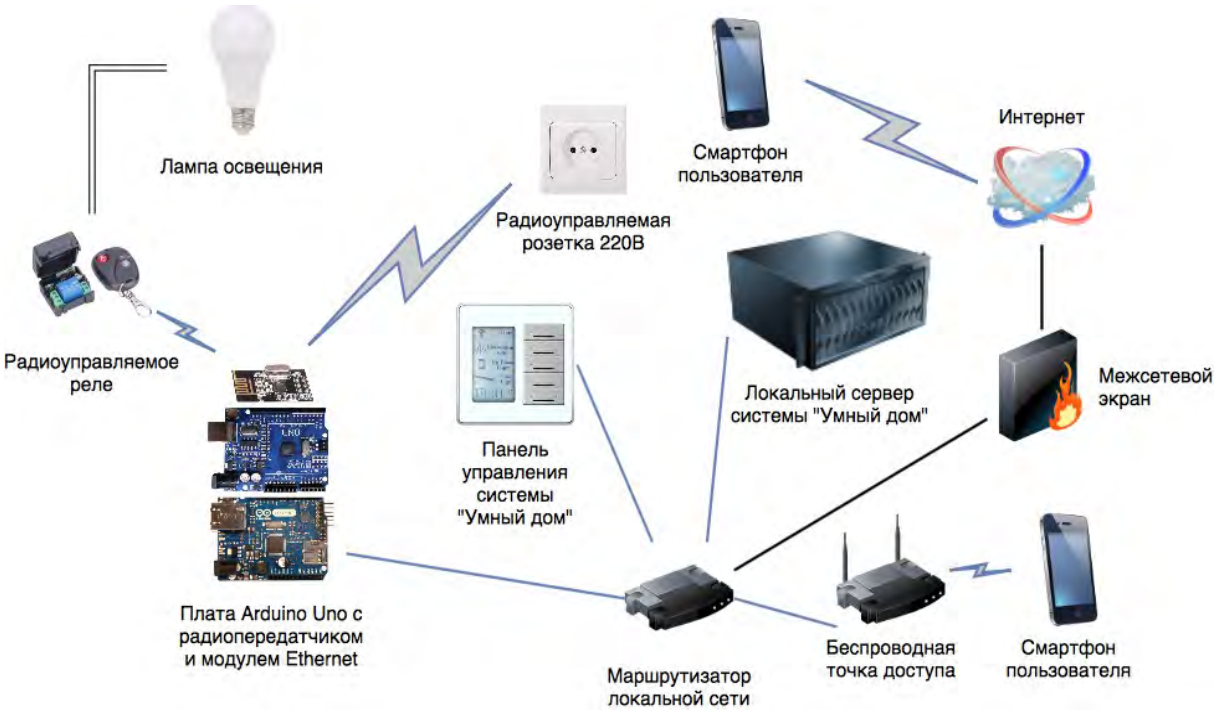


Рис. 2. Функциональная схема системы управления бытовыми приборами по радиоканалу

В качестве технологического базиса предлагается использовать дружелюбную платформу Arduino, имеющую бесплатная официальную среду программирования Arduino IDE, работающая под Windows, Mac OS или Linux.

Список используемых источников

1. Петин В. А. Создание умного дома на базе Arduino. М. : ДМК Пресс, 2018. 180 с.
2. Долгун В. О., Литвинов В. Л. Анализ протоколов информационной безопасности в IOT-среде // Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. 2017. С. 515–517.

УДК 004.89
ГРНТИ 28.23.37

СРАВНИТЕЛЬНЫЙ АНАЛИЗ НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ В ЗАДАЧАХ ОЦЕНКИ УРОВНЯ ЗНАНИЙ АБИТУРИЕНТОВ

В. Л. Литвинов, К. Б. Мурсалимова, Л. Д. Трофимова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье проведен сравнительный анализ нейросетевых моделей как подходов к оценке уровня знаний абитуриентов. На основании результатов анализа и классификации нейросетевых моделей введена система оценок интенсивности проявления критериев. Применен экспертный метод попарных сравнений для оценивания значения коэффициента важности каждого показателя. Также рассмотрена эффективность использования нейросетевых моделей для анализа различных видов деятельности предприятия.

нейронные сети, метод попарных сравнений, анализ деятельности предприятия.

Многие образовательные учреждения сталкиваются с проблемами постоянных ошибок и не соответствий при приеме и обработке документов абитуриентов. Для получения комплексной оценки знаний абитуриента требуется длительное время, четкая координация и формирование системы отбора соответствующей компетенции с учетом уровня знаний и достижений поступающего. Данные условия требуют подбора и усовершенствования соответствующих отборочных средств и технологий, методов накопления и анализа результатов, а также обработку аналитических оценок состояния на каждом этапе. При моделировании многокомпонентных, сложных систем и разработке методов структурирования, эффективным инструментом является нейронная система, представляющая собой систему искусственного интеллекта, которая, на основе обучения, с использованием метода обратного распространения ошибки, присваивает веса факторам, использующимся при проведении оценки уровня знаний абитуриента.

В работе проведен сравнительный анализ нейросетевых моделей на основе выделения показателей и введении системы оценок интенсивности проявления критериев в задачах определения уровня знаний абитуриентов.

Из-за огромного потока информации в период работы приема документов абитуриентов происходит недостаточная и длительная проверка данных. Нейросетевая модель (рис. 1) должна обладать определенными характеристиками и параметрами для оптимизации ресурсов и устранения некачественной работы.

Рис. 1. Схема нейросетевой модели

Классификация нейронных сетей [1] представлена на рис. 2.

Рис. 2. Классификация нейронных сетей

Нейронные сети (НС) по характеру обучения делятся на два типа: нейросети, использующие обучение с учителем и нейросети, использующие обучение без учителя.

По настройке весов различаются:

– сети с фиксированными связями – весовые коэффициенты нейронной сети выбираются сразу, исходя из условий задачи;

– сети с динамическими связями – для них в процессе обучения происходит настройка синаптических весов.

По типу входной информации можно выделить:

– аналоговая НС – входная информация представлена в форме действительных чисел;

– двоичная НС – вся входная информация в таких сетях представляется в виде нулей и единиц.

По модели нейронной сети можно выделить:

• Сети прямого распространения – все связи направлены строго от входных нейронов к выходным. К таким сетям относятся, например, простейший персептрон и многослойный персептрон.

• Реккурентные нейронные сети – сигнал с выходных нейронов или нейронов скрытого слоя частично передается обратно на входы нейронов входного слоя [2].

При формировании модели первым этапом является системный анализ, позволяющий в максимальной степени структурировать задачу. В рамках используемого подхода модель уровня знаний абитуриента можно представить в виде иерархической структуры, представленной на рис. 3.

Рис. 3. Схема уровня знаний абитуриента

На нижнем уровне оценивается множество данных, которые не подлежат дроблению на более мелкие и являются основой модели оценки уровня знаний абитуриентов. Особенностью отбора представленной модели является факт использования некоторой совокупности «базовых оценок» поступающего, как базиса, заложенных в личном деле, таких как результаты ЕГЭ, наличие аттестата с отличием, наличие портфолио и др.

Оценка уровня знаний абитуриентов нижнего уровня производится на основании показателей $x = (x_1, x_2, \ldots, x_n)$, в качестве которых могут выступать результаты ЕГЭ, наличие аттестата с отличием, наличие портфолио. Метод попарного сравнения позволяет выявить наивысшие рейтинги у различных абитуриентов по тому или иному показателю оценки через последовательное сравнение абитуриентов друг с другом [3].

Работа приемной комиссии предполагает обработку и отбор документов абитуриентов, поэтому необходимо сформировать систему показателей для интеллектуального отбора информации с учетом всех требований для предотвращения различных ошибок.

В зависимости от характера показателя оценки коэффициент может принимать различные допустимые значения и измеряться в разных шкалах (табл. 1, 2, 3).

ТАБЛИЦА 1. Шкала отбора по баллам ЕГЭ (по трём предметам)

Кол-во баллов (интервал баллов)	Уровень знаний	Критерии отбора уровня знаний
280–300	максимальный уровень	Не менее 280 набранных баллов
208–279	средний уровень	Не менее 208 набранных баллов
162–207	минимальный уровень	Не менее 162 набранных баллов
0–161	минимальный уровень не достигнут	Не более 161 набранных баллов

ТАБЛИЦА 2. Шкала отбора по аттестату

Средний балл аттестата	Уровень знаний	Критерии отбора уровня знаний
5.0	максимальный уровень	Не менее 5.0 средний балл аттестата
< 5.0	средний уровень	Менее 5.0 средний балл аттестата

ТАБЛИЦА 3. Шкала отбора по баллу портфолио

Кол-во баллов	Уровень достижений	Критерии отбора уровня знаний
7–10	максимальный уровень	Не менее 7 набранных баллов
2–6	средний уровень	Не менее 2 набранных баллов
1	минимальный уровень	Не менее 1 набранного балла

Предлагаемая процедура оценки знаний абитуриентов сводится к тому, что по результатам выполнения оценочных средств полученные баллы (по ЕГЭ, наличие аттестата с отличием, балл портфолио) вносятся в качестве входных параметров в предварительно обученную на обучаемой выборке нейросетевую модель, которая на выходе проводит ускоренный отбор абитуриентов, которые не подходят по данным показателям.

Исследование проблем оценки уровня знаний абитуриентов выводит нас на новый уровень – проблему управления данными с учетом минимизации ресурсов и улучшении эффективности на основе использования систем искусственного интеллекта.

Важным свойством нейросетевых моделей, определившим их растущую популярность, является отсутствие изначальной необходимости в каких-либо априорных предположениях о форме исследуемой зависимости, а также нелинейный характер формируемых моделей.

Процесс отбора показателей эффективности во многом субъективен, что, безусловно, осложняет выбор пользователя среди достаточно большого количества существующих показателей эффективности, отражающих тот или иной аспект деятельности организации [4]. Использование нейросетевых моделей позволяет использовать существенно большее количество исходных данных, по сравнению с традиционными статистическими методами, что безусловно повышает качество обработки данных и точность выполнения их анализа.

Список используемых источников

1. AIPORTAL. URL: http://www.aiportal.ru/articles/neural-networks/neural-networks.html (дата обращения: 20.03.2020).

2. Птицына Л. К. Интеллектуальные системы и технологии: учеб. пособие. СПб. : СПбГУТ, 2019. 231 с.

3. Алгазин Г. И., Чудова О. В. Информационные технологии комплексной оценки компетентности выпускника вуза // Вестник НГУ. Серия: Информационные технологии. 2009. № 3. URL: https://cyberleninka.ru/article/n/informatsionnye-tehnologii-kompleksnoy-otsenki-kompetentnosti-vypusknika-vuza (дата обращения: 20.03.2020).

4. Ширшов Е. В., Иванченко А. А. Применение кластерного анализа для оценки эффективности деятельности предприятия на основе использования нейросетевых технологий // Colloquium-journal. 2020. №5 (57). URL: https://cyberleninka.ru/article/n/primenenie-klasternogo-analiza-dlya-otsenki-effektivnosti-deyatelnosti-predpriyatiya-na-osnove-ispolzovaniya-neyrosetevyh-tehnologiy (дата обращения: 20.03.2020).

УДК 004.891.2
ГРНТИ 20.23.17

ИНТЕЛЛЕКТУАЛИЗАЦИЯ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ОТДЕЛА ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

В. Л. Литвинов, Л. С. Филимонов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрены основные понятия и проанализированы методы разработки и проектирования интеллектуальных систем поддержки принятия решений, в том числе методы имитационного моделирования. В работе предложена модель процесса технической поддержки пользователей информационной системы регионального управления в среде AnyLogic.

интеллектуальные системы поддержки принятия решений, экспертные системы, имитационное моделирование, методы разработки, Anylogic.

Одним из показателей успешной деятельности отдела технической поддержки является срок обработки заявки. Необходимо быстро и корректно направить заявку исполнителю, который способен решить ее максимально качественно и в кратчайшие сроки. При этом необходимо учитывать текущую загрузку исполнителя. Маршрутизация заявки от пользователя к исполнителю через несколько линий поддержки становится рутинной задачей, а при назначении заявок лицу, принимающему решение (ЛПР), приходится руководствоваться прежде всего эмпирическими данными, что может привести к увеличению рисков принятия неверного решения.

При этом с ростом накопленной информации о поступающих заявках и показателей работы операторов технической поддержки появляется возможность автоматизации процесса маршрутизации. Использование интеллектуальных систем поддержки принятия решения позволяет сократить сроки обработки заявок, увеличить скорость их маршрутизации без ущерба качеству работы технической поддержки.

Интеллектуальная СППР (ИСППР) – это такая система, которая ассистирует ЛПР в принятии решений, используя инструментарии анализа больших данных, моделирования и визуализации, обладает дружелюбным интерфейсом, устойчива по качеству, интерактивна и гибка по настройкам.

Среди разнообразных инструментов СППР важное место занимает имитационное моделирование как основа поливариантного прогнозирования и анализа систем высокой степени сложности. Одним из мировых лидеров в этой области является имитационная платформа AnyLogic [4], которая

позволяет создавать детализированные виртуальные среды для обучения и тестирования интеллектуальных систем. Имеется возможность запускать модели в облаке или использовать открытый API для создания собственных приложений. Поддерживается генерирование неограниченного количества релевантных, выверенных, структурированных и размеченных синтетических входных данных для обучения с учителем. Такие данные могут быть использованы в машинном обучении, аналитике и Data Mining. Тестирование работы спроектированной системы осуществляется в реалистичной и безрисковой среде. Поведение обученных систем можно исследовать и анализировать с помощью имитационной модели.

С помощью имитационной модели опишем процесс предоставления технической поддержки пользователям информационной системы регионального управления.

В техническую поддержку поступают заявки с элемента **source** с интенсивностью 8.9 заявок в час. Далее с вероятностями $p11$, $p12$, $p13$, $p14$ на элементе selectOutput1 заявки распределяются по четырем отделам:

Отдел 1 – Первая линия поддержки (рис. 1). На элементе selectOutput2 поток заявок с вероятностями $p21$ и $p22$ распределяется по двум очередям (queue_dp_1 и queue_dp_1_05) с двумя задержками (delay_dp_1, delay_dp_1_05). Данные элементы отражают наличие двух групп исполнителей, решающих разные задачи. На элементах selectOutput3, selectOutput3_1 поток заявок распределяется по шести специалистам поддержки 1–6 (queue_dp_1_1 и delay_dp_1_1, queue_dp_1_2 и delay_dp_1_2 … queue_dp_1_6 и delay_dp_1_6) с вероятностями $p31$, $p32$, $p33$, $p34$, $p35$, $p36$. На элементе selectOutput4 поток заявок, поступивший с элементов queue_dp_1_05 и delay_dp_1_05, с вероятностями $p46$, $p47$, $p48$ распределяются по специалистам 6 – 8 (queue_dp_1_6 и delay_dp_1_6, queue_dp_1_7 и delay_dp_1_7 и queue_dp_1_8 и delay_dp_1_8). Соответственно специалист 6 (queue_dp_1_6 и delay_dp_1_6) получает и выполняет заявки из обеих очередей (queue_dp_1 и queue_dp_1_05), но с разными вероятностями ($p36$ и $p46$, соответственно). Поток заявок от специалистов 1–8 поступает на элемент selectOutput5, где с вероятностью: $p51$ – заявка решена и попадает на элемент sink для уничтожения, $p52$ – заявка эскалируется на Отдел 2, $p53$ – заявка эскалируется на Отдел 3, $p54$ – заявка эскалируется на Отдел 4.

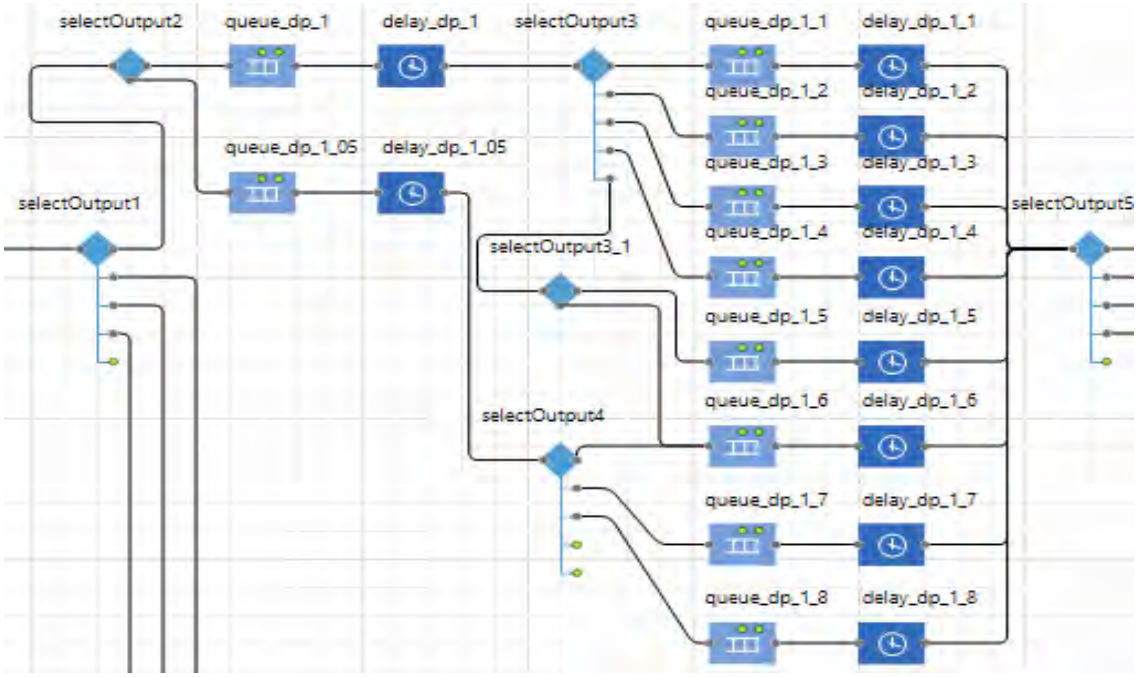


Рис. 1. Модель отдела 1 в AnyLogic

Отдел 2 (рис. 2). Заявки в отдел приходят либо напрямую из элемента selectOutput1 с вероятностью $p12$, либо с элемента selectOutput5 с вероятностью $p52$, после обработки этих заявок в Отделе 1. Отдел 2 имеет собственную очередь заявок queue_dp_2 и задержку delay_dp_2, регламентирующую нахождение заявок в общей очереди, до распределения по специалистам. В этом отделе 3 специалиста. Заявки распределяются на элементе selectOutput6 с вероятностями $p61$, $p62$, $p63$ по специалистам (queue_dp_2_1 и delay_dp_2_1, queue_dp_2_2 и delay_dp_2_2 и queue_dp_2_3 и delay_dp_2_3). После обработки заявок с соответствующей специалисту задержкой они поступают на элемент selectOutput7, где с вероятностью $p71$ – заявка решена и попадает на элемент sink для уничтожения, $p72$ – заявка эскалируется на Отдел 4.

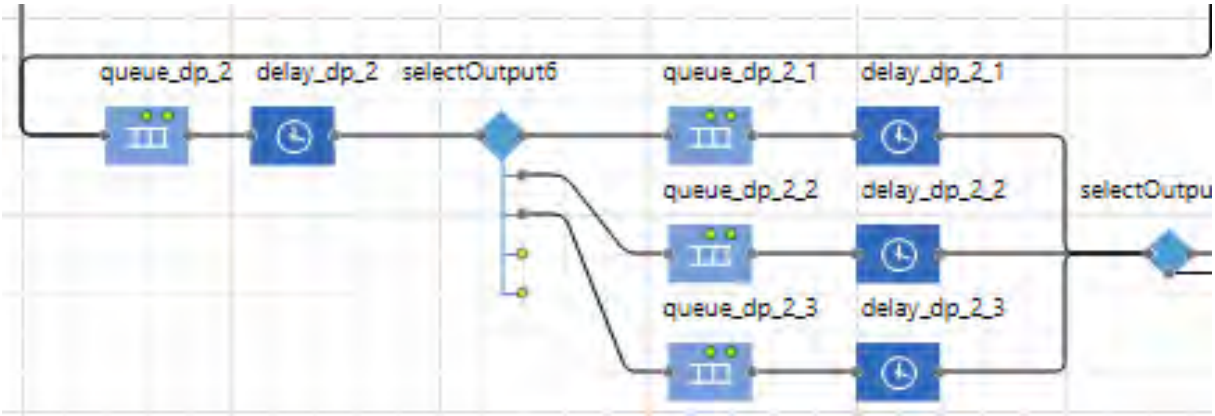


Рис. 2. Модель отдела 2 в AnyLogic

По аналогии построим имитационные модели отдела и отдела 4 (рис. 3 и 4).

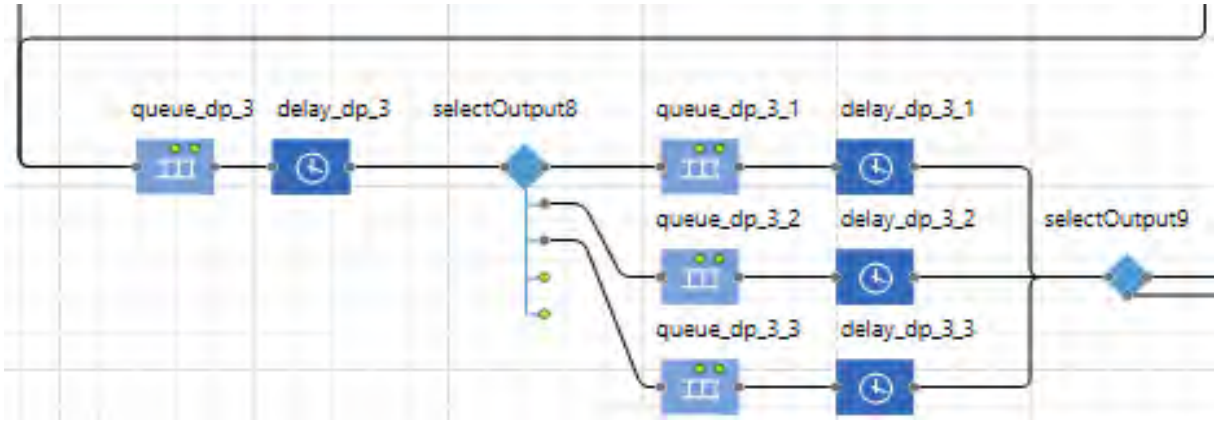


Рис. 3. Модель отдела 3 в AnyLogic

После обработки заявок с соответствующей специалисту задержкой они поступают на элемент sink для уничтожения. Отдел 4 решает 100 % поступающих на него заявок, так как сотрудники данного отдела обладают всеми необходимыми компетенциями.

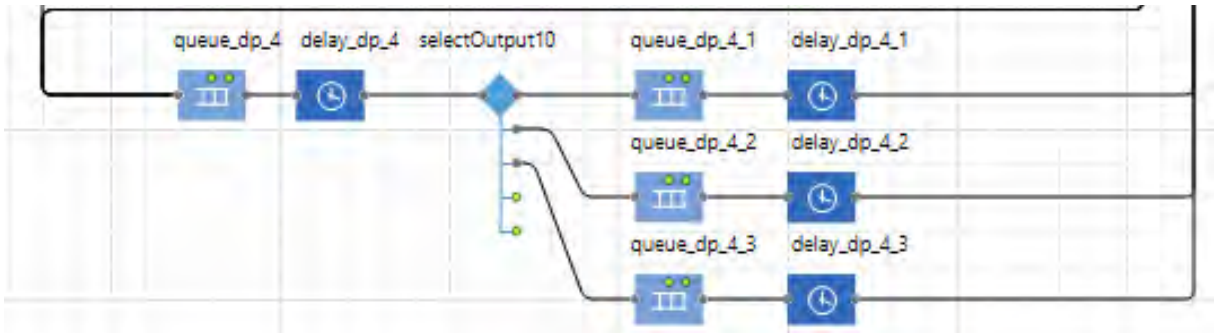


Рис. 4. Модель отдела 4 в AnyLogic

Ниже приведена таблица свойств элементов, используемых в модели технической поддержки информационной системы регионального управления (табл. 1), а также таблица параметров вероятности распределения агентов, генерируемых в элементе source между отделами и специалистами каждого отдела (табл. 2).

Результаты имитационного моделирования, представленные на рис. 5, позволяют оценить эффективность работы отдела.

ТАБЛИЦА 1. Свойства элементов имитационной модели

Элемент	Свойство	Значение
source	Прибывают согласно: Интенсивность прибытия:	Интенсивности 8,9

Элемент	Свойство	Значение
	Максимальное количество прибытий:	400
queue queue_dp_1 queue_dp_1_05	Вместимость:	400
queue_dp_1_1 queue_dp_1_2 queue_dp_1_3 queue_dp_1_4 queue_dp_1_5 queue_dp_1_6 queue_dp_1_7 queue_dp_1_8 queue_dp_2_1 queue_dp_2_2 queue_dp_2_3 queue_dp_3_1 queue_dp_3_2 queue_dp_3_3 queue_dp_4_1 queue_dp_4_2 queue_dp_4_3	Вместимость:	5
delay_dp_1 delay_dp_1_05	Время задержки: Вместимость:	triangular(0.5, 1, 1.5) минуты 1
delay_dp_1_1 delay_dp_1_2 delay_dp_1_3 delay_dp_1_4 delay_dp_1_5	Время задержки: Вместимость:	triangular(0.002, 5.9, 0.25) часы 2
delay_dp_1_6	Время задержки: Вместимость:	triangular(0.002, 9, 0.2) часы 2
delay_dp_1_7 delay_dp_1_8	Время задержки: Вместимость:	triangular(0.016, 9, 0.05) часы 2
delay_dp_2_1 delay_dp_2_2 delay_dp_2_3	Время задержки: Вместимость:	triangular(0.03, 6, 0.16) часы 1
delay_dp_3_1 delay_dp_3_2 delay_dp_3_3	Время задержки: Вместимость:	triangular(0.016, 5.5, 0.03) часы 2
delay_dp_4_1 delay_dp_4_2 delay_dp_4_3	Время задержки: Вместимость:	triangular(0.01, 6, 0.1) часы 1

ТАБЛИЦА 2. Значение вероятностей в распределения заявок в имитационной модели

Параметр	Значение	Параметр	Значение	Параметр	Значение
$p11$	0,66	$p46$	0,33	$p71$	0,99
$p12$	0,01	$p47$	0,33	$p72$	0,01

Параметр	Значение	Параметр	Значение	Параметр	Значение
*p*13	0,32	*p*48	0,33	*p*81	0,33
*p*14	0,01	*p*51	0,825	*p*82	0,33
*p*21	0,7	*p*52	0,04	*p*83	0,33
*p*22	0,3	*p*53	0,035	*p*91	0,99
*p*31	0,195	*p*54	0,1	*p*92	0,01
*p*32	0,195	*p*61	0,33	*p*101	0,33
*p*33	0,195	*p*62	0,33	*p*102	0,33
*p*34	0,195	*p*63	0,33	*p*103	0,33
*p*35	0,195				
*p*36	0,025				

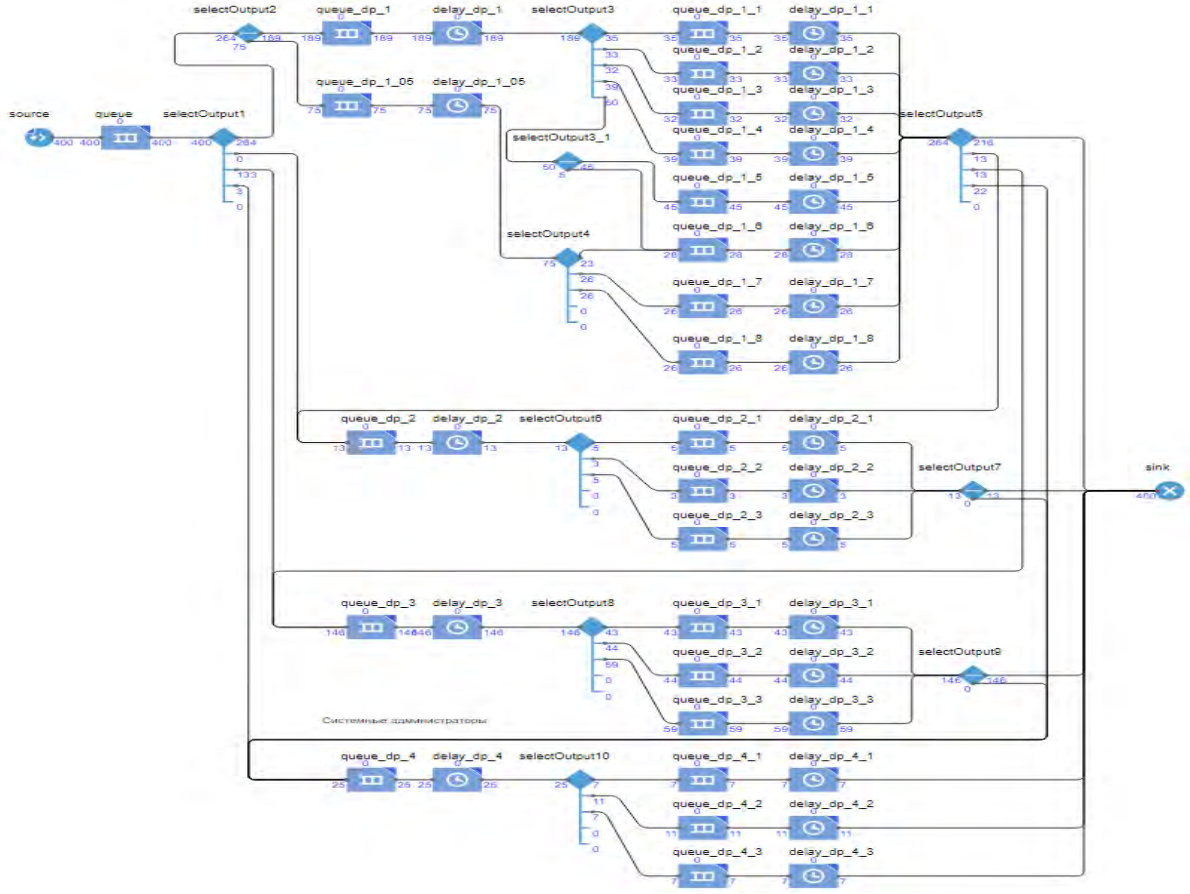


Рис. 5. Результаты имитационного моделирования

Таким образом, будущее интеллектуальных СППР за гибкостью решений. Ни один из известных способов (классические модели, машинное обучение, теория игр) не универсален с точки зрения эффективности для всех задач, должны сочетаться различные инструменты моделирования.

Список используемых источников

1. Компания AnyLogic [Электронный ресурс]. URL: https://www.AnyLogic.ru/ features/artificial-intelligence/ (дата обращения: 26.02.2020).

УДК 004.891.2
ГРНТИ 50.39.02

ИССЛЕДОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ МЕТОДОВ МОНИТОРИНГА ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

В. Л. Литвинов, М. В. Шальков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Для успешной деятельности инфокоммуникационных систем необходимо иметь возможность оперативно реагировать и устранять все возникающие в процессе эксплуатации отклонения в работе системы и не допускать их эскалации. Именно по этой причине одно из ключевых мест в работе инфокоммуникационных систем занимает её всесторонний мониторинг. В работе оцениваются варианты существующих методов мониторинга инфокоммуникационных систем. Рассмотрены сущность и содержание основных понятий мониторинга. Проведено исследование предпосылок развертывания системы мониторинга. Проанализированы способы сбора, хранения и обработки информации системами мониторинга, а также примеры сценариев использования полученных данных. Рассмотрены подходы построения систем мониторинга, а также её ключевые составляющие.

системы мониторинга, Service Level Agreement, инфокоммуникационные системы, сервис, сервер, сетевое оборудование.

Окружающий мир находится в постоянном, непрерывном изменении. Появляются новые города, современные высокотехнологичные трассы, небоскребы, тоннели длинной в десятки километров, мосты, соединяющие материки и т. д. На современном этапе развития человеческой деятельности все это не может существовать без качественной, тщательно спланированной и распределенной инфокоммуникационной системы. Однако, для успешной деятельности всей системы необходимо иметь возможность оперативно реагировать и устранять все возникающие в процессе эксплуатации отклонения в работе системы и не допускать их эскалации. Именно по этой причине одно из ключевых мест в работе инфокоммуникационных систем занимает её всесторонний мониторинг.

Мониторинг [1] – составная часть управления информационной инфраструктурой, которая представляет собой процесс постоянного наблюдения и периодического анализа параметров инфокоммуникационной системы с отслеживанием динамики изменений, результатом которого является совокупность измеренных значений параметров, получаемых на примыкающих интервалах времени и оценивание на их основе состояния инфокоммуникационной системы.

Вне зависимости от размеров компании необходимо, чтобы технические специалисты, отвечающие за тот или иной компонент системы, получили исчерпывающую информацию о поломках или проблемах в инфраструктуре раньше, или, в крайнем случае, одновременно с пользователями системы. Постоянный мониторинг позволяет избежать простоев в работе инфраструктуры, поддерживать ключевые бизнес-сервисы в рабочем состоянии и сохранять необходимый, отвечающий установленным показателям качества, уровень работы системы, планировать модернизацию системы на основе получаемых показателей, а также эффективно предотвращать возникновение неполадок.

Предпосылками появления систем мониторинга можно обозначить следующее:

1. Отсутствие мониторинга загрузки инфокоммуникационных систем.
2. Отсутствие оперативной информации по работе всех составляющих инфокоммуникационных систем.
3. Большие трудозатраты на изучение журналов системы на наличие в них информации о сбоях.
4. Сложная и распределенная структура инфокоммуникационных систем.
5. Часто пользователи системы узнают о проблемах раньше, чем технические специалисты.
6. Длительные простои системы ввиду сложности локализации проблемы.

На данный момент существующие системы мониторинга можно разделить на активные и пассивные. Пассивный мониторинг представляет собой только получение данных в режиме реального времени с целью их сбора, обработки и хранения. Такой подход позволяет оперативно и точечно реагировать на выявленные проблемы или аномальное поведение компонентов системы, которое может привести к неполадкам в работе инфраструктуры. Однако, диагностика и поиск неисправностей происходит уже после обнаружения неполадок и наличия проблем в работе аппаратного или программного обеспечения.

Под активным мониторингом подразумевается мониторинг, который способен не только обеспечивать удаленный мониторинг в режиме реального времени и регулярно проверять состояние компонентов системы,

но и обладает возможностью реагирования на входные данные, т. е. при возникновении определенных условий или параметров производится какое-то действие.

Все современные системы мониторинга построены с использованием архитектуры клиент-сервер. Их взаимодействие обеспечивается с помощью стандартных, либо проприетарных протоколов. Сервер формирует запросы, собирает и обрабатывает информацию, на основе которой создает оповещения и структурирует информацию для отображения в графическом или ином виде. Клиент кэширует или хранит в оперативной памяти только ту информацию, которая используется в данный момент времени. Основное его предназначение – отображение всей имеющейся информации в консоли управления и возможность конфигурирования системы мониторинга.

Для построения системы мониторинга используют два подхода:

– подход от инфраструктуры – организация наблюдения за ключевыми компонентами отдельными техническими специалистами, основываясь на их специализации;

– подход от сервисов – формирование списка услуг, для каждого из которых разрабатывается своя сервис-ресурсная модель, отражающая взаимодействие между сервисом и другими компонентами инфраструктуры, нужными для его работы. Использование данной модели способствует повышению полезности системы мониторинга не только для технических специалистов поддержки, но и других служб.

При использовании сервисного подхода для каждого сервиса задается определенный уровень качества его предоставления, после чего формируется Соглашение об уровне качества сервисов [2] (*Service Level Agreement*, SLA). Согласно SLA, система осуществляет сбор и хранение информации о качестве предоставления сервисов, на базе которой формируются отчеты, которые в дальнейшем помогают осуществлять оценку уровня предоставления сервисов, реорганизацию деятельности и дальнейшую модернизацию инфокоммуникационной системы.

Активные системы мониторинга инфокоммуникационных систем работают по следующему принципу: система мониторинга опрашивает некоторый узел (оборудование, программное обеспечение), получает результат запроса и сравнивает его с установленными параметрами. К примеру, для проверки загруженности активного оборудования используется протокол SNMP. Система мониторинга опрашивает устройство, получает необходимое значение, сравнивает со значением, установленным для такого типа устройств и в зависимости от результата, создает оповещение, либо выполняет заданный сценарий управления данным устройством.

SNMP – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектуры TCP/UDP [3]. К поддерживающим SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие

станции, принтеры, модемные стойки и другие. Кроме данного протокола у систем мониторинга имеются свои, проприетарные протоколы для реализации обмена данными, но SNMP остается наиболее популярным и используется как в активном, так и в пассивном мониторинге.

Для определения доступности почтового протокола SMTP, система мониторинга опрашивает 25-й порт TCP/IP. При подключении система мониторинга представляется почтовому серверу с помощью команды HELO/EHLO, в ответ на которую получает список параметров.

Другой пример – проверка свободного места на системном диске. Система мониторинга опрашивает сервер, получает текущие значения использования логического диска системы и сравнивает его с предельно допустимым значением, например, 85 %. Если диск заполнен более чем на 85 %, система мониторинга должна дать оповещение. Такой метод называется методом проверки допустимых значений опрашиваемых величин.

В процессе конфигурирования системы необходимо устанавливать четкие критерии того, что является нормой для работы системы, а что – потенциальной проблемой или сбоем и может привести к аварийной ситуации в будущем. Системы мониторинга способны прогнозировать поведение объектов наблюдения на шаг вперед, но в распределенных системах этого может быть не всегда достаточно. Например, распределенная инфраструктура, включающая в себя несколько объектов, представляющих собой один сервис, в случае выхода из строя одного из узлов распределит нагрузку на оставшихся. Система мониторинга при оценивании нагрузки на центральный процессор может ошибочно воспринять данную ситуацию как критическую, когда на самом деле это ожидаемо для рассматриваемой ситуации. Подобные ложные сообщения могут скрывать под собой реальные сбои в работе системы, что может перейти в создание аварийной ситуации как для всей системы в целом, так и для сервиса в частности.

Исходя из проведенного анализа, можно сделать вывод, что для корректной оценки работы инфокоммуникационной системы необходимо создать комплексную систему мониторинга, способную гибко оценивать работоспособность системы.

Комплексная система мониторинга включает в себя:

– мониторинг сетей передачи данных и их производительность;
– мониторинг и управление конфигурациями сетевого оборудования;
– мониторинг производительности серверов;
– мониторинг аппаратных сбоев на серверах;
– мониторинг сбоев операционной системы;
– мониторинг приложений и их сервисов;
– мониторинг сбоев в приложениях;
– мониторинг производительности приложений;
– мониторинг сервисов;

– центр управления ресурсами;
– отчетность.

При выборе системы мониторинга следует обратить внимание на уровень их защищенности от возникновения критических ситуаций:

– отказ отдельных элементов системы;
– отказ системы в целом;
– воздействие на систему извне.

Учитывая, что в подобных системах используется центральный сервер, который берет на себя всю вычислительную нагрузку, необходимо исключить вероятность угрозы остановки всей системы в целом ввиду его выхода из строя. Для этой цели необходимо создать элемент самодиагностики системы, который самостоятельно отслеживает состояние своих компонентов, и, в случае необходимости, перераспределяет задачи вышедшего из строя узла.

Таким образом, в работе рассмотрены сущность и содержание основных понятий мониторинга инфокоммуникационных сетей. Проведен анализ существующих способов мониторинга инфокоммуникационных систем. Рассмотрены методы систем мониторинга, а также подходы их построения. По мере модернизации компаний, усложнения существующих систем и увеличении автоматизации, значимость систем мониторинга будет непрерывно расти.

Список используемых источников

1. Мониторинг [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Мониторинг (дата обращения: 07.03.2020).

2. Service Level Agreement [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Service-level_agreement (дата обращения: 07.03.2020).

3. A Simple Network Management Protocol (SNMP) [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/SNMP (дата обращения: 07.03.2020).

УДК 004.725.4
ГРНТИ 50.41.23

ИСПОЛЬЗОВАНИЕ KUBERNETES ДЛЯ УПРАВЛЕНИЯ РАСПРОСТРАНЁННОЙ СИСТЕМЫ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ В СЕТЯХ 5G

А. А. Лоборчук, А. С. А. Мутханна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье будет проанализировано использование открытого программного обеспечения Kubernetes для автоматизации развёртывания, масштабирования контейнеризированных приложений на базе Docker и управления ими в рамках программно-конфигурируемой сети для построения и управления распространённой системы граничных вычислений в сетях нового поколения 5G. Так же будет уделено внимание новым принципам, преимуществам и дальнейшим перспективам построения сетей на базе распространенной системы граничных вычислений и управление развернутой системой как программно-конфигурируемой сетью с контейнезированными приложениями, как со стороны передачи данных от клиента к серверу, так и со стороны управления данной сетью.

5G, SDN, MEC, Kubernetes.

На формирование абонентских сетей пятого поколения влияют 3 фактора.

Во-первых, большинство людей используют именно мобильный телефон для доступа в интернет. По статистике [1] в 2019 году интернет насчитывал 4,39 миллиарда людей, а доступ с мобильных устройств осуществляет почти 4 миллиарда человек. При этом 92 % процента всех пользователей смотрят видео онлайн.

Во-вторых, ожидается [2], что в 2030 году количество устройств интернета вещей будет насчитывать более 50 миллиардов устройств.

В-третьих, на сегодняшний момент все большее количество компаний переходят на open source решения [3] в программном обеспечении.

В данной статье будет рассмотрено 2 технологии. Это использование границ облачных вычислений в качестве физической архитектуры построения абонентских сетей нового поколения, и Kubernetes для построения и управление NFV-SDN сети.

Облачные вычисления на границе сети

В основе идеи построения границы облачных вычислений (MEC) лежит простая идея, что трафик не обязательно сразу же передавать дальше,

его можно обрабатывать непосредственно возле узла связи и передать только в определенных случаях.

При использовании границы облачных вычислений в сетях с устройствами интернета вещей позволяет снизить издержки, за счет обработки входящей информации практически локально. К примеру, важной информации можно считать:

– передача усредненных значений за больший промежуток времени;

– передача значений, только если они выходят за установленные границы;

– локального хранения информации;

– установка нескольких контроллеров для обработки информации и управлением определенной части сети и одного оркестратора;

– развертывание приложений на основе нейронных сетей или машинного/глубокого обучения для минимизации задержек.

Использование границы облачных вычислений позволяет снизить нагрузку на сеть и предоставить большие вычислительные мощности с малым временем отклика. Но большое количество вычислительных серверов и СХД, их бесперебойная работа и вариативность применений в каждом отдельно взятом случае вызывают сложность в управление сетью, но и увеличивают количество необходимых инженеров для первичной настройки сети и поддержанию ее в рабочем состоянии.

Система оркестрации контейнеров Kubernetes

Для решения проблем, возникающих при использовании MEC, возможно использовать open source систему для автоматизации развёртывания, масштабирования контейнеризированных приложений и управления ими – Kubernetes.

В качестве основы для Kubernetes используются распределенное файловое хранилище, поверх которого работают виртуальные контейнеры Docker, iptables и т. д. Данное решение не только позволяет относиться ко всей сети и серверам граничных вычислений как к различным классам в программе.

Во-первых, использование технологии контейнеризации Docker позволяет отделить уровень операционной системы от уровня приложений, а также унифицировать используемые образы приложений во всей сети;

Во-вторых, управление сетью можно полностью автоматизировать с помощью скриптов;

В-третьих, появляется возможность изменять не только программное обеспечение на серверах, но и логические связи между ними: в режиме реального времени балансировать нагрузку между различными серверами.

В-четвертых, благодаря использованию идеологии DevOps присутствует возможность уменьшения линейного персонала благодаря автоматизации процесса жизни продукта.

Сеть, создаваемую с помощью технологий Kubernetes и MEC, можно разделить на 3 сегмента:

- Уровень физических серверов MEC. На этом уровне мы взаимодействуем с физическим оборудованием и связями между ним.
- Уровень FVN. Этот уровень позволяет абстрагироваться от особенностей физической реализации серверов и перейти к развертыванию унифицированных контейнеров с приложениями на базе Docker.
- Уровень SDN. Данный уровень объединяет независимые контейнеры в сервисы и позволяет управлять связями между ними.

Также следует отдельно обратить внимание на использование связки двух технологий, MEC и Kubernetes, в качестве архитектуры для обработки информации в сетях VANET [4].

Сеть VANET – это автомобильные самоорганизующиеся сети с большой нагрузкой для вычислительных серверов и необходимостью иметь минимальную задержку.

К преимуществам данного решения можно отнести:

– автоматизацию управления;

– абстракцию от физического уровня управления сети;

– возможность гибкой конфигурации уже настроенных серверов и их быстрое изменение;

– использование менее производительного оборудования в автомобилях и перенос вычислений на «общие» сервера.

Сравнительное тестирование скорости доступа

В качестве методики сравнения скорости доступа к серверам в сети интернет и серверу MEC, была выбрана утилита ping, как наиболее простая для оценки задержек сети. Сервером с IP 192.168.1.141 является сервер MEC с развернутым на нем nginx на базе Kubernetes. Для получения более точной настройки было произведено 500 запросов ping, с интервалом в 0,1 секунду к серверам расположенными в разных частях света. Результат показан в табл. и на рис.

ТАБЛИЦА. Результат тестирования

Имя сервера	Минимальное значение запроса	Среднее значение запроса	Максимальное значение запроса	Стандартное отклонение времени запроса
0.oceania.pool.ntp.org	334,27	335,59	408,38	3,56
1.oceania.pool.ntp.org	316,47	317,85	394,55	4,09

Имя сервера	Мини-мальное значение запроса	Среднее значение запроса	Максимальное значение запроса	Стандартное отклонение времени запроса
1.south-america.pool.ntp.org	173,97	233,85	287,39	30,14
1.south-america.pool.ntp.org	229,23	230,91	308,07	3,61
0.asia.pool.ntp.org	223,39	227,27	327,60	9,91
1.north-america.pool.ntp.org	195,68	196,79	269,38	3,38
0.africa.pool.ntp.org	170,58	172,41	218,82	3,61
0.north-america.pool.ntp.org	163,31	168,01	308,72	18,98
amazon.com	111,03	115,28	210,63	11,47
1.africa.pool.ntp.org	78,58	79,28	89,53	1,02
0.europe.pool.ntp.org	41,19	46,70	107,28	14,02
1.europe.pool.ntp.org	36,33	37,11	49,35	1,10
facebook.com	35,33	36,29	45,77	1,04
yandex.ru	13,54	14,36	30,10	1,31
eltex-co.ru	12,61	13,66	34,38	1,64
1.asia.pool.ntp.org	12,68	13,58	26,36	1,07
192.168.1.141	1,60	2,71	9,84	0,73

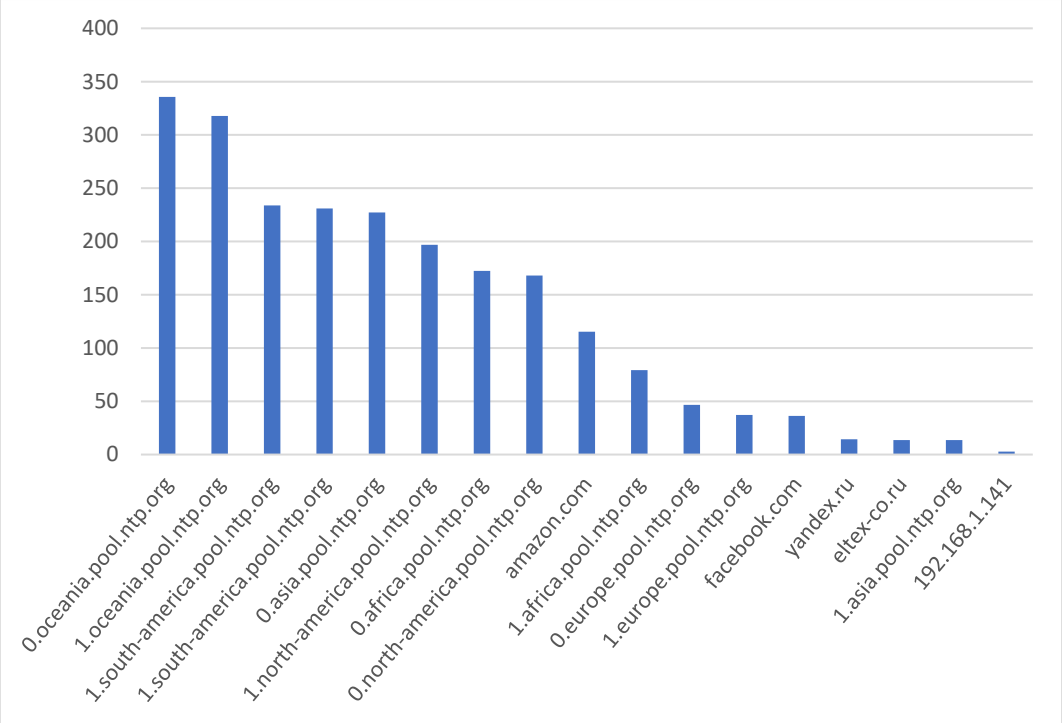


Рис. Среднее время выполнения команды ping

В качестве дополнительного тестирования была использована утилита iperf3 для оценки скорости передачи данных между сервером iperf3 в интер-

нете – iperf.volia.ne, и сервером MEC. По результатам тестирования, 100 тестирований, средняя скорость доступа к серверу MEC была равна 186 Мбит/с, а средняя скорость доступа к удаленному серверу равнялась 12 Мбит/с. Это дает преимущество в 15 раз при использовании серверов границы облачных вычислений.

Выводы

В заключении можно предположить сразу несколько сценариев использования NFV - SDN сети на базе MEC и Kubernetes:

– малое время отклика позволяет применять данную архитектуру для организации работы различных беспилотных автомобилей или различных роботов;

– можно снизить нагрузку на транспортную сеть изолировав трафик, к примеру, в торговом центре путем предоставления услуг: AAA (аутентификации, авторизации, учёта), карты торгового центра, вывод различных коммерческих предложений на основе местоположения пользователя; предоставление услуг приложений на основе нейросетей, к примеру, для организации виртуальных примерочных;

– повысить безопасность сетей путем унификации образов, который возможно тестировать и собирать автоматически;

– упростить управление сетью благодаря сочетанию технологий виртуализации сетевых функций и программно-конфигурируемых сетей.

Список используемых источников

1. Digital 2019: Global Internet Use Accelerates [Электронный ресурс]. URL: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates.

2. Strategy Analytics: Internet of Things Now Numbers 22 Billion Devices But Where Is The Revenue? [Электронный ресурс]. URL: https://news.strategyanalytics.com/press-release/iot-ecosystem/strategy-analytics-internet-things-now-numbers-22-billion-devices-where.

3. A Red Hat Report The State of Enterprise Open Source [Электронный ресурс]. URL: https://www.redhat.com/cms/managed-files/rh-enterprise-open-source-report-detail-f21756-202002-en.pdf.

4. Хакимов А. А, Суминов А. В., Мутханна А. С. А Разработка метода организации распределения граничных вычислений в сетях VANET // Информационные технологии и телекоммуникации. 2019. Том 7. № 2. С. 47–55. DOI 10.31854/2307-1303-2019-7-2-47-55.

УДК 004.056.5
ГРНТИ 81.93.29

ВЫБОР И ОБОСНОВАНИЕ ЭФФЕКТИВНЫХ МЕР КОМПЛЕКСНОЙ ЗАЩИТЫ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

В. А. Малофеев, И. Б. Паращук, Е. О. Шестаков

Военная академия связи

Рассматривается подход к процедуре выбора и обоснования эффективных мер комплексной защиты данных в информационных системах. Подход позволяет сформировать значения вероятностного коэффициента эффективности использования способа (или комплекса способов и средств) борьбы с угрозами безопасности данных, основан на совместном и сочетательном анализе ключевых видов угроз, средств и методов борьбы с ними и финансовых затрат на реализацию этой борьбы.

информационная система, комплексная защита данных, эффективность, угроза, ресурс.

Задачи обеспечения защиты данных, которые хранятся, передаются и обрабатываются в информационных системах (ИС), являются не просто актуальными, а приобретают новые, нередко приоритетные, тенденции [1].

Вместе с тем, современное состояние, темпы развития ИС и широкое внедрение информационных технологий в практику, позволяют решать данную задачу на качественно новом, высоком уровне, с учетом эффективных мер комплексной защиты данных (КЗД).

Позиционируя ИС как объект КЗД, необходимо предусмотреть:

– современный и постоянно обновляемый защищенный компьютерный парк, парк оборудования ИС и периферийных устройств (принтеры, сканеры и др.) в достаточном количестве как для технических специалистов (администраторов ИС), так и для пользователей, позволяющие обеспечить их необходимыми данными (контентом);

– широкомасштабное, но максимально защищенное подключение к сети Интернет, WiFi в местах коллективного доступа к ИС;

– технологии, обеспечивающие контроль действий пользователей ИС;

– технологии, предотвращающие несанкционированный доступ к ресурсам ИС, утрату, несанкционированное изменение и кражу данных.

Кроме того, нужно предусмотреть ориентированное на пользователя программное обеспечение, которое, в свою очередь:

– позволит обеспечить скорость обработки данных и качество предоставляемых услуг ИС;

– предоставит возможности получения данных с применением мобильных технологий;

– предоставит пользователям ИС точку доступа к интегрированным информационным мультиформатным ресурсам региона, страны и мира;

– обеспечит персонифицированное предоставление услуг пользователям ИС;

– предоставит возможность авторизации и аутентификации пользователей ИС;

– позволит развивать и продвигать сервисы дополненных услуг для мобильных и стационарных пользователей ИС.

Все эти сервисы безусловно являются объектами КЗД начиная со стадии создания ИС.

Все стадии жизненного цикла ИС особенно ярко проявляются в области защиты от несанкционированного доступа (НСД) к информации и контроля разграничения доступа к информационным ресурсам систем такого класса [1]. Считается, что защита данных должна рассматриваться пользователями и задачами, решаемыми в рамках ИС, не только с позиции конфиденциальности этих данных, но и с точки зрения комплексного обеспечения всех аспектов безопасности данных, включая их доступность и целостность [2].

Обусловлено это тем, что разнородность ресурсов, используемых ИС, предполагает наличие не только аппаратных, программных и информационных различий в области их построения и использования, но и различий в системах защиты информации (СЗИ): политиках безопасности, в применяемых механизмах защиты, в схемах разграничения доступа и т. д. Поэтому использование распределенными ИС таких ресурсов предопределяет уточнение и доработку политик безопасности и механизмов защиты, доработку процедур оценки защищенности данных и алгоритмов управления политикой безопасности.

Современными исследователями признается тот факт, что из-за особенностей архитектуры, распределенные ИС имеют недостаточную защиту. Актуальными угрозами для информационной безопасности являются: получение несанкционированного доступа к данным; нарушение подлинности и целостности информации и нарушение доступа к данным [2].

Поэтому в настоящее время КЗД является компромиссным решением и может обеспечить эффективную защиту данных от наиболее вероятных и опасных угроз. В зависимости от средств, используемых в КЗД, различают следующие виды защиты, претендующие на относительную самостоятельность:

– организационная защита, ориентированная на необходимость руководствоваться регламентирующими нормативно-правовыми документами;

– техническая защита, которая является комбинацией технических элементов и систем, как в виде самостоятельных средств, так и встроенных в процессе создания средств обработки данных;

– аппаратно-программная защита, предполагающая использование программного обеспечения (ПО), а также аппаратных устройств, являющихся частью технических средств.

К аппаратно-программной защите данных относят:

– межсетевые экраны (брандмауэры) – локальные или функционально-распределенные программные (программно-аппаратные) средства, контролирующие потоки данных, входящие и выходящие из информационной системы. Примерами межсетевых экранов являются PaloAltoNetworks, FortiGate и межсетевые экраны от компании Huawei;

– антивирусные программы – специализированное программное обеспечение, выполняющее поиск, лечение и уничтожение вируса. Наиболее популярными антивирусными программами в настоящее время являются: Kaspersky, ESETNOD32, Dr.Web;

– программно-аппаратные средства разграничения доступа, которые предоставляют доступ к объектам ИС исходя из полномочий субъектов, то есть контролируют очередность получения ресурсов информационной системы. Такими средствами разграничения доступа являются: Аккорд, DallasLock, SecretNet;

– сканеры безопасности, которые выполняют мониторинг ИС и сетей. Существует два способа поиска уязвимостей: сканирование и зондирование. Сканирование – метод мониторинга, при котором сканер по косвенным признакам определяет существование уязвимостей. Зондирование – механизм поиска уязвимости на заданном узле ИС. В настоящее время наиболее популярными сканерами безопасности являются: Nessus, MaxPatrol, Internet Scanner, Retina Network Security Scanner, Shadow Security Scanner (SSS).

– средства криптографической защиты. В основе этого направления защиты данных лежит их шифрование, также криптографические средства защиты обеспечивают аутентификацию и подтверждение авторства. Программно-аппаратными средствами криптографической защиты являются системы КриптоПро CSP, VipNet.

Многообразие и разносторонность средств и методов защиты данных наталкивает на выводы о том, что проблема оптимального сочетания различных направлений и видов защиты, проблема выбора и обоснования эффективных мер КЗД в ИС, должна рассматриваться как важнейшая проблема в области обеспечения не только безопасности систем такого класса, обеспечения безопасности отдельных ИС, но и в области безопасности информационных ресурсов страны в целом, затрагивая при этом оборонную, социальную, экономическую, политическую, экологическую и другие

составляющие, элементами управления которых являются информационные системы.

Обеспечение точного и оперативного выбора и обоснования мер КЗД в ИС должно опираться на результаты анализа эффективности комплексной защиты, когда решение принимается на основе полученных оценок, характеризующих сохранение конфиденциальности данных ИС, их целостности и доступности.

Одним из возможных подходов к выбору и обоснованию мер КЗД, является подход, предложенный в работе [3] и использующий значения P_{snm} – вероятностного коэффициента эффективности использования способа (или комплекса способов и средств) борьбы с угрозой безопасности данных, где: $S = \{1…s\}$ – способ борьбы, включающий, в нашем случае, средства и методы реализуемые различными, ранее рассмотренными устройствами защиты данных; $N = \{1…n\}$ – конкретное решение по защите данных; $M = \{1…m\}$ – конкретная угроза.

Результатом реализации такого подхода к выбору и обоснованию мер КЗД на основе оценивания эффекта комплексной защиты данных может выступать трехмерная матрица (рис.), содержащая различные значения P_{snm}, позволяющая сочетать и комбинировать средства защиты данных в различных вариантах и дающая заказчику возможность понять от каких угроз и с какой результативностью то или иное средство (или их сочетание) обеспечит эффективную защиту данных.

	Вредоносное ПО	Фишинг	DDoS-атаки	Спам	
Конфиденциальность	0,436	0,312	-	0,127	
Целостность		-	-		
Доступность		-		0,196	
СРД «Аккорд»	-	0,997	-	0,999	30175 ₽
СРД «Dallas Lock»	-	0,998	-	0,999	34500 ₽
СРД «SecretNet»	-	0,998	-	0,999	39591 ₽
Антивирусное ПО Dr Web	0,9978	0,9998	-	0,9998	4700 ₽
Антивирусное ПО Kaspersky	0,9983	0,9999	-	0,9999	3900 ₽
Межсетевой экран Pallo Alto Networks	0,985	0,995	0,799	0,995	79670 ₽
Межсетевой экран Huawei USG9500	0,989	0,999	0,81	0,999	76300 ₽
Межсетевой экран FortiGate 3980E	0,988	0,998	0,805	0,998	77800 ₽
Anti-DDoS Cloudways	-	-	0,997	-	25000 ₽
Anti-DDoS Akamai	-	-	0,999	-	33600 ₽
Anti-DDoS Imperva Incapsula	-	-	0,998	-	30100 ₽

Рис. Трехмерная матрица вероятностных коэффициентов эффективности противодействия угрозам безопасности данных в ИС

Матрица (рис.) учитывает аспекты, отвечающие за конфиденциальность, целостность и доступность данных в ИС, содержит грань, элементы которой характеризуют, (в качестве примера) ключевые виды угроз [4]: вредоносное ПО, фишинг, DDoS-атаки и спам, а также средства аппаратно-программной защиты, т. е., способы борьбы, включающие, в нашем случае, средства и методы, реализуемые различными, ранее рассмотренными устройствами аппаратно-программной защиты данных (могут содержать, в рамках КЗД, и их возможные комбинации).

Безусловным достоинством данного подхода является возможность учета финансовых затрат на КЗД, о чем говорит третья грань матрицы вероятностных коэффициентов эффективности противодействия угрозам безопасности данных в ИС. Эта грань (рис.) содержит значения цены на средства защиты, формируя мнение о стоимости реализации КЗД.

Иными словами, полученные в ходе исследования данные могут дать реальную возможность осуществить оценивание эффективности комплексной защиты данных, учитывая риски угроз и результативность противоборства, но не забывая при этом о стоимости реализации КЗД в ИС.

Таким образом, предложен подход к процедуре выбора и обоснования эффективных мер комплексной защиты данных в информационных системах. Подход позволяет сформировать значения вероятностного коэффициента эффективности использования способа (или комплекса способов и средств) борьбы с угрозами безопасности данных и основан на совместном и сочетательном анализе ключевых видов угроз, средств и методов борьбы с ними и финансовых затрат на реализацию этой борьбы.

Предложенный подход, по мнению авторов, позволит повысить точность и оперативность анализа эффективности КЗД, что, в свою очередь, позволит повысить качество принимаемых решений по управлению защитой информационных ресурсов.

Список используемых источников

1. Васильков А. В., Васильков А. А., Васильков И. А. Информационные системы и их безопасность: учеб. пособие. М. : Форум, 2011. 528 с.

2. Miller D., Harris S., Harper A., VanDyke S. Security Information and Event Management (SIEM) Implementation. London, McGraw-Hill. 2010. 464 p.

3. Паращук И. Б., Чернявский А. В., Шестаков Е. О. Эффективность комплексной защиты информации в системах хранения данных и электронных библиотеках: модели и методы оценивания. // Информационная безопасность регионов России (ИБРР-2019) XI-я Санкт-Петербургская Межрегиональная конференция. Санкт-Петербург, 23–25 октября 2019 г., Материалы конференции, СПб., СПОИСУ, 2019. 596 с. С. 248–250.

4. Авраменко В. С., Бобрешов-Шишов Д. И., Беденков В. Н., Маликов А. В. Определение актуальных угроз безопасности информации в инфокоммуникационных системах на основе аппарата нечеткой логики // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). VI Международная научно-техническая

и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 3. 535 с. С. 13–18.

УДК 004.056.5
ГРНТИ 50.37.23

АНАЛИЗ ОСОБЕННОСТЕЙ ИСПОЛНЕНИЯ ПРИЛОЖЕНИЙ В ДОВЕРЕННОЙ СРЕДЕ ИСПОЛНЕНИЯ НА ОСНОВЕ ТЕХНОЛОГИИ ARM TRUSTZONE

Д. О. Маркин, В. М. Миначев

Академия ФСО России

В статье приводится анализ и классификация технологий построения доверенных сред исполнения в электронных вычислительных машинах на основе процессоров с архитектурой ARM. Описаны различия уровней привилегий для исполняемого кода в данных процессорах и технические средства, осуществляющие их поддержку. Представлена и описана схема взаимодействия пользовательских приложений, функционирующих в недоверенной операционной системе, и трастлетов – доверенных приложений, функционирующих под управлением так называемых доверенных операционных систем на основе технологии ARM TrustZone.

TrustZone, доверенная среда исполнения, ARM, TEE, SMC, трастлет.

В настоящее время сохраняется тенденция по росту количества мобильных устройств и микрокомпьютеров, начиная мобильными абонентскими устройствами (телефоны, смартфоны, планшетные компьютеры, интеллектуальные часы и т. п.) и заканчивая датчиками, встроенными микрокомпьютерами в офисной технике, автомобилях, промышленных датчиков и сенсоров, «Интернета-вещей». Информация, обрабатываемая и создаваемая устройствами, растет, вместе с ней растет и объем критически важных данных, требующих защиты, поэтому для новых устройств, так или иначе оптимизирующих работу систем, требуются специфичные механизмы защиты, один из таких это – логическая изоляция выполнения кода программы или создание так называемой доверенной среды исполнения (ДСИ).

Основная доля таких устройств реализована на основе электронных вычислительных машин (ЭВМ) на базе процессоров с архитектурой ARM, разработчиком которых является одноименная британская компания ARM. Известно, что в данных ЭВМ реализована технология TrustZone, реализующая

разграничение доступа между исполняемым кодом пользовательской операционной системы (*Android*, *iOS, Sailfish* и др.) и приложений и так называемых доверенных приложений – трастлетов и доверенной операционной системы.

Лидирующими компаниями по разработке и внедрению в свои процессоры ДСИ являются Intel, AMD и ARM. В работе [1] проведен сравнительный анализ и классификация наиболее распространенных аппаратных технологий для построения ДСИ. В [2] также рассмотрен ряд атак и способов защиты некоторых из этих технологий. Согласно [3] все технологии реализации ДСИ можно разделить на уровни их функционирования:

– кольцо 3 – пользовательский уровень (*Intel* SGX [4], *Sanctum* [5])

– кольцо 0 – уровень ядра (AEGIS [6])

– кольцо – 1 – уровень гипервизора (*Bastion* [7])

– кольцо – 2 – уровень специальных функций обеспечения и безопасности системы (SMM [8], *TrustZone* [9])

– кольцо – 3 – уровень сопроцессора и аппаратных компонентов вне процессора (TPM [10], *Intel* ME [11])

Защищенность и корректность функционирования кода, реализующего технологию ARM TrustZone, долгое время было затруднительно анализировать из-за его закрытости и недостатка информации [12]. Однако за последние несколько лет внимание к TrustZone заметно увеличилось. Появились проекты по применению ее в различных сферах деятельности: мобильной [13], промышленной [14], автомобильной [15] и аэрокосмической [16]. Внимание к технологии поддерживается публикациями крупных компаний производителей технических деталей и рекомендаций для разработки [17].

Особенности реализации технологии TrustZone позволяют проводить исследования в области повышения безопасности обработки данных, в отличии от проприетарных решений, рассмотренных выше.

Ряд как практических исследований безопасности кода, реализующего технологию *TrustZone*, так и конкретные сертифицированные решения появились и в России. В частности в августе 2019 года был сертифицирован по требованиям ФСТЭК (профиль защиты «ИТ.СД3.УБ2.ПЗ») модуль «Aladdin TSM» [18, 19], основанный на использовании технологии TrustZone.

Производительность современных компьютерных систем, как правило, зависят от размера доверенных вычислительных баз (*Trusted Computing Bases*, TCBs). TrustZone ограничивает TCB, так как вводит в систему два логических домена для выполнения программ это – secure world и normal world. Secure world представлена в виде специальной операционной системы (ОС) также называемой доверенной, в которой происходить обработка конфиденциальных данных с высоким уровнем привилегий с помощью приложений-трастлетов. Normal world – пользовательская или richOS, например Linux,

Android или другая ориентированная на пользователя система. Взаимодействие этих «миров» происходит за счет вызова привилегированной инструкции вызова монитора безопасности (*Secure Monitor Call*, SMC) в режиме *Secure*, в котором может быть изменен новый 3-й *NS*-бит регистра (*Secure Configuration Register*, SCR).

Для более безопасного обмена данными между «мирами» используется специальный буфер памяти, управляемый модулем управления памятью – Shared World Memory (SWM).

ДСИ могут строиться в двух вариантах – ДСИ-ядро и ДСИ-сервис. Первый является набором базовых функций для управления ресурсами системы и разрабатывается поставщиком оборудования, вторая – реализация конкретной функции безопасности и может функционировать только при наличии ДСИ-ядра. При этом одновременно в системе может быть несколько сервисов. Наиболее важные классы таких сервисов:

– доверенное хранилище – файлы для хранения загружаются в доверенную ОС для шифрования и хранения в гостевой ОС;

– аутентификация и криптографические функции – хранение криптографических ключей, One-Time-Password на основе времени и недоступного гостевой ОС счетчика, двухфакторная аутентификация и контроль доступа реализуются в доверенной ОС;

– проверка и контроль richOS – мониторинг ресурсов, проверка целостности ядра, драйверов и обнаружение загрузочного вредоносного кода (руткитов) в гостевой ОС;

– доверенный пользовательский интерфейс – применение драйверов устройств из гостевой ОС с загрузкой их в режиме *secure* для изоляции процесса.

Схема взаимодействия пользовательского приложения и трастлета представлена на рис. (см. ниже).

Данная схема допускает работу и со встроенным производителем, и с собственным трастлетом. Основными этапами функционирования приложения являются следующие:

1. Пользовательское приложение по уникальному идентификатору трастлета обращается к менеджеру трастлетов.

2. Менеджер трастлетов передает ID трастлета драйверу взаимодействия, который, используя SMC, загружает трастлет в оперативную память secure world.

3. Доверенная ОС обрабатывает вызов SMC и обращается к менеджеру выполнения для проверки целостности трастлета с его последующим запуском.

4. Загруженный менеджером трастлет находится в отдельной секции памяти в зависимости от предоставляемых ему прав или его копии.

5. Драйвер взаимодействия создает экземпляр контейнера WSM для записи в него входных данных из пользовательского приложения.

6. Пользовательское приложение уведомляет secure world о готовности запроса.

7. Трастлет обрабатывает запрос, результат которого помещается в созданный менеджером выполнения экземпляр контейнера WSM.

8. Цикл запросов и ответов с 5 по 7 пункты могут повторяться несколько раз.

9. Пользовательское приложение завершает сессию работы с трастлетом.

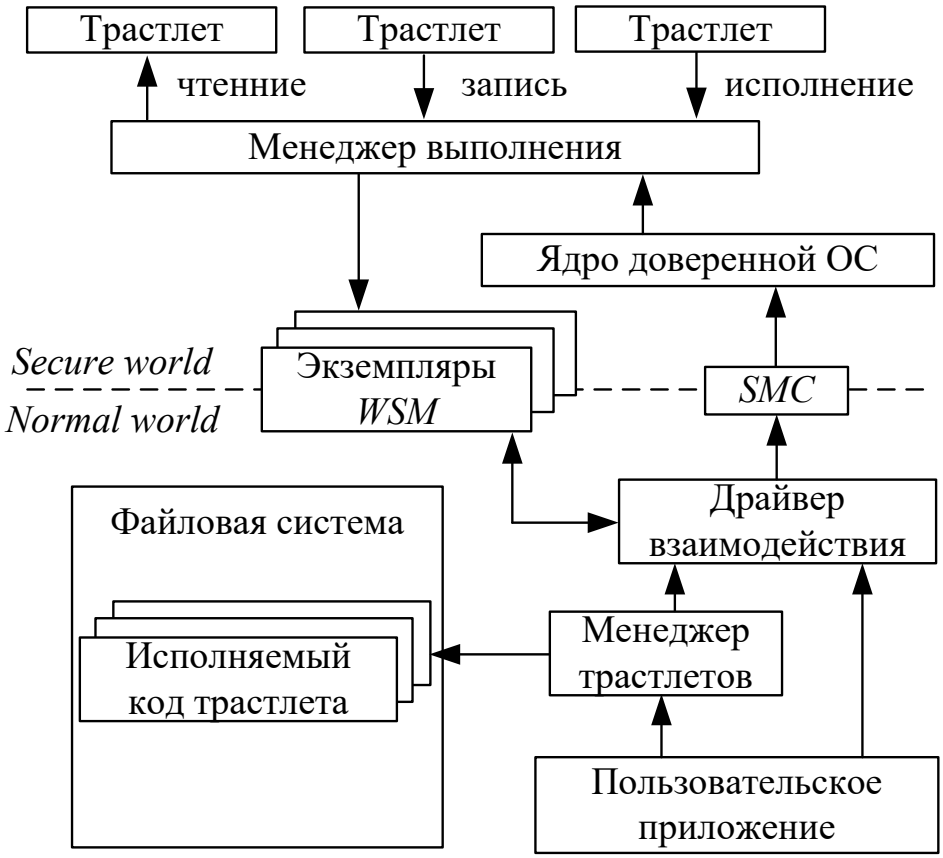


Рис. Вариант схемы взаимодействия пользовательского приложения и трастлета

Анализ особенностей функционирования ДСИ в современным ARM процессорах позволяет сделать вывод, что адаптация технологии TrustZone для нужд отечественной экономики за счет применения подходов по повышению доверия к ней, включая сертификацию и разработку отечественного ПО на основе TrustZone, является важным направлением совершенствования отечественных технологий обеспечения безопасности информации в условиях отсутствия производства достаточного количества элементной базы. Особенно, учитывая количество современных устройств, в основе которых лежат процессоры с архитектурой ARM.

Список используемых источников

1. Pinto S., Santos N. Demystifying Arm TrustZone: A Comprehensive Survey // ACM Computing Surveys, 2019. January 10. p. 36.

2. Fengwei Zhang SoK: A Study of Using Hardware-assisted Isolated Execution Environments for Security // HASP, 2016. June 18. p. 8.

3. Ning Z., Zhang F., Shi W. Position paper: Challenges towards securing hardware-assisted execution environments. In Hardware and Architectural Support for Security and Privacy // ACM, 2017. Article 6.

4. Costan V., Devadas S. Intel SGX explained. IACR Cryptology // ePrint Archive, 2016. p. 86.

5. Costan V., Lebedev I., Devadas S. Sanctum: Minimal hardware extensions for strong software isolation // Proceedings of the USENIX Security Symposium. USENIX Association, 2016. P. 857–874.

6. Suh G., Clarke D., Gassend B., M. van Dijk, Devadas S. AEGIS: Architecture for tamper-evident and tamper-resistant processing // Proceedings of the Annual International Conference on Supercomputing. ACM, 2003. PP. 160–171.

7. Champagne D., Lee R. B. Scalable architectural support for trusted software // Proceedings of the International Symposium on High-Performance Computer Architecture. 2010. PP. 1–12.

8. Intel. 64 and IA-32 Architectures Software Developer's Manual. URL: http://www.intel.com/content/en/processors/architectures-software-developer-manuals.html (дата обращения: 10.12.2019).

9. Alves T., Felton D. TrustZone: Integrated hardware and software security // Tech. In-Depth 3, 4, 2004. PP. 18–24.

10. Trusted Computing Group. TPM Main: Part 1 Design Principles, Version 1.2, 2011. p. 116.

11. Ruan X. Platform Embedded Security Technology Revealed: Safeguarding the Future of Computing with Intel Embedded Security and Management Engine, 2014. p. 10.

12. Winter J. Experimenting with ARM TrustZone–Or: How I met a friendly piece of trusted hardware // Proceedings of the IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2012. PP. 1161–1166.

13. Kostiainen K., Ekberg J., Asokan N., Rantala A. On-board credentials with open provisioning // Proceedings of the Symposium on Information, Computer, and Communications Security. ACM, 2009. PP. 104–115.

14. Fitzek A., Achleitner F., Winter J., Hein D. The ANDIX research OS – ARM TrustZone meets industrial control systems security // Proceedings of the IEEE International Conference on Industrial Informatics, 2015. PP. 88–93.

15. Kim S. W., Lee C., Jeon M., Kwon H. Y., Lee H. W., Yoo C.. Secure device access for automotive software // Proceedings of the International Conference on Connected Vehicles and Expo, 2013. PP. 177–181.

16. Pinto S., Tavares A., Montenegro S. Space and time partitioning with hardware support for space applications // Data Systems in Aerospace, European Space Agency, ESA SP 736, 2016. PP. 250.

17. Xilinx. Programming ARM TrustZone Architecture on the Xilinx Zynq-7000 All Programmable SoC. User Guide, UG1019 (v1.0). URL: https://www.xilinx.com/support/documentation/user_guides/ug1019-zynq-trustzone.pdf (дата обращения: 10.12.2019).

18. Доверенная платформа для процессоров ARM // ЗАО "Аладдин Р. Д." URL: https://www.aladdin-rd.ru/catalog/tsm (дата обращения: 10.12.2019).

19. Сертификат соответствия ФСТЭК России № 4155 // ЗАО "Аладдин Р. Д.". URL: https://www.aladdin-rd.ru/public/files/tsm/sertifikat_fstek_4155_tsm.pdf (дата обращения: 10.12.2019).

УДК 004.056.53
ГРНТИ 50.37.23

МЕТОДЫ И СРЕДСТВА ОБФУСКАЦИИ И ДЕОБФУСКАЦИИ ИСХОДНЫХ ТЕКСТОВ ВЕБ-ПРИЛОЖЕНИЙ НА ЯЗЫКЕ JAVASCRIPT

Д. О. Маркин, Д. А. Рыков

Академия ФСО России

В работе приводится исследование актуальных методов и средств обфусцирующих преобразований программного кода на языке JavaScript. Описаны основные метрики, применяемые для определения стойкости обфускации исходных текстов приложений. Исследованы основные методы деобфускации JavaScript-кода и средства их реализации. Предложена концептуальная структура универсального деобфускатора веб-приложений на JavaScript, учитывающая достоинства и недостатки известных технологий деобфускации, а также методов анализа программного обеспечения.

JavaScript, обфускация, деобфускация, эмуляторы кода, веб-приложения.

Основу современной глобальной информационно-телекоммуникационной системы в настоящее время составляют информационные сервисы на базе веб-технологий. Разработка веб-приложений для таких сервисов должна отвечать требованиям безопасности с учетом того, что часть программного кода может исполняться на стороне клиентов. В связи с тем, что объем кода современных веб-приложений очень велик, для анализа его безопасности, как правило, применяют автоматизированные методы анализа защищенности, поиска уязвимостей и недекларированных возможностей. К таким методам, в частности, относится фаззинг. Эффективность фаззинга зависит от разных факторов, одним из которых является количество информации, которым обладает фаззер об объекте анализа (модели «черного», «серого» или «белого» ящика).

В большинстве современных веб-приложениях основу клиентского программного кода составляет объектно-ориентированный язык программирования JavaScript, а наиболее распространенный используемый метод защиты – обфускация [1, 2]. Фаззинг обфусцированных веб-приложений, как и исполняемого на стороне обфусцированного *JavaScript* кода, является

нетривиальной задачей в связи с проблемой идентификации в коде точек входа, и требует применения деобфускации или использования дополнительных методов анализа.

От анализа веб-приложений написанных на языке JavaScript, кроме обфускации, применяются следующие способы защиты: шифрование данных, приемы защита от отладки, приемы обнаружения эмуляторов, кодовые замки, связывание данных, обнаружение прав администратора, проверка целостности файлов и данных, защита среды выполнения, подпись кода, криптография на основе белого ящика [5]. Для защиты *JavaScript* кода от статического анализа, используемого для обнаружения точек входа, используется, как правило, обфускация.

Обфускацией программы называется всякое ее преобразование, которое сохраняет вычисляемую программой функцию, но при этом придает программе такую форму, что извлечение из текста программы ключевой информации об алгоритмах и структурах данных, реализованных в этой программе, становится трудоемкой задачей [1, 3].

Наиболее распространенными способами обфускации являются [4]:

1. Удаление пробельных символов.
2. Удаление комментариев.
3. Замена имен идентификаторов.
4. Преобразование выражений условного оператора if-else.
5. Логическое преобразование.
6. Сокращение констант.
7. Кодирование чисел.
8. Кодирование строк.

На сегодняшний день существует множество обфускаторов, применяющих различные способы преобразований. К самым известным относятся: JSPacker, JSmin, YUI Compressor, Google Closure Compiler, JJencode, JSUnpack, WebStorage, uglifyjs2, JSFuck, AAencode, URLencode, Packer, JS Obfuscator.

Качество проведенных с кодом преобразований – обфускации, классифицируют по следующим критериям [4]:

– эффективность, оцениваемая метриками сложности программного обеспечения (ПО);

– устойчивость кода к деобфускации;

– сложность, добавленная в обфусцированный код;

– скрытность.

К метрикам сложности ПО в работе [5] относят:

– длину программ;

– цикломатическую сложность;

– сложность ветвления;

– сложность потока данных;

– метрику Кафура (*fan in*/*out complexity*).

– сложность структуры данных.

– объектно-ориентированную метрику.

Устойчивость к деобфускации определяется стойкостью кода к применению автоматических, автоматизированных методов деобфускации, а также может определяться длительностью работы квалифицированного эксперта, использующего доступные средства анализа, для восстановления алгоритма исследуемого им обфусцированного JavaScript кода.

Скрытность обфускации определяется способностью обфускатора исключать из обфусцированного кода демаскирующие признаки: комментарии, имена информационных и функциональных объектов, идентифицирующие обфускатор признаки и другие.

Основные задачи, которые решают современных обфускаторы JavaScript программного обеспечения – это: замена символов, контроль потока управления, обфускация данных, контроль целостности кода, защита среды выполнения, обеспечение требуемого многообразия и гибкости.

Основные методы деобфускации JavaScript кода представлены на рис. 1.

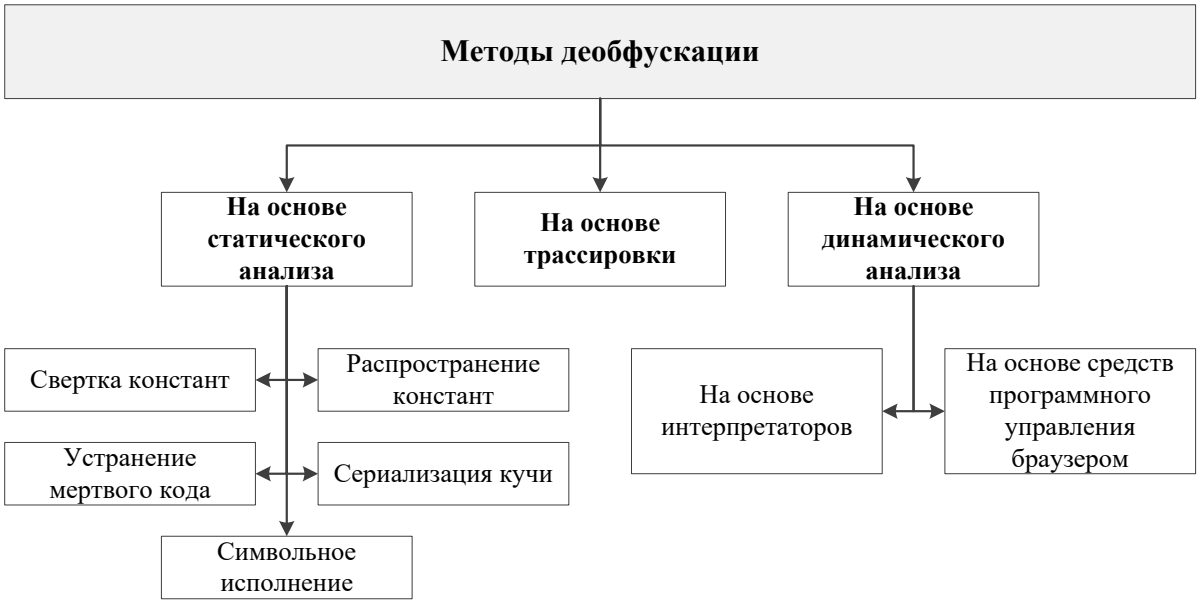


Рис. 1. Методы деобфускации

Инструменты для деобфускации JavaScript кода можно разделить следующим образом:

1. Средства анализа вредоносных программ (*JStillery*, *JSDetox* и др.).

2. Деобфускаторы (*JStillery*, *JSDetoxI*, *JSNice* и др.).

3. Оптимизаторы (*Prepak.io*, *Closure compiler*, *jsbeautifier* и др.).

4. Средства эмуляции JavaScript (*Google V8*, *SpiderMonkey*, *Nodejs's VM module* и др.).

В случаях, когда используемый для защиты кода обфускатор известен либо обфусцированный код имеет ярко выраженные идентифицирующие обфускатор признаки (например, алфавит или особенности компоновки текста), по которому можно выбрать доступный деобфускатор, то задача восстановления кода решается тривиально. Однако для общего случая полное восстановление исходного текста обфусцированного приложения, как известно [6], невозможно. Тем не менее, существующие методы анализа программного обеспечения позволяют повысить качество деобфускации, например, за счет динамического анализа кода [7].

На рис. 2 представлена модульная схема средства, решающего задачу идентификации точек входа удаленного веб-приложения путем комплексного анализа обфусцированного клиентского *JavaScript* кода.

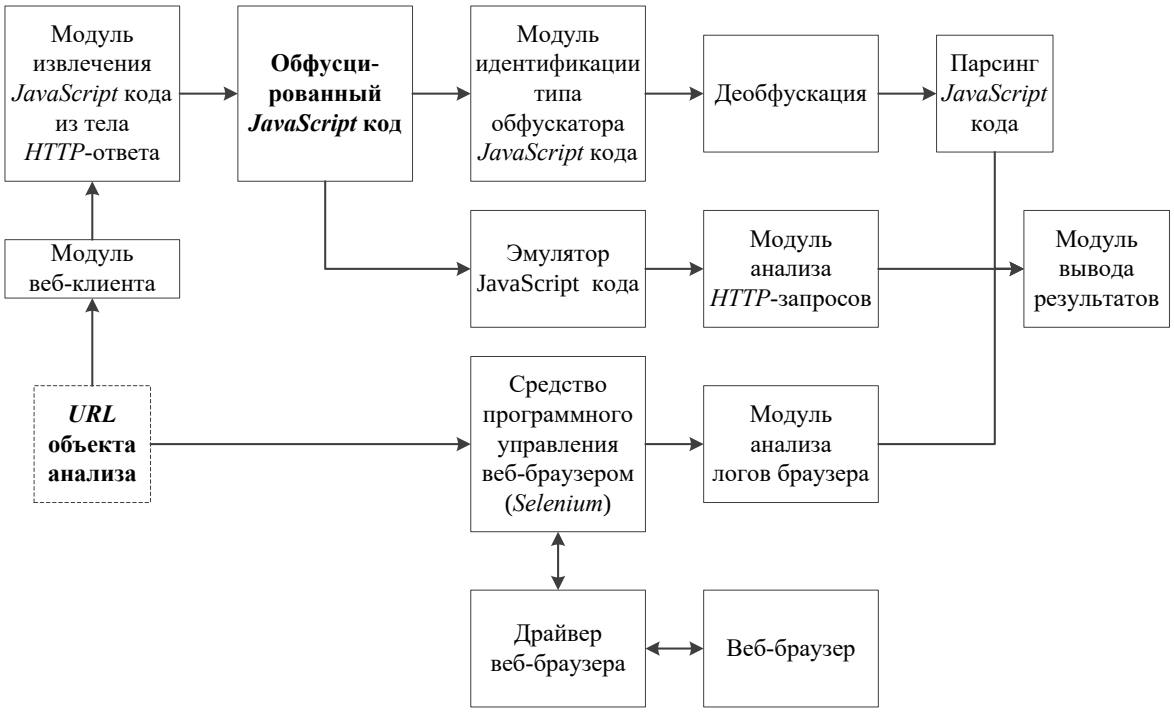


Рис. 2. Схема средства идентификации точек входа удаленного веб-приложения

Динамическими средствами анализа в предложенном средстве являются – эмуляторы *JavaScript* кода, сопряженные с модулем анализа, а также средство программного управления веб-браузером с модулем анализа логов браузера.

Предлагаемая схема средства идентификации точек входа позволяет использовать средства динамического анализа – эмуляторы JavaScript кода и программно-управляемые браузеры. За счет этого результаты идентификации точек входа веб-приложений фактически не зависят от стойкости обфускации и количества правил, используемых парсерами. Однако недостатком такого подхода является повышение требований к составу и производительности программно-аппаратного комплекса, а также не позволяет

обеспечить гарантированный результат, поскольку требует перебора всех возможных исходных данных, что теоретически в общем случае невозможно. Тем не менее, предлагаемый подход по исследованию обфусцированных приложений лишен недостатков, присущих статическим методам анализа, которые практически неэффективны в отношении современных сайтов, содержащий многослойный, сложных, обфусцированные JavaScript приложении.

Список используемых источников

1. Кузнецова А. О., Верхотурова Г. Н. Об особенностях применения методов обфускации программного кода языка JavaScript // Информационные технологии интеллектуальной поддержки принятия решений. 2019. С. 117–122.

2. Полухин П. В. Байесовские модели и алгоритмы управления процессом тестирования веб-приложений методом фаззинга // Наука и современность. 2012. № 16–1. С. 313–318.

3. Byung-Ik Kim, Chae-Tae Im, Hyun-Chul Jung. Suspicious Malicious Web Site Detection with Strength Analysis of a JavaScript Obfuscation. International Journal of Advanced Science and Technology. 2011.

4. Colberg C., Thomborson C., Low D. A taxonomy of obfuscating transformations. Technical Report #148. Department of Computer Science. The University of Auckland, New Zeland. 1997.

5. Pedro F. A methodology for Assessing JavaScript Software Protections. OWASP AppSec Europe. 2018.

6. Варнавский Н.П., Захаров В.А., Кузюрин Н.Н., Шокуров А.В. Современное состояние исследований в области обфускации программ: определение стойкости обфускации // Труды ИСП РАН. Т. 26. Вып. 3. 2014. С. 167–198. DOI: 10.15514/ISPRAS-2014-26(3)-9.

7. Маркин Д. О., Зверев А. А., Саклаков А. И., Рыков Д. А. Технологии распознавания моделей точек входа веб-приложений // Безопасные информационные технологии : Десятая международная научно-техническая конференция : сб. трудов, Москва, 3–4 декабря, 2019 г. Москва : МГТУ им. Н. Э. Баумана, 2019. 409 с. С. 275–280.

УДК 004.056.5
ГРНТИ 50.37.23

СРАВНИТЕЛЬНЫЙ АНАЛИЗ «ДОВЕРЕННЫХ» ОПЕРАЦИОННЫХ СИСТЕМ, РАЗРАБОТАННЫХ НА ОСНОВЕ ТЕХНОЛОГИИ TRUSTZONE

Д. О. Маркин, Хо Тхай Чунг

Академия ФСО России

В статье приводится анализ и классификация технологий построения доверенных сред исполнения в электронных вычислительных машинах на основе процессоров с архитектурой ARM. Проведен сравнительный анализ современных "доверенных" операционных систем для ЭВМ на базе процессоров с архитектурой ARM. Выделены их особенности, степень доступности исходных текстов, сферы применения, разработчики. Сформулированы выводы в отношении развития технологий проектирования доверенных сред исполнения

TrustZone, доверенная среда исполнения, ARM, TEE, SMC, трастлет.

Введение

Объективная потребность в повышении защищенности исполнения приложений, функционирующих в составе систем безопасности и обрабатывающих защищаемую информацию, привела к появлению программно-аппаратных технических решений, создающих так называемые доверенные среды исполнения (ДСИ) на основе аппаратных средств доверенных загрузки (СДЗ) или аппаратно-программных модулей доверенной загрузки (АПМДЗ). Наиболее далеко в разработке таких средств защиты продвинулись разработчики компаний *Intel*, *ARM*.

Термин «доверенный» в отношении программного, аппаратного и программно-аппаратного обеспечения обозначает, что использование указанного средства удовлетворяет действующим требованиями субъекта, его эксплуатирующего.

В сложившихся геополитических обстоятельствах доверие к программно-аппаратным техническим решениям иностранного производства исключено. Однако в связи с отсутствием аналогичных отечественных технологий и элементной базы применяются специальные процедуры проверки соответствия (сертификация, аттестация) [1, 2], позволяющие повысить степень доверия к подобным техническим решениям.

Попытка применения концепции изолированного выполнения приложений на аппаратном уровне привела к появлению технологии доверенных

сред исполнения ДСИ (TEE – *Trusted Execution Environment*). Соответственно, аппаратные компоненты системы, обеспечивающие создание такой среды называются средствами доверенной загрузки (TSM – *Trusted Security Module*). При этом необходимо различать ДСИ, построенные на основе технологий программной виртуализации, т. е. только лишь за счет программного обеспечения, и ДСИ, построенные с использованием аппаратного обеспечения.

В настоящее время известны следующие технологи построения ДСИ, основанные на использовании встроенных модулей в аппаратные элементы ЭВМ (элементы центрального процессора и/или аппаратной архитектуры):

1. Intel: Trusted Execution Technology;
– Intel Management Engine (Intel ME) [3,4];
– «Silent Lake» (процессоры Atom);
– System Management Mode (SMM) [5] и Dynamic Root for Measurements (DRTM) [6,7];
– Intel Software Guard Extensions (SGX) [8].
2. AMD:
– Platform Security Processor (PSP) [9];
– AMD Secure Execution Environment.
3. ARM:
– TrustZone [10].
4. RISC-V:
– MultiZone™ Security Trusted Execution Environment.

Сравнительный анализ «доверенных» операционных систем, разработанных на основе технологии TrustZone

Технология TrustZone [10] – это основанное на возможностях аппаратного обеспечения среда доверенной загрузки, позволяющая создавать ДСИ. Данная технология формирует две среды исполнения приложений или так называемых в терминах компании ARM «мира». ДСИ на основе TrustZone называется в терминологии ARM – Secure World или Secure OS, «недоверенный» – Rich Execution Environment или Rich OS (*iOS*, *Android*, *Sailfish*, *Tizen*, *Linux*, *Windows* и др.). Порядок загрузки ЭВМ с процессором ARM представлен на рис. 1, а взаимодействие режимов ДСИ (*Secure OS*) и гостевой операционной системы (ОС) (*Rich OS*) на рис. 2.

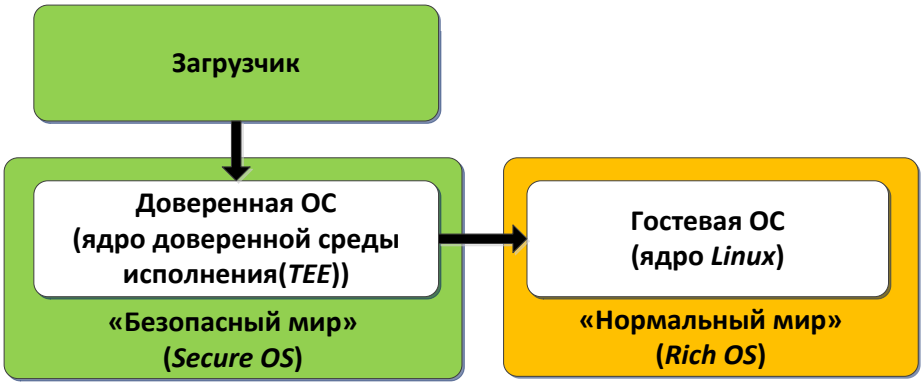


Рис. 1. Порядок загрузки в платформах на основе ARM-процессоров

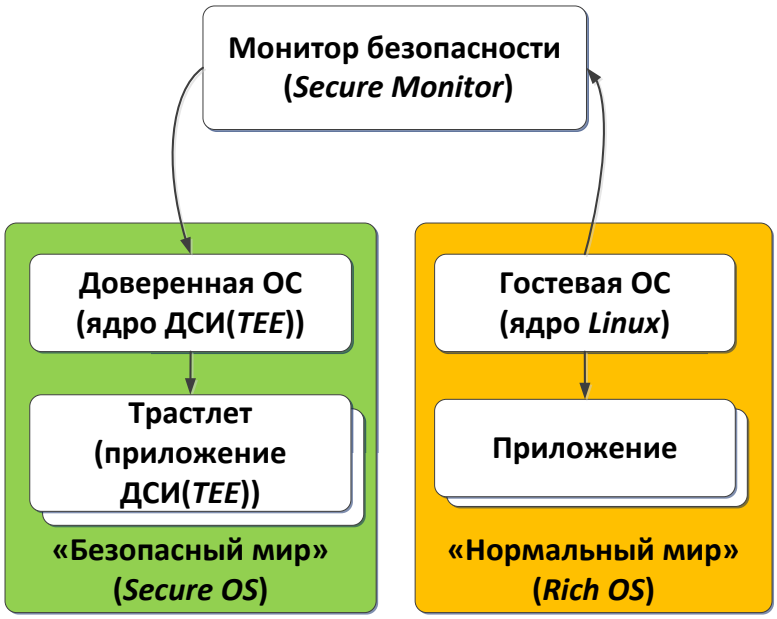


Рис. 2. Взаимодействие доверенной и гостевой операционных систем в платформах на основе ARM-процессоров

В настоящее время существует около десяти [11] так называемых «доверенных» ОС, использующих функционал TrustZone. Ряд реализаций технологии TrustZone закрыты от исследователей (*Trustonic* TSP, *Qualcomm* QSEE).

Сравнительный анализ известных реализаций «доверенных» ОС приведен в табл.

ТАБЛИЦА. Сравнительный анализ «доверенных» ОС

Наименование	Разработчик	Особенности
GlobalPlatform	Некоммерческое объединение компаний G&D Mobile Security, ARM, FIME, Trustonic, Gemalto, Oracle	Промышленный стандарт TEE

Наименование	Разработчик	Особенности
General Dynamics OKL4	Open Kernel Labs	Основана на ОС L4 (L3) – микроядре для систем i386, разработано для IoT-устройств с 2012 г. исходные тексты закрыты
Google Trusty TEE	Google (только для ОС Android)	Совместима с процессорами ARM и Intel Состоит из трех основных элементов: 1) ядро ОС (основано на Little Kernel); 2) драйвер ядра для управления взаимодействием TEE (Trusty) и REE (Android); 3) библиотека пользовательского пространства для управления взаимодействием REE (Android) и TEE (Trusty)
Linaro OP-TEE	Исследовательская группа Linaro, STMicroelectronics	Основана на GlobalPlatform 1.1 Проект с открытым исходным текстом: Состоит из трех основных элементов: 1) ядро ОС (модули управления памятью, прерываниями и др.); 2) клиент недоверенного пользовательского пространства – монитор-посредник между пространствами пользователя и ядра, библиотеки реализации GlobalPlatform TEE Client API; 3) драйвер ядра для выполнения транзакций между доверенной и недоверенной ОС
Jailhouse	Siemens	В общем смысле является не ОС, а монитором обращений к ресурсам. Может быть запущен в составе ОС FreeRTOS, Erika3, Linux, Zephyr Поддерживает процессоры с архитектурами: ARMv8, ARMv7, x86_64. Требует наличия 2-х процессоров и 50 Мб оперативной памяти
QSEE [12]	Qualcomm Secure Execution Environment	Основана на General Dynamics OKL4 Закрытый исходный текст
seL4	Open Kernels labs	Основана на ОС L4 Прошла формальную верификацию корректности методом определения спецификации функциональности и доказательства его корректности средствами строгого логического вывода. Открытый исходный текст ОС реального времени для прошивок процессоров беспроводных модемов Qualcomm Объем кода – около 9 600 строк Прерывания при исполнении кода отключены Поддерживает процессоры ARM до ARMv8
TrustTonic Kinibi	TrustTonic	Закрытый исходный текст. Для ОС Android Для устройств (смартфонов и планшетных компьютеров) Samsung. Обеспечивает шифрование данных и аутентификацию устройств. Трастлеты имеют доступ к сети.

Наименование	Разработчик	Особенности
		Имеется набор разработчика (SDK), совместимый со стандартами GlobalPlatform API
Xen	Университет Кэмбриджа	Является гипервизором микроядра Поддерживает процессоры ARM и Intel
Xvisor	Сообщество разработчиков Xvisor	Гипервизор 1-го типа Открытый исходный текст Имеет модуль управления памятью, планировщик, балансировщик нагрузки и потоков
Aladdin TSM [13]	ЗАО «Аладдин Р.Д.»	Поддерживает процессоры i.MX6 Сертифицирован по требованиям ФСТЭК к средствам доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты "ИТ.СДЗ.УБ2.ПЗ" (сертификат № 4155) [14]

Выводы

Анализ особенностей функционирования ДСИ в современным ARM процессорах позволяет сделать вывод, что адаптация технологии TrustZone для нужд отечественной экономики за счет применения подходов по повышению доверия к ней, включая сертификацию и разработку отечественного ПО на основе TrustZone, является важным направлением совершенствования отечественных технологий обеспечения безопасности информации в условиях отсутствия производства достаточного количества элементной базы. Особенно, учитывая количество современных устройств, в основе которых лежат процессоры с архитектурой ARM.

Список используемых источников

1. Закалкин П. В., Мельников П. В. Система анализа программного обеспечения на предмет отсутствия недекларированных возможностей // Программная инженерия. 2018. Т. 9. № 2. С. 69–75.

2. Закалкин П. В., Мельников П. В., Горюнов М. Н., Борзов Р. В. Подход к разработке анализатора исходных текстов программ на основе использования LLVM // Программная инженерия. 2019. Т. 10. № 1. С. 14–19.

3. Ruan X. Platform Embedded Security Technology Revealed: Safeguarding the Future of Computing with Intel Embedded Security and Management Engine. Apress, 2014.

4. Wojtczuk R., Tereshkin A. Introducing Ring-3 Rootkits. URL: http://invisiblethingslab.com/itl/Resources.html, 2009.

5. Intel. 64 and IA-32 Architectures Software Developer's Manual. URL: http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html.

6. Intel. Trusted Execution Technology. URL: http://www.intel.com/content/www/us/en/trusted-execution-technology/trusted-execution-technology-security-paper.html.

7. Advanced Micro Devices, Inc. AMD64 ArchitectureProgrammer's Manual Volume 2: System Programming. URL: http://support.amd.com/TechDocs/24593.pdf. June 2015.

8. Costan V., Devadas S. Intel SGX explained. IACR Cryptology // ePrint Archive, 2016. p. 86.

9. AMD TATS BIOS Development Group. AMD Security and Server Innovation. URL: http://www.uefi.org/sites/default/files/resources/UEFI PlugFest AMD Security and Server innovation AMD March 2013.pdf, 2013.

10. ARM. ARM Security Technology – Building a Secure System using TrustZone Technology. URL: http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/ PRD29- GENC-009492C trustzone security whitepaper.pdf, 2019.

11. Raz Ben Yehuda, Roee Leon, Nezel Jacob Zaidenberg ARM Security Alternatives // Proceedings of the ECCWS 2019 (At Coimbra, Portugal, July, 2019). At Coimbra, 2019. PP. 604–612.

12. Rosenberg D. QSEE TrustZone kernel integer overflow vulnerability // Proceedings of the Black Hat Conference, 2014.

13. Доверенная платформа для процессоров ARM // ЗАО "Аладдин Р. Д." URL: https://www.aladdin-rd.ru/catalog/tsm (дата обращения: 10.12.2019).

14. Сертификат соответствия ФСТЭК России № 4155 // ЗАО "Аладдин Р. Д." URL: https://www.aladdin-rd.ru/public/files/tsm/sertifikat_fstek_4155_tsm.pdf (дата обращения: 10.12.2019).

УДК 007:519.2
ГРНТИ 27.43.15

МОДЕЛИ БИНАРНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ. ПРОДОЛЖЕНИЕ

В. А. Медведев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Продолжается описание подхода к исследованию бинарной последовательности как модели различных её реализаций, в которой дискрета может случайным образом принимать одно из двух возможных значений, обозначенных как 0 и 1. Развиваются понятия и уточняются определения, сформулированные в [1]. Выполнен переход от понятия вероятности отсчета значения одной позиции к понятию плотности значений бинарной последовательности. Показано различие между средним значением и математическим ожиданием числа нулей (единиц) для конечного фрагмента бинарной последовательности.

бинарная последовательность, модель, вероятность, среднее значение.

Если имеется реализация бинарной последовательности (БП), и если даже она детерминированная (известен закон чередования нулей и единиц), всё равно элемент случайности остаётся. Он связан с входом в неё, с нача-

лом. Именно поэтому все последовательности – случайны. Для их исследования применяются модели, которые позволяют получить не случайные характеристики этих случайных последовательностей.

Первой, самой общей моделью БП, является представление её замкнутой бесконечностью, в которой нули и единицы чередуются случайным образом [1].

Если Q – количество позиций в последовательности, а q – общее количество единиц в последовательности, то вероятность получить единицу при отсчете одной позиции определяется следующей константой:

$$P(1) = \frac{q}{Q}. \quad (1)$$

Вероятность получить нуль при отсчете одной позиции определяется соотношением

$$P(0) = \frac{Q-q}{Q}. \quad (2)$$

Естественно, что

$$P(0) + P(1) = 1. \quad (3)$$

Исходя из последнего, в дальнейшем будем использовать одну из указанных вероятностей.

Этим исчерпываются возможности данной модели.

Первым расширением этой модели является задание условных вероятностей при отсчете двух соседних позиций. Например, чтобы получить пару «01», следует воспользоваться условной вероятностью $P(0/1)$, обозначающей нахождение «1» рядом с «0»:

$$P(01) = P(0)\,P(0/1). \quad (4)$$

Т. к. модель БП – замкнутая, то она не чувствительна к направлению и как показано в [1] в этом случае $P(01) = P(10)$. Это свойство БП даёт возможность получить безусловные вероятности БП через условные вероятности [1]:

$$P(0) = \frac{P(1/0)}{P(1/0)+P(0/1)}; \quad (5)$$

$$P(1) = \frac{P(0/1)}{P(1/0)+P(0/1)}. \quad (6)$$

Следующее расширение исходной модели предполагает отсчет трёх соседних позиций БП. Возникают вероятности типа $P(11/0)$ или $P(01/1)$, обозначающие получение результата отсчета одной позиции при известных значениях двух предыдущих. В результате условные вероятности предыдущего расширения модели БП получают определение через эти условные вероятности [1]:

$$P(1/0) = \frac{P(11/0)}{P(11/0) + P(01/1)}; \quad (7)$$

$$P(0/1) = \frac{P(00/1)}{P(00/1) + P(10/0)}. \quad (8)$$

Применяя подобный приём можно последовательно расширять исходную модель БП. Используемые при этом условные вероятности формируют иерархическую структуру, на вершине которой располагается безусловная вероятность исходной модели.

На рис. изображен фрагмент структуры вероятностей модели бинарной последовательности (применительно к вероятности $P(0)$).

«Недостаток» описанной модели заключается в том, что первичные определения, заданные соотношениями (1) и (2), устанавливают вероятности «изолированных», произвольных отсчетов, никак не связанных между собой. Это – что называется независимыми испытаниями. Они не указывают конкретную позицию, а устанавливают вероятности отсчета одной позиции; любой позиции; позиции вообще.

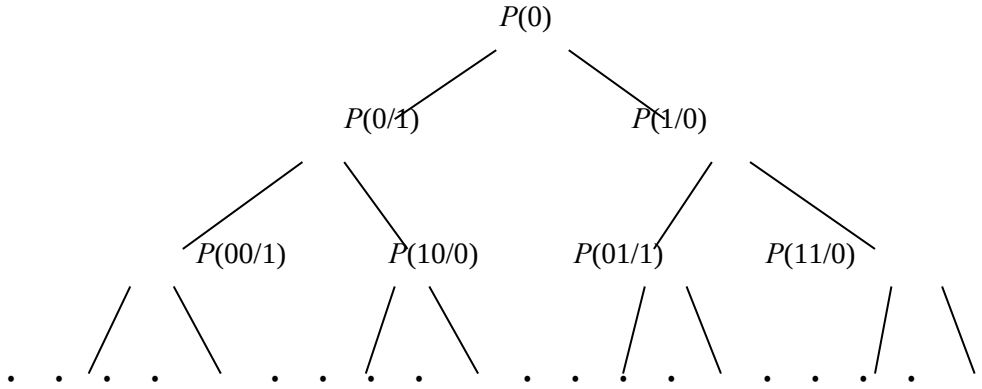


Рис. Структура вероятностной модели бинарной последовательности

Для устранения этого «недостатка» приходится вводить условные вероятности: сначала для двух соседних отсчетов, затем – для трёх, потом – для четырёх, etc. Но всё равно исходной точкой их определения являются вероятности $P(0)$ и $P(1)$. Однако, как показывает рис., от условных вероятностей можно придти к безусловным. Тем самым получаются первичные определения (вероятности) из дополнительно введенных сторонних

средств, которые также являются вероятностями (данное направление подробно рассмотрено в [2, 3, 4, 5]). Но эти вероятности никак не определены данной моделью.

Однако вернёмся к истокам. Как ни странно, но соотношение (1) имеет и иной смысл. Оно задаёт не только вероятность получения значения БП при отсчете одной позиции, но и плотность распределения этого значения для БП. Другими словами, оно определяет плотность единиц в БП, т. е. как часто (плотно) они размещены в ней.

Таким образом, установлено, что вероятность – это плотность. Но знак равенства между ними ставить нельзя. Потому что плотность – это не вероятность; она самостоятельно определяется (в различных сферах) без всякого упоминания о вероятности.

Если $P(1)$ обозначить через «p», а плотность единиц в БП – через «d», то последняя констатация может быть обозначена так:

$$p => d, \tag{9}$$

что означает: «p» это «d»; обратное не верно.

Хотя плотность и существует отдельно от вероятности, но они всё-таки связаны в (9). В контексте модели БП единицей измерения плотности является одна позиция последовательности. Величина «d», согласно (9) и (1) показывает, сколько единиц приходится на одну позицию. Но получить единицу на позиции БП есть событие случайное, а плотность есть величина не случайная; она характеризует среднее количество единиц, приходящихся на одну позицию БП.

Если взять «n» позиций, то величина «d·n» определит число единиц, приходящихся на эти позиции. И эта величина равна среднему значению числа единиц, находящихся на нескольких позициях БП. Таким образом, плотность характеризует среднее значение.

Плотность «d» связана с одной позицией БП и её численное значение всегда меньше единицы. Но рассмотрение «n» позиций БП приводит к тому, что связанная с ними плотность «d·n» в общем случае может быть произвольным числом (обычно больше единицы). А плотность – это среднее; среднее случайной величины. Поэтому рассмотрение «n» позиций БП естественным образом определяет новую случайную величину – число единиц, попавших на «n» позиций БП, значениями которой являются целые неотрицательные числа. И у этой случайной величины присутствует первая характеристика – среднее значение «d·n».

В классической теории вероятностей у случайной величины есть своё среднее, которое называется математическим ожиданием. Очевидно, что значение математического ожидания этой новой случайной величины

должно совпадать со средним значением «d·n». Если математическое ожидание обозначить через «M», то последнюю констатацию можно записать так:

$$M => dn, \tag{10}$$

что означает: «M» это «d» умноженное на «n»; обратное не верно.

Математическое ожидание определяется строго математически как сумма произведений значений случайной величины и соответствующих им вероятностей.

$$M = \sum_{k=0} k\, p_k\,, \tag{11}$$

где p_k – вероятность значения «k».

Как видно из (11), математическое ожидание отнюдь не зависит от среднего значения «dn»; оно определяется взвешенной суммой входящих в него значений. Запись (10) с точки зрения математики означает лишь одно: численное значение математического ожидания «M» должно равняться численному значению среднего «dn» в рамках данной модели бинарной последовательности.

Исходя из вышеизложенного, становится очевидным, что входящие в (11) вероятности p_k должны быть выведены только из данной модели бинарной последовательности. Задача состоит в том, чтобы определить их.

Список используемых источников

1. Медведев В. А. Модели бинарной последовательности//IV Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: сб. науч. ст. Т. 1. СПб. : СПбГУТ, 2015. С. 538–542.

2. Медведев В. А. Вероятностные характеристики бинарной последовательности // V Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: сб. науч. ст. Т. 2. СПб. : СПбГУТ, 2016. С. 137–140.

3. Медведев В. А. Вероятностные характеристики бинарной последовательности. Продолжение // VI Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: сб. науч. ст. Т. 3. СПб. : СПбГУТ, 2017. С. 329–333.

4. Медведев В. А. Вероятностные характеристики бинарной последовательности. Окончание // VII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: сб. науч. ст. Т. 2. СПб. : СПбГУТ, 2018. С. 491–494.

5. Медведев В. А. Вероятностные характеристики бинарной последовательности. Резюме // VIII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: сб. науч. ст. Т. 2. СПб. : СПбГУТ, 2019. С. 453–457.

УДК 621.396.4
ГРНТИ 49.33.29

ОПТИМИЗАЦИЯ ЭФФЕКТИВНОСТИ ЦЕНТРА ОБРАБОТКИ ДАННЫХ

Н. В. Михайличенко, М. А. Попков, В. Н. Стриженко, Я. М. Султанова

Военная академия связи

На основе анализа процессов функционирования существующих центров обработки данных в статье рассмотрены проблемы, возникающие в процессе их функционирования. Рассмотрены методы управления дата-центрами, которые способны повысить эффективность их функционирования Определены способы и пути решения данных проблем.

центр обработки данных, ИТ-инфраструктура, эффективность функционирования.

В настоящее время в свете сокращения финансирования и роста требований к производительности ИТ-инфраструктуры, необходимо внедрение новых процессов управления инфраструктурой дата-цента (ЦОД) [1]. Происходит внедрение решений способных повысить эффективность ЦОД, упростить методы управления им, повысить надежность и снизить затраты на его эксплуатацию.

Современные дата-центры получили большое развитие. Поскольку организации, эксплуатирующие ЦОД, переходят от распределенных вычислительных ресурсов к более централизованным операциям, конфигурация и управление дата-центрами стали более важными факторами для успешного функционирования организации. Виртуализация хранилищ данных, ужесточение требований к соответствию нормативным документам и более широкое использование цифровых технологий способствовало росту зависимости организации от ресурсов ЦОД [2, 3]. Увеличение расходов, связанных с ростом потребления энергии дата-центрами является основной проблемой организаций, но последствия выходят далеко за рамки бюджетных проблем. Однако прямое влияние резкого увеличения требований к энергопотреблению представляет собой лишь часть проблем инфраструктуры, присущих современным более масштабным и критически важным ИТ-инфраструктурам. ИТ-ресурсы должны быть чрезвычайно гибкими, чтобы их можно было быстро обновлять, реконфигурировать и расширять в соответствии с меняющимися требованиями. Это может быть чрезвычайно дорогостоящим мероприятием, поскольку изменение существующих систем

и внедрение новых ресурсов связано как с капитальными, так и с эксплуатационными расходами. Этот факт является еще более сложным для организаций, которые уже достигли максимума доступной емкости ЦОД. Для этого организации, эксплуатирующие ЦОД, должны принимать очень дорогостоящие меры по расширению существующих мощностей дата-центра или принять меры для максимального увеличения существующего пространства, что является более прагматичным и экономически эффективным подходом.

Основным методом, который в настоящее время используется для повышения эффективности использования энергии, пространства и производительности центра обработки данных, является консолидация серверов на более мощных платформах (таких как *blade*-серверы, мэйнфреймы и суперкомпьютеры) [4]. Однако этот подход создает ряд новых проблем для управления ИТ-инфраструктурой.

Определение того, какие услуги наиболее подходят для консолидации, определение оптимальной конфигурации инфраструктуры и управление более сложными аппаратными платформами, способствуют росту проблем управления дата-центрами [5].

Для обеспечения эффективного функционирования дата-центра необходимо рассмотреть уровни развития эффективности ЦОД.

Уровень 1 (реактивный). Процессы управления дата-центром определяются в основном инцидентами и решаются в основном с помощью ручных воздействий, дополненных некоторыми сценариями. Инструменты управления, как правило, зависят от устройства, с небольшим количеством инструментов корпоративного класса и практически без автоматизации. Ключевые элементы этого этапа включают в себя:

– использование элементно-ориентированных инструментов управления;

– управление реагирует на инциденты;

– безопасность ограничивается изолированными точечными решениями – в первую очередь брандмауэрами и антивирусным программным обеспечением;

– основные решения должны повысить эффективность и сократить расходы.

Уровень 2 (активный). На данном этапе все еще остаются первостепенными оперативные проблемы, но некоторые процессы в настоящее время документированы и повторяются. Инструменты управления используются целыми отделами и включают в себя некоторую, хотя и ограниченную, автоматизацию. Управление уровнем обслуживания остается в реальном времени с производительностью и доступностью:

– мониторинг и автоматизация управления минимальны;

– основные проблемы на улучшении доступа и контроля, безопасности и аварийного восстановления.

Уровень 3 (проактивный). Процессы управления по-прежнему в первую очередь обусловлены проблемами, но их легче исправить с помощью процедур для определения первопричины. Это представляет собой переход от реактивного управления инцидентами к предотвращению проблем. Инструменты управления интегрированы и автоматизированы в нескольких управляемых средах, а оповещения в режиме реального времени. Ключевыми элементами этого этапа являются:

– решения для управления теперь выбираются стратегически, а не реактивно;

– рабочие процессы автоматизированы для сбора лучших практик.

Уровень 4 (динамический). На наиболее зрелом этапе управления центрами обработки данных повседневные проблемы с производительностью и доступностью в значительной степени решаются с помощью автоматизации, поэтому ИТ-специалисты могут сосредоточиться на динамической оптимизации инфраструктуры ЦОД. Планирование новых услуг и повышение качества обслуживания – это главное, а не просто поддержка или устранение поломок. Инструменты управления предоставляют подробные данные о среде, которые позволяют принимать реальные решения по управлению инфраструктурой ЦОД. Ключевыми элементами этого этапа являются:

– имеются автоматизированные решения для почти всех функций управления, включая корректирующие действия, отчеты, динамическое предоставление услуг и управление изменениями.

В заключении можно ряд факторов, которые позволят поддерживать ЦОД в режиме максимальной готовности. Внедрение в ЦОД единой системы диспетчеризации и мониторинга. Описание порядка действий персонала в случае наступления нештатной ситуации. четкий регламент профилактических работ по всем инженерным системам ЦОД. Заключение сервисных договоров со специализированными организациями, где оговариваются время реакции на проблемы и сроки ее устранения. Оптимальный подбор обслуживающего персонала.

Список используемых источников

1. Паращук И. Б., Михайличенко Н. В. Эффективность современных центров обработки данных // Материалы III-й Межрегиональной НПК «Перспективные направления развития отечественных информационных технологий». Севастополь: СевГУ, 2017. 256 с., С. 24–26.

2. Чуднов А. М., Путилин А. Н., Попов А. И. Комплексное управление маршрутизацией пакетов и режимами работы радиосредств в неоднородной сети передачи данных // Радиотехнические и телекоммуникационные системы», март 2019. С. 46–56.

3. Авраменко В.С. Маликов А.В. Анализ компьютерных инцидентов безопасности с применением искусственных нейронных сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании : VII Международной научно-технической и научно-методической конференции: в 4 т. Т. 2. СПб.: СПБГУТ, 2018. 670 с. С. 7–11.

2. Крюкова Е. С., Малофеев В. А., Паращук И. Б. Анализ современных подходов к оценке качества систем хранения данных и электронных библиотек. // XVI Международная научно-практическая конференция «Новые информационные технологии и системы» (НИТиС-2019). Пенза, 2019. 312 с., С. 177–180.

3. Бирюков М. А. Разработка модели нарушителя правил разграничения доступа к единому информационному пространству // Математические методы в технике и технологиях – ММТТ. 2017. Т. 3. С. 107–110.

УДК 004.8
ГРНТИ 28.23.01

ИССЛЕДОВАНИЕ ВОПРОСОВ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ СВЯЗИ И УПРАВЛЕНИЯ

О. А. Михалев, М. И. Петренко, В. С. Типаков, Д. Ф. Ткачев, Т. А. Яковлев

Военная академия связи

Рассматриваются вопросы применения элементов искусственного интеллекта, как элемент развития сопутствующих систем. Внедрение и применение передовых технологий в системах связи и управления. Указывается, что построение и использование интеллектуальных блоков на основе нейронных сетей позволяет использовать имеющиеся классические алгоритмы, так и находить новые пути решения существующих задач.

искусственный интеллект, системы связи, системы управления, нейронные сети, когнитивные блоки управления.

Искусственный интеллект (ИИ) – это научное направление, которое изучает и разрабатывает теории, методы, технологии и прикладные системы для моделирования, развития и расширения человеческого интеллекта. Фундаментальная природа ИИ заключается в моделировании процесса мышления человека. Прошло более полувека с тех пор, как концепция ИИ была официально предложена в 1956 году. В течение всего этого времени люди неустанно занимались научными открытиями и технологическим развитием в смежных областях исследований в надежде лучше понять суть вопроса. Как и любая другая новая дисциплина, которая когда-то проходила

фазу эмбриона, раннее развитие ИИ было сопряжено с трудностями, была подвергнута сомнению, и совершила много взлетов и падений. В последние годы такие стимулы, как рост больших данных, инновации теоретических алгоритмов, улучшение вычислительных возможностей и развитие сетевых средств, привели к революционным успехам в индустрии ИИ, которая накопила знания за более чем 50 летний период [1].

Мы живем в беспрецедентную эру ИИ. Основываясь на последних достижениях алгоритмов, вычислительной мощности и больших данных, глубокое обучение, как самый яркое направление ИИ, добилось существенных прорывов в широком спектре областей, от компьютерного зрения, распознавания речи, обработки естественного языка до игры в шахматы (например, AlphaGo) и робототехники. Благодаря этим прорывам, широко признано, что различные интеллектуальные приложения значительно улучшают образ жизни людей, повышают производительность труда и повышают социальную эффективность [2].

Кроме уже привычных применений ИИ в виде интеллектуальных помощников, умных домов, автономных машин, существует ряд перспективных направлений, позволяющих использовать все аспекты технологии ИИ – это создание интеллектуальных систем для внедрения в системы связи и управления.

Решение задачи интеллектуализации систем связи и управления проявляется в проектировании интеллектуальных блоков, на основе искусственных нейронных сетей. Именно нейронные сети являются рассматриваемым элементом искусственного интеллекта.

Нейронные сети – мощный аппарат для имитации процессов и явлений, который предоставляет возможность воспроизводить достаточно сложные зависимости. Нейронные сети позволяют находить решения для задач с высокой размерностью. Другая их особенность – возможность обучения такой сети. Процесс обучения – подгонка параметров той модели процесса или явления, которая реализуется нейронной сетью. Нейронная сеть состоит из простейших элементов сети – искусственных нейронов. Модель искусственного нейрона: векторный или скалярный входной сигнал умножается на векторный или скалярный весовой коэффициент, результирующий взвешенный вход является аргументом функции активации нейрона. Следовательно, при внедрении в систему нейронной сети необходимо решить следующий перечень задач: выбор сети с определенной технологией, определение набора параметров, которые необходимы для управления, подбор структуры нейронной сети. После определения количества слоев сети и числа нейронов в каждом из них назначается значение весов и смещений, которые минимизируют ошибку решения. Это достигается с помощью процедур обучения [3].

Многообразие применения нейронных сетей определяется их возможностями, тем самым решается целый спектр задач в системах связи и управления. К примеру, если обучить нейронную сеть анализировать канал передачи данных, можно получить адаптирующуюся под изменяющуюся среду систему – когнитивную радиосвязь, архитектура которой изображена на рис. [4].

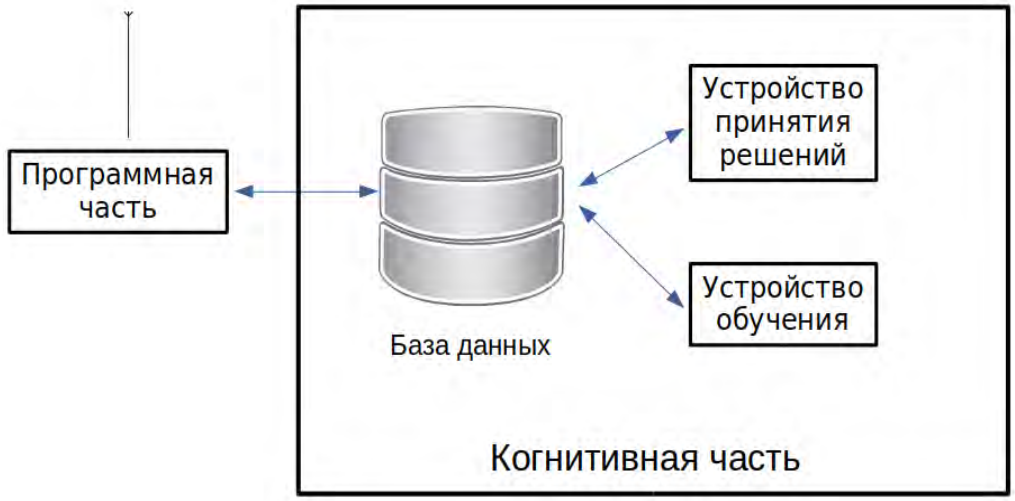


Рис. Архитектура когнитивного радио с использованием искусственного интеллекта

Выделяют четыре основные области применения искусственных нейронных сетей в системах связи:

– управление коммутацией;
– маршрутизация;
– управление трафиком;
– распределение каналов в подвижных системах радиосвязи.

Используя нейронные сети, возможна реализация множества алгоритмов для быстрой и безопасной передачи информации по сетям связи. Тут и методы построения безопасных маршрутов, надежность которых характеризуется состоянием кабельных линий и реализация технологий высокоскоростной коммутационной сети с пакетной передачей для повышения пропускной способности, где нейронная сеть выступает в роли интеллектуального коммутатора, и др. За счет «умной» коммутации становится возможным построение коммутаторов с нейросетевым управлением на несколько сотен каналов. Такая система обеспечивает устранение или ослабление влияния возникающих неисправностей отдельных элементов сети и изменения во времени потоков информации между абонентами и узлами сети на качество обслуживания заявок абонентов и передачи инфор-

мации. При использовании искусственных нейронных сетей в многоступенчатых системах связи, где основные встречающиеся трудности данных систем обусловлены тем, что заранее неизвестны параметры характеризующие потоки информации, а также требования к качеству могут со временем меняться, нейронная сеть решает задачи оптимизации [5].

Кроме вышеуказанных областей применения, перспективными является использование нейронных сетей в задачах кодирования и декодирования, обработки речевой информации, изображения и видео, оптимизации сжатия информации [6].

Искусственные нейронные сети отлично показывают себя в системах управления. Интеллектуальный контроллер на основе нейронной сети выполняет задачу выработки необходимого адекватного управляющего сигнала для управления сменой состояний управляемого объекта от начального состояния до необходимого итогового состояния. Смена должна происходить по оптимальной траектории. Исполнение интеллектуального контроллера и контроль за объектом управления в большей степени зависят от выбранного алгоритма обучения и используемой структуры управления.

Используя нейронные сети, возможно использовать как классические алгоритмы управления, так и находить новые решения. В итоге получается необходимый инструментарий для применения и внедрения, а также разработки новых систем управления, некоторые представлены в работах [7, 8, 9]:

– построение систем множественного доступа;
– построения системы прогнозирующего управления;
– адаптивные системы управления нелинейными динамическими объектами;
– интеллектуальные самоорганизующиеся системы управления.

В результате, тенденции развития передовых технологий, в данном случае искусственного интеллекта, нарастающая актуальность и увеличение возможностей ее применения, влечет за собой развитие и современность систем связи и управления. Придает толчок к ретроспективе уже известных алгоритмов, чтобы вдохнуть новую жизнь.

Список используемых источников

1. Zheng You, Shaojun Wei, White Paper on AI Chip Technologies – Beijing Innovation Center for Future Chips (ICFC), 2018.

2. Zhi Zhou, Xu Chen, En Li, Liekang Zeng, Ke Luo, Junshan Zhang Edge Intelligence: Paving the Last Mile of Artificial Intelligence with Edge Computing. Proceedings of the IEEE Volume: 107 , Issue: 8 , Aug. 2019, 1738–1762.

3. Федотов В. В. Применения нейронных сетей в телекоммуникационных сетях связи // Известия высших учебных заведений. Северо-Кавказский регион. Естественные науки 2004. № 5. С. 90–94.

4. Мирошникова Н. Е. Обзор систем когнитивного радио // T-Comm - Телекоммуникации и Транспорт 2013. № 9. С. 108–111.

5. Лавренков Ю. Н., Комарцова Л. Г. Анализ характеристик канала передачи информации на основе нейронной сети // Прикладная информатика. 2014. № 5. С. 79–99.

6. Комашинский В. И., Смирнов Д. А., Нейронные сети и их применение в системах управления и связи. М. : Горячая линия–Телеком, 2003. 94 с.

7. Степанов М. Ф. Интеллектуальные самоорганизующиеся системы автоматического управления. Саратов: Сарат. гос. техн. ун-т, 2002. 112 с.

8. Безручко Т. В., Шипитько И. А. Об одном методе построения системы прогнозирующего управления на основе нейронной сети // Вологдинские чтения. 2007. С. 38–40.

9. Хо Д. Л. Синтез адаптивных систем управления нелинейными динамическими объектами на базе нечетких регуляторов и нейросетевой технологии : дис. ... д-ра техн. наук : 05.13.01 / Хо Дак Лок. М., 2002. 233 с.

УДК 004.932.2
ГРНТИ 20.53.19

ИССЛЕДОВАНИЕ МЕТОДОВ ОБРАБОТКИ ИЗОБРАЖЕНИЯ

Т. В. Мусаева

Санкт-Петербургский государственный университет телекоммуникаций им проф. М. А. Бонч-Бруевича

В статье рассматривается вопрос определения процента ветхости изображения. Для достижения цели предлагается исследование существующих методов обработки изображения в программе LabView для выбора оптимального.

изображение, ветхость, качество.

В области компьютерной графики объектами исследования являются графические изображения разного формата, типа и назначения. Многие процедуры обработки изображений заключаются в их препарировании, то есть в приведении к такому виду, которые могут отличаться от оригинала (эталона), но позволяют осуществить визуальную интерпретацию и машинный анализ.

Выбор оптимального метода, более подходящего для решения определенного круга задач является важным.

Проблема определения качества изображения на вопрос ветхости является актуальной. Цель работы – исследование методов и алгоритмов обработки изображений для определения соответствия.

К объектам исследования в данном вопросе могут относиться искусственно созданные изображения с помощью средств современных техноло-

гий. Такие изображения могут быть разного содержания и назначения, созданные и измененные с применением разных методов. К ним могут относиться фотографии, картины (созданные на планшете), денежные банкноты, карты местности и т. д. Все исследуемые объекты – растровые изображения. Данные исследования могут быть актуальны для задач определения ветхости изображений денежных банкнот, фотографий, автоматического распознавания документов, изображений местности и т. д.

Предмет исследования – критерии, методы определения процента ветхости изображения.

Любые изображения на разных носителях информации имеют свой жизненный цикл от момента создания до момента утилизации. Этот жизненный цикл имеет разный период и может меняться в зависимости от естественных и искусственных воздействий и причин.

Существуют разные методы и критерии, определяющие качество изображения в бумажном или цифровом формате. Метод определения на вопрос изношенности может определяться визуально, тактильно для бумажных вариантов представления информации. Изношенным может быть сам носитель (бумага) и изображение. К разновидностям изношенности могут относиться повреждения, плохое качество при масштабировании, наличие шумов и т. д. Качество бумаги может влиять на качество самого изображения. Плохое качество изображения не может влиять на носитель. В цифровом представлении изменение масштаба изображения (растрового), может влиять на качество. Изображение, полученное разными способами, может иметь разное качество. Или же изображение может менять свое качество в процессе поэтапной визуализации.

В большом современном толковом словаре русского языка 2012 года дано следующее определение, ветхость – полуразрушенное состояние, изношенность [1]. Далее, в работе будет использован термин «изношенность».

Если рассматривать вопрос изношенности цифрового изображения, то на сегодняшний день нет четких определений по данному критерию, нет регламентирующих документов, которые бы раскрывали суть термина. Но, в соответствии с регламентирующими документами Банка России, существуют определенные требования, определяющие признаки ветхих банкнот [2].

Критерии определения ветхости купюры: наличие равномерного общего загрязнения поверхности (снижение яркости изображения на 8 процентов и более), разрывы краев, сквозные отверстия (проколы), посторонние надписи, рисунки, штампы, контрастные пятна, а также купюры рваные, заклеенные, обожженные и т. д. [2].

Из перечисленных критериев в данной статье рассматривается только вопрос, относящийся к яркости, цветности изображения, определяемый лю-

бым устройством спектрофотометрического или колориметрического измерения цвета, позволяющим преобразовывать результаты измерений в параметры колориметрической системы CIE LAB, либо путем визуального сравнения. В разных странах по данному вопросу имеются свои требования.

Для объективности исследования в работе выбраны два объекта исследования, образец фотографии и денежной банкноты на вопрос определения процента соответствия негатива или изношенного изображения оригиналу. Вопрос идентификации подлинности образца не рассматривается.

К изображениям применяются одинаковые методы преобразований (инверсия, сепия), сравниваются результаты применения этих преобразований.

Любое изображение можно представить в виде значений элементов матрицы, размерностью $n\ x\ m$ (1).

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{1n} \\ a_{21} & a_{22} & a_{2n} \\ \dots\dots & \dots\dots. & \dots\dots. \\ a_{m1} & a_{m2} & a_{nm} \end{bmatrix}_{nxm}, \quad (1)$$

где $a_{nm} = \{x_{nm}, y_{nm}\}$ – это координаты пикселя в двумерной системе координат.

Кроме координат, каждый пиксель имеет цвет, например совокупность значений модели RGB, в пределах от 0 до 256.

Эталон изображения и его прототип (изношенное изображение) представляются в виде двух матриц для сравнения значений элементов. Каждый элемент сравнивается по сумме трех значений модели RGB. Вычисляется процент несоответствия каждого элемента на вопрос цветности (2).

$$B = \begin{bmatrix} b_{11} & b_{12} & b_{1n} \\ b_{21} & b_{22} & b_{2n} \\ \dots\dots & \dots\dots. & \dots\dots. \\ b_{m1} & b_{m2} & b_{nm} \end{bmatrix}_{nxm}, \quad (2)$$

где $b_{nm} = \{x_{nm}, y_{nm}\}$ – это координаты пикселя в двумерной системе координат, и $a_{nm} = b_{nm}$ – координаты растрового изображения должны оставаться неизменными для эталона и прототипа для точности сравнения.

Для возможности сравнения прототипа и эталона, уменьшения изношенности, изменяются значения компонентов цвета методом инвертирования яркости растрового изображения, что позволяет осветлить тёмные области и затемнить светлые, что улучшает процесс глобальной пороговой обработки. Яркость – величина, характеризующая цвет, измеряемая по ахроматической шкале и изменяющаяся от черного до белого, также называется

светлотой или отражением света, иначе, это количество белого цвета на изображении. Чем выше яркость, тем светлее изображение. Значения яркости находятся в диапазоне от 0 до 255. Для того чтобы яркость можно было уменьшать и увеличивать, значения яркости берут в диапазоне от -255 до 255, затем по формуле вычисляют цвет и приводят к диапазону от 0 до 255.

Модель *RGB* можно представить в виде множества $K = \{k_r, k_g, k_b\}$, где k_r, k_g, k_b имеет диапазон значений от 0 до 256 (3).

$$I * (K) = M - [K]_{mxn}, \quad (3)$$

где $M = 256$

Инвертирование не всегда улучшает работу алгоритма глобальной пороговой обработки. Если гистограмма изображения представляет собой очень сложную форму, то тогда инвертирование не имеет смысла, ведь от этого общая сложность формы гистограммы не изменится, и алгоритм корректно работать не будет.

Сравнение первичного (эталона) изображения и его преобразованного прототипа позволяет оценить изношенность и соответствие, осуществить отбор подходящего метода, путем исключение не существенных для определенного круга задач. Также этот выбор может быть нацелен на значительное лучшее визуальное качество обработанного изображения.

В виду того, что не разрешается редактировать денежные банкноты в оригинале, и многие редакторы также блокируют эту возможность, то в работе приведены только результаты сравнения.

При исследовании выполнено несколько этапов работ. При первичном компьютерном представлении оригинала изображение имеет высокое качество яркости, насыщенности. визуальность восприятия на точность соответствия равна 99 %. При исследовании цифровой версии денежной купюры наблюдается максимальное соответствие оригиналу по цветности, ветхости изображения, точность передачи 95 %.

При сохранении фотографии в формате bmp (256-цветный рисунок) качество визуально не меняется в сторону ухудшения, уменьшается коэффициент яркости, насыщенности. При сохранении банкноты качество изображения отличается от цифрового оригинала на 20 %, появляются шумы в оттенках зеленого цвета. Цветовые оттенки могут быть иными, при выборе другого изображения.

В работе проведено поэтапное изменение изображения по выбранной шкале измерений RGB. На рис. 1 представлено изображение, полученное методом обратного преобразования.

Рис. 1. Метод обратного преобразования

На рис. 2 для сравнения представлены изображения оригинала и изображения, полученного обратным преобразованием.

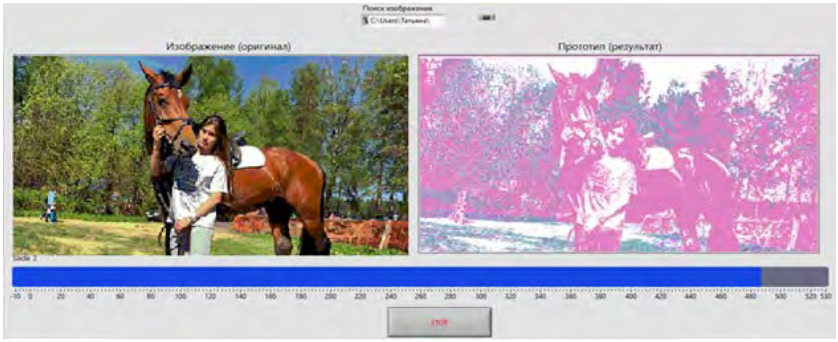


Рис. 2. Сравнение изображений

В результате проведенного исследования, осуществленного в программе LabView, были сделаны выводы о том, что одни и те же примененные методы по-разному влияют на результат визуализации изображений, отличающихся по цифровому представлению. Также, для определения изношенности изображений денежных банкнот и фотографий рассмотренные методы не дают ожидаемых результатов. Визуальное восприятие имеет меньший процент погрешности, чем погрешность при цифровой обработке. Операции бинарного квантования могут быть применены, если для анализа требуется выделить только очертание объекта на изображении, без детализации внутреннего содержимого объектов и фона. Выбранные для исследования критерии яркости и цветности не позволяют дать точную визуальную информацию о проценте ветхости изображения. Погрешность измерений на вопрос ветхости достаточно высокая, что требует введения дополнительных критериев и применения других методов обработки изображения для определения ветхости.

Список используемых источников

1. Тезаурус русского языка [Электронный ресурс]. 2012. URL: https://slovar.cc/rus/tezaurus/ 1387527.html

2. Банкноты Банка России, содержащие повреждения, перечень которых установлен в приложении к Указанию Банка России от 27.02.2010 № 2405 «О внесении изменений в Положение Банка России от 24 апреля 2008 года № 318-П «О порядке ведения кассовых операций и правилах хранения, перевозки и инкассации банкнот и монеты Банка России в кредитных организациях на территории Российской Федерации», зарегистрированному Министерством юстиции Российской Федерации 23.03.2010 № 16687, кредитными организациями и их внутренними структурными подразделениями выдаче клиентам не подлежат и сдаются в учреждения Банка России.

3. Гурченков А. А., Бочкарева В. Г., Мурынин А. Б., Трёкин А. Н. Улучшение качества изображений методом экстраполяции пространственных спектров // Вестник Московского государственного технического университета им. Н. Э. Баумана. Серия естественные науки. 2016. № 2 (65). С. 91–102.

4. Вудс Р., Гонсалес Р. Цифровая обработка изображений. М. : Техносфера, 2005. 1072 с.

5. Визильтер Ю. В. [и др.] Обработка и анализ цифровых изображений с примерами на LabVIEW и IMAQ VIsion. М. : ДМК, 2017. 464 с.

УДК 004.7:004.422.8
ГРНТИ 20.01.07

ИССЛЕДОВАНИЕ МЕТОДОВ И СРЕДСТВ РАСПРЕДЕЛЕННЫХ РЕГИСТРАЦИЙ В ИНФОРМАЦИОННЫХ СТРУКТУРАХ

Л. К. Птицына, Т. Р. Сулякаев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Показана объективная необходимость развития методического сопровождения распределенных систем. Поставлены задачи расширения методического сопровождения жизненного цикла систем распределенных регистраций данных в информационных структурах. Выделены методы оптимизации распределения регистраций по узлам компьютерной сети. Представлены основные компоненты методики определения функциональной спецификации типовой системы распределенных регистраций в информационных структурах. Описаны базовые средства распределенных регистраций данных в информационных структурах.

распределенная система, методическое сопровождение, расширение, оптимизация, компоненты, информационная структура, средства.

В настоящее время проводятся обширные научные исследования по профильным вопросам организации информационных структур и оптимизации их корпоративных сегментов [1, 2, 3]. Реальные условия жизнеде-

ятельности в социуме в критических ситуациях становятся основным фактором скачкообразного повышения значимости информационных структур, их функциональности, качества функционирования, надежности и живучести. Новыми реалиями повышенной степени распределенности и высоких интенсивностей использования информационных структур в социуме предопределяется объективная необходимость совершенствования технологического сопровождения информационных структур.

В соответствии со «Стратегией развития информационного общества Российской Федерации на 2017–2030 годы», с программой «Цифровая экономика Российской Федерации», «Национальной стратегией развития искусственного интеллекта Российской Федерации» и с анализом известных результатов научных исследований в области организации информационных структур актуализируется необходимость развития формализаций по организации распределенных регистраций в информационных структурах.

В контексте представленной актуальности целью проводимых исследований является повышение производительности распределенной системы за счет обработки большого объема данных при рациональном размещении информационных файлов в компьютерной сети, а также формирование необходимого состава аппаратно-программных средств, ориентированных на распараллеливание операций и предназначенных для обработки больших объемов данных с учетом распределения регистраций данных.

Для достижения поставленной цели решаются следующие задачи:

1. Систематизация представлений знаний о технологиях обработки больших массивов данных в распределенных информационных структурах.

2. Разработка модификаций известных архитектурных решений для повышения производительности информационных структур, эффективность которых зависит от технологий обработки данных в режиме реального времени и от времени отклика в условиях распределения регистраций данных.

3. Формирование математического обеспечения типовой интеллектуальной системы распределенных регистраций в информационных структурах.

Проведённый анализ современного состояния и перспектив развития распределенных систем в информационных структурах показал, что для координация обработки распределенной информации применяются: методика организации распределенных баз данных и методика реплицирования информации.

Методика организации распределенных баз данных ориентируется на обеспечение синхронного фиксирования изменений в базах после завершения транзакций на нескольких устройствах распределенной системы.

В методике реплицирования информации предусматривается отказ от физического распределения и выполнение информационного дублирования в разных узлах сети компьютеров.

CASE-средства для моделирования данных предназначаются для ускорения процедур их разработки, снижения трудовых затрат и повышения качества проектирования.

В вариациях алгоритмов информационной обработки в компьютерной сети отлеживается многообразие требований к распределенной базе данных при обеспечении управления ее функционированием с учетом единовременного доступа, защиты и восстановления данных, которые определяются применяемой СУБД и характером возможных запросов.

Во время анализа известных достижений выделяются научные подходы к определению и оценке характеристик времени реакции, показателей производительности и показателей надежности.

Исследование вариаций в организации файлового размещения по узлам компьютерной сети с коммутацией пакетов выполняется в трех направлениях.

Первое направление сопрягается с разработкой основ теории коммутации пакетов в системах распределения.

Второе направление связывается с математической теорией оптимизации потоков в сетях и выбором выгодных сетевых маршрутов с пакетной коммутацией.

Третье направление касается разработки современных аппаратно-программных ресурсов для коммутации пакетов.

При анализе устройств распределения и переключения в сети выявляется, что применение аппаратных нагрузочных распределителей обеспечивает работоспособность сервера, состоящего из нескольких машин.

В предлагаемую методику определения функциональной спецификации типовой системы распределенных регистраций в информационных структурах вводится оптимизация распределения регистраций по узлам локальной компьютерной сети на основе численного критерия качества обслуживания.

Целевая функция (критерий качества) выбирается в виде комбинации параметров трафика по каналам связи в сети.

В методике учитывается разница во времени ожидания запросов на обслуживание в отдельных устройствах.

При использовании проанализированных моделей процессов функционирования компьютерной сети и способов оценки показателей качества обслуживания получаются квазиоптимальные решения в случае последовательной коррекции структуры и характеристик компьютерной сети.

При выборе рационального файлового размещения проводилась оценка возможностей методики оптимизационного моделирования в среде инструментальной системы Matlab.

При применении проанализированной тактики дублирования и распределения единичных фрагментов баз данных предоставляется возможность повышения производительности и уменьшения времени реакции системы за счет двух факторов: параллельной обработки однотипных запросов и возрастания доли локально доступных данных.

Для реализации алгоритмов оптимизации размещения запросов по серверам компьютерной сети предусматривается модификация. В предложенной структуре серверы распределенной базы данных, используемые для обработки больших массивов данных, объединяются между собой в единый кластер при помощи высокоскоростной вычислительной сети и программируемого активного коммутатора. В сеть вводится компьютер администратора для управления коммутатором.

Разработанный при исследованиях алгоритм балансирования загрузки узлов сети распределенной базы данных предназначается для обработки больших и сверхбольших объемов данных.

Список используемых источников

1. Васильев С. Н., Макаров А. А., Макаров В. Л., Махутов Н. А., Новиков Д. А. [и др.]. Управление развитием крупномасштабных систем. М. : Физматлит, 2015. 473 с.

2. Буренин А. Н., Легкое К. Е., Оркин В. В. Алгоритм адаптивного управления информационными системами в условиях массовых возмущений // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. №. 6. С. 90–95.

3. Горелов Б. А., Давыдов А. Д., Силаев А. В., Тихонов А. В. Модели управления развитием распределенных технических систем // Изв. вузов: Машиностроение. 2018. № 3. С. 92–103.

УДК 004.7:004.422.8
ГРНТИ 28.29.01

ФОРМАЛИЗАЦИЯ ЗАДАЧИ ПЛАНИРОВАНИЯ ДЕЙСТВИЙ В ИНТЕЛЛЕКТУАЛЬНЫХ СЕРВИС-ОРИЕНТИРОВАННЫХ СИСТЕМАХ НА ЯЗЫКЕ PDDL С ОЦЕНКОЙ ИХ КАЧЕСТВА НА ОСНОВЕ МОДЕЛЬНО-АНАЛИТИЧЕСКОГО ИНТЕЛЛЕКТА

Л. К. Птицына, Н. Эль Сабаяр Шевченко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Актуализирована задача планирования действий для динамической композиции бизнес-процессов с точки зрения онтологии. Раскрыта методика перевода онтологического описания OWL-S сервисов на язык PDDL. Построена модель динамического бизнес-процесса, объединяющего разные типовые шаблоны интеграции сервис-ориентированных средств. Выбраны показатели качества работы динамических бизнес-процессов интеллектуальных сервис-ориентированных систем. Формализован математический аппарат оценки качества временного профиля динамических бизнес-процессов для интеллектуальных сервис-ориентированных систем.

сервис-ориентированные системы, динамический бизнес-процесс, адаптивное управление качеством, временной профиль, онтология.

При переходе к цифровой экономике, с ужесточением конкуренции, ростом автоматизации промышленности и экспоненциальным увеличением больших данных актуализируется интеллектуализация сервис-ориентированных средств с адаптивным управлением их качеством, являющихся архитектурной основой корпораций, крупных кластеров и различных распределенных систем.

Сервис-ориентированная архитектура (SOA) является фундаментом интеграции и функциональной совместимости расширяющихся субъектов рынков. Однако в подавляющем большинстве современные сервис-ориентированные системы отстают своим жестким подходом к вопросно-ответному взаимодействию с окружающей средой. Главная проблема является их неспособность адаптироваться к динамическим временным регламентам и справляться с априорной неопределенностью [1]. Подобный ограничительный уклон разработки сервис-ориентированных систем справляется с фиксированным видом деятельности по принципу работы жестких бизнес-процессов, без учета изменений окружающей среды, где развернуты распределенные сервис-ориентированные средства.

Главным образом сервис-ориентированная архитектура базируется на веб-сервисах. Начальное состояние веб-сервисов включает описание всех входных данных в начале исполнения, в то время как целевое состояние описывает желаемые выходные данные по завершению бизнес-процесса. По определению будем считать, что домены предметной области изначально описаны OWL-S онтологией. Профиль онтологии определяется согласно семантике «IOPE» (*input, output, precondition, effect*). OWL-S (*Ontology Web Language for Services*) представляет собой язык для описания свойств и возможностей онтологий [2]. Следовательно, модель сервиса определяется кортежем:

$$wService = \langle wsName, wsInput, wsOutput, wsPREC, wsPOSTC \rangle;$$

где *wsName* – название веб-сервиса; *wsInput – входные параметры, wsOutput* – данные, выдаваемые сервисом по завершению его работы; *wsPREC* – предусловия для запуска сервиса, *wsPOSTC* – постусловия, эффект и состояние системы после завершения работы сервиса.

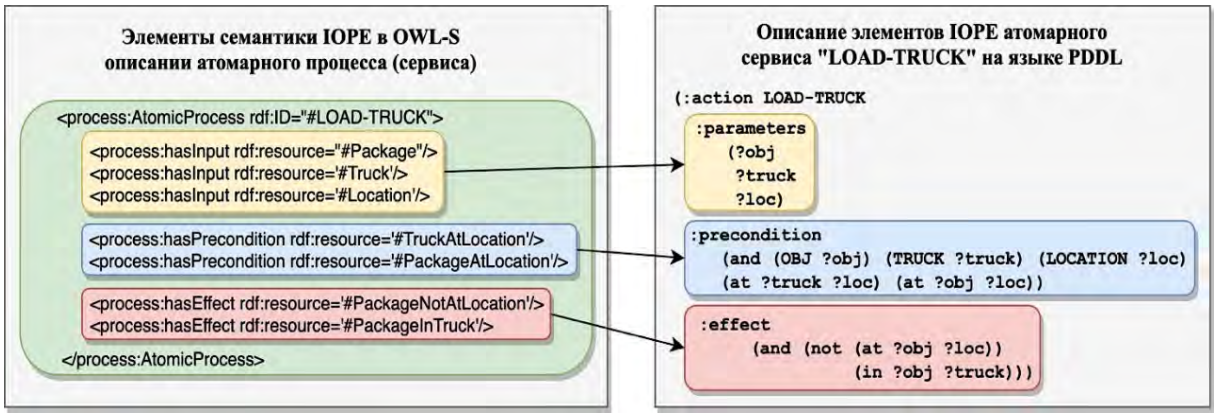


Рис. 1. Правила соответствия элементов семантики «IOPE» OWL-S сервисов на языке PDDL на примере атомарного сервиса «LOAD-TRUCK» из типового домена планирования логистики.

В качестве примера рассматривается домен предметной области и функциональной совместимости сервисов логистики, с точки зрения интеллектуальной сервис-ориентированной конфигурации. Конвертация семантических элементов «IOPE» на язык PDDL (рис. 1).

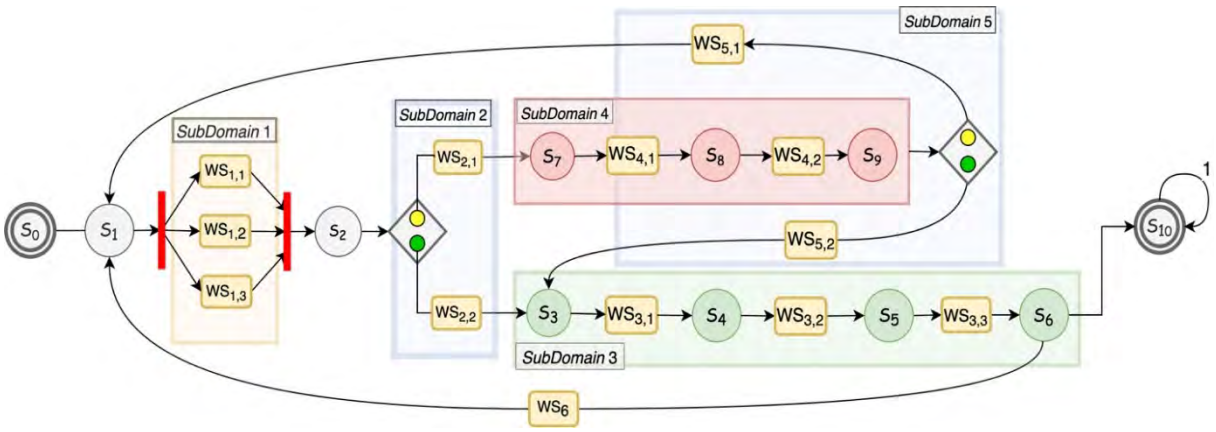


Рис. 2. Модель динамического бизнес-процесса,
объединяющего различные типовые шаблоны интеграции последовательных,
альтернативных и параллельных действий

Язык PDDL [3] представляет собой де-факто стандарт для решения большинства задач классического и нелинейного планирования, является официальным языком на международных чемпионатах по планированию, а также в последние годы разработано множество систем планирования, поддерживающих данный язык.

На рис. 2 представлен комплексный нелинейный бизнес-процесс «Logistics», чьи поддомены соответствуют типовым шаблонам интеграции. Поддомен «1» содержит сервисы параллельно выполняемые, и оценивается типовым шаблоном для параллельных действий по функции «И» и «ИЛИ». Поддомены «2» и «5» соответствуют узлам решения выбора альтернативных действий. Поддомены «3» и «4» соответствуют типовым шаблонам последовательного выполнения действий.

Важным механизмом качественной адаптации сервис-ориентированной системы к резким изменениям в окружающей среде является управление временной разверткой. В этой связи целесообразно оценивать статистические временные характеристики с помощью плотности распределения вероятностей $u(k_{1,2,\ldots,i,\ldots,I})$ дискретного времени выполнения деятельности интегрируемых сервис-ориентированных систем. Исходя из этого, выделяются следующие показатели качества:

– $E[k_{0,1,\ldots,i,\ldots,I}]$ и $D[k_{0,1,\ldots,i,\ldots,I}]$ – соответственно математическое ожидание и дисперсия дискретного времени $k_{0,1,\ldots,i,\ldots,I}$ выполнения деятельности,

– $R(k_{0,1,\ldots,i,\ldots,I} > C)$ – риск срыва временного регламента или вероятность невыполнения деятельности по установленному временному регламенту C (верхняя граница допустимого времени).

Основные этапы оценки выбранных показателей качества подробно раскрываются в работе [4].

Математическое ожидание позволяет оценить среднее время выполнения комплексируемых сервис-ориентированных средств. Дисперсия отражает разброс вокруг среднего времени выполнения. Третий показатель, риск срыва временного регламента, позволяет оценить вероятность неудачного выполнения составленной интеграции в рамках установленного временного регламента. Далее следует вызов сервисов для их интеграции согласно выбранному типовому шаблону. По завершению, формируется статистический профиль закономерностей путем кластеризации каждого вида деятельности [5], фиксируется количество единиц дискретного времени, за которое выполнилась деятельность, и присваивается соответствующая вероятность из сформированной модельно-аналитическим интеллектом плотности распределения вероятностей.

Сформированный план действий можно описать матрицей переходов между состояниями с некоторой вероятностью обратной связи, согласно теории конечных цепей Маркова [1, 6, 7]. Максимальная длительность функционирования бизнес-процесса равна количеству допустимых циклов квадратной матрицы. Последнее состояние в матрице является поглощающим, и представляет собой завершение работы бизнес-процесса. Таким образом, определяется плотность распределения вероятностей времени выполнения сервис-ориентированной деятельности с учетом обратной связи:

$$\mathbf{P} = \begin{bmatrix} 0 & f(N) & f(N-1) & f(N-2) & f(N-3) & \dots & f(1) & 0 \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 0 \\ q & 0 & 0 & 0 & 0 & \dots & 0 & (1-q) \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix},$$

где $\mathbf{P}$ – квадратная матрица ((N + 2)×(N + 2)) переходов во множестве дискретных состояний $\boldsymbol{S}$, $|\boldsymbol{S}| = N + 2$, где (N + 2)-е псевдосостояние является поглощающим;

$$f(n) = u(k_{0,1,\dots,i,\dots,I}),\ n = k_{0,1,\dots,i,\dots,I},\ N = K_{0,1,\dots,i,\dots,I},$$

$$\sum_{k_i=0}^{K_{0,1,\dots,i,\dots,I}} u(k_i) = 1,$$

где $u(k_{0,1,\ldots,i,\ldots,I})$ – плотность распределения вероятностей $k_{0,1,\ldots,i,\ldots,I}$ времени выполнения сервиса без обратной связи; $K_{0,1,\ldots,i,\ldots,I}$ – максимально возможное время выполнения сервиса без обратной связи; q – вероятность активизации обратной связи.

Нахождение $u(k_{0,1,\ldots,i,\ldots,I,(I+1)})$ плотности распределения вероятностей $k_{0,1,\ldots,i,\ldots,I,(I+1)} = 1,2,\ldots,N,\ldots$ времени выполнения сервиса с обратной связью определяется согласно соотношению:

$$u(k_{0,1,\ldots,i,\ldots,I,(I+1)}) = P_{1,N+2}^{(k_{0,1,\ldots,i\ldots,I,(I+1)})} - P_{1,N+2}^{(k_{0,1,\ldots,i\ldots,I,(I+1)^{-1})},$$

где $P_{1,N+2}^{(k_{0,1,\ldots,i\ldots,I,(I+1)})}$ – $(1,(N+2))$-й элемент $k_{0,1,\ldots,i,\ldots,I,(I+1)}$-й степени матрицы; $P_{1,N+2}^{(k_{0,1,\ldots,i\ldots,I,(I+1)^{-1})}$ – $(1,(N+2))$-й элемент $(k_{0,1,\ldots,i,\ldots,I,(I+1)}-1)$-й степени матрицы.

Сумма распределения вероятностей $u(k_{0,1,\ldots,i,\ldots,I,(I+1)})$ при матрице переходов с обратной связью стремиться к единице, от чего следует определить предел итерации контрольным пороговым отсечением δ:

$$1-\left(\sum_{k_i=1}^{k_{0,1,\ldots,I,(I+1)}}(P_{1,N+2}^{(k_i)} - P_{1,N+2}^{k_i-1})\right) \le \delta.$$

Предложенная методика формирования планов действий на языке PDDL на основе онтологии позволяет учитывать априорные знания о взаимосвязях сервисов и управлять их динамическим комплексированием, что обеспечивает наиболее оптимальный профиль качества интеграции и адаптивности в условиях сложных гетерогенных систем. Формализованный математический аппарат позволяет управлять качеством временного профиля совместной работы комплексируемых распределенных сервисов в сервис-ориентированных экосистемах, благодаря чему становится возможным осуществление интеграционного процесса субъектов рынков и отраслей в условиях перехода к цифровой экономике.

Список используемых источников

1. Птицына Л. К., Эль Сабаяр Шевченко Н. Н., Белов М. П. Моделирование сервис-ориентированных систем в условиях неопределённости // Международная конференция по мягким вычислениям и измерениям. 2018. № Секция 2. С. 291–294.

2. OWL-S: Semantic Markup for Web Services. URL: http: //www.w3.org/TR/ws-arch/ (дата обращения: 09.12.2019).

3. Peer J. A PDDL Based Tool for Automatic Web Service Composition // 2nd International Workshop on Principles and Practice of Semantic Web. Vol. 3208. 2004. PP. 149–163.

4. Птицына Л. К., Смирнов Н. Г. Программное обеспечение компьютерных сетей. Управление крупно-гранулярными процессами на основе языка BPEL : учеб. пособие. СПб. : Изд-во Политехн. ун-та, 2011. 105 с.

5. Птицына Л. К., Эль Сабаяр Шевченко Н. Динамический профиль сервис-ориентированных систем с адаптивным управлением их качеством // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 2. С. 523–528.

6. Птицына Л. К., Птицын А. В. Генерация системно-аналитического ядра безопасных информационных технологий. СПб. : Изд-во Политехн. ун-та, 2011. 264 с.

7. Кемени Д. Д., Снелл Д. Л. Конечные цепи Маркова. М. : Наука, 1970. 272 с.

УДК 004.031
ГРНТИ 20.15.05

ОБЗОР СУЩЕСТВУЮЩИХ МОДЕЛЕЙ УПРАВЛЕНИЯ РЕСУРСАМИ В РАСПРЕДЕЛЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ

Т. С. Рожкова

Академия ФСО России

В качестве объекта исследования в данной статье рассматривается распределенная вычислительная система. Проводится обзор существующих моделей управления ресурсами в распределенной вычислительной системе. Указываются их основные особенности и недостатки. Приводится модель, наиболее близкая к исследуемому объекту, и обосновывается необходимость ее модификации.

распределенные вычислительные системы, мобильные облачные вычисления, аукцион.

В наши дни применение мобильных вычислительных устройств становится все более повсеместным. Однако, их возможности ограничены вычислительными ресурсами и энергоемкостью аккумулятора. На сегодняшний день широко применяется перенаправление сложных и ресурсоемких задач в удаленные облачные сервисы. Но при возрастании количества подобных задач увеличивается задержка передачи данных в сети, а также расход энергии при их передаче на большие расстояния. В связи с этим, предлагается использование незадействованных вычислительных ресурсов мобильных устройств, находящихся в непосредственной близости, без передачи выполнения задач в удаленное облако. При этом, мобильным устройствам необходимо дополнительное поощрение для предоставления собственных вычислительных ресурсов другим устройствам.

Объектом исследования является распределенная вычислительная система, представляющая собой множество разнородных по составу мобильных устройств, разнесенных в пространстве, обладающих возможностью динамического выхода из системы или перемещения в ней, а также с децентрализованным подходом к доступности ресурсов и взаимодействию между собой, так как каждый узел играет как роль клиента, так и роль сервера, предназначенная для распределения вычислительных ресурсов. Для выбора наиболее подходящего метода поощрения и повышения результативности применения распределенных вычислительных систем необходимо их моделировать.

Целью данной работы является выбор модели управления вычислительными ресурсами в распределенной вычислительной системе.

В работах [1, 2] представлен онлайн аукцион в сенсорных сетях. В приведенных работах структура аукциона – это централизованный аукционный дом, где аукционист – это базовая станция, а сенсорные устройства – участники торгов.

Наиболее популярным способом распределения ресурсов в проанализированных работах является двойной аукцион [3, 4, 5, 6, 7, 8]. В работе [3] представлен совместимый со стимулами механизм аукциона (ICAM) с закрытыми предложениями для торговли ресурсами между покупателями и продавцами. В [4] распределение ресурсов рассматривается как проблема аукциона в экономике сети. Недостатком двойного аукциона в [5] является то, что каждая точка доступа (продавец) предоставляет услугу только для одного оператора мобильной сети (покупателю) в каждый период времени. Многоуровневая архитектура приведена в [6]. При этом для распределения ресурсов в пограничной вычислительной главный аукционист должен обладать глобальными знаниями о мобильной системе. В [7] представлены две схемы двойного аукциона с динамическим ценообразованием: двойной аукцион на основе безубыточности (BDA), в котором вычислительные ресурсы пограничных серверов назначаются статически, и, более эффективный, двойной аукцион на основе динамического ценообразования (DPDA), однако, не гарантирующий достоверность продавцов. В статье [8] предложен механизм многораундового комбинированного двойного аукциона, в котором используется платформа облачных вычислений, имеющая несколько распределенных центров геоданных, применяемая для обработки больших данных.

В работах [9, 10] представлены аукционы по второй цене, достигающие равновесия по Нэшу. Предполагая, что каждый пользователь имеет ограниченный бюджет для участия в торгах, используется стратегия равновесия Нэша [9]. В статье [10] предлагается метод, основанный на аукционе, который определяет победителя путем применения механизма теории игр. В предлагаемом методе, конечной точкой игры является точка равновесия

Нэша, где игроки больше не склонны изменять свои ставки на ресурс, и окончательная ставка также удовлетворяет функции полезности аукциониста. Особенностью метода является использование удаленных облачных сервисов.

Комбинаторный аукцион по заменяемым и дополняемым ресурсам представлен в работе [11]. В разных группах ресурсы предоставляют разные функции, и, следовательно, ресурсы дополняют друг друга при создании облачных сервисов для пользователей.

В работах [9, 10, 12] приведен аукцион, который определяет победителя путем применения механизма теории игр и проведения повторяющейся игры с неполной информацией в некооперативной среде. В [12] формулируется игра Штакельберга, которая изучает процессы принятия решений рядом независимых игроков. Данный подход не учитывает предпочтения выполнения задачи. Более того, модель в [12] рассматривает только одного покупателя мобильных ресурсов, что исключает конкуренцию между несколькими покупателями в общей модели.

Классическое распределение ресурсов, а также распределение ресурсов с учетом настроек, приведены в работе [2]. Классическая проблема выделения ресурсов применима к доменам, где задачи не могут совместно использовать ресурсы.

Модель обратного аукциона представлена в [13, 14]. В работе [13] предлагается механизм стимулирования на основе обратных аукционов mCloudAuc для проведения аукционов в реальном времени. При этом используется удаленное облако или куллеты. В подходе [14] предлагается алгоритм торговли с прогнозом, чтобы помочь брокеру пользователя использовать его способность прогнозирования для распределения ресурса сети в режиме онлайн.

Оптимальный аукцион на основе глубокого изучения распределения ресурсов с использованием нейронных сетей приведен в [15].

Планирование задач в распределенных системах обработки данных описан в [6, 16, 17]. Две главные отличительные особенности модели [17]: планирование заданий осуществляется с использованием единой для всех вычислительных устройств территориально распределенной системы абсолютных приоритетов. Вторая особенность, заключается в том, что использование абсолютных приоритетов делает затруднительным составление расписания запусков заданий.

Управление ресурсами предприятий в условиях неопределенности представлено в [18]. В данной работе предлагается развитие подхода виртуального рынка и метод ситуационного управления ресурсами, итерационно работающий от «узкого звена» по тому критерию, где наблюдаются худшие значения.

Наиболее близкой к исследуемому объекту является модель, опубликованная в [19]. В данной модели покупатель представляет свою заявку предпочитаемым продавцам, в которой указывается количество требуемых ресурсов, максимальная цена, которую он готов заплатить за единицу ресурса, и требование ко времени пребывания исполнителя задачи в системе. После получения заявок от покупателей продавец локально определяет кандидатов-победителей и сумму, требуемую для оплаты от каждого покупателя. В связи с распределенным характером, продавец может обманным путем самостоятельно выбирать цены таким образом, чтобы получить более высокое значение функции полезности. Чтобы решить эту проблему, после получения решения по аукциону, покупатели должны совместно оценить, обманывает ли их продавец. При обнаружении мошеннической активности текущий продавец удаляется из системы. Данный процесс может проводиться циклически, до достижения удовлетворяющей эффективности системы.

Описанный механизм аукциона удовлетворяет следующим свойствам. Вычислительная эффективность: разработанный механизм аукциона имеет возможность получать результаты с полиномиальной сложностью по времени. Индивидуальная рациональность: механизм аукциона гарантирует, что каждый выигравший покупатель платит не больше, чем его ставка, а каждый продавец получает не меньше минимальной запрашиваемой цены. Достоверность: механизм аукциона гарантирует, что ни один участник торгов не сможет улучшить свою собственную полезность, подав заявку, отличную от ее истинной оценки. Бюджетный баланс: нет экономических потерь для каждого раунда аукциона.

Несмотря на очевидные достоинства данной модели, ее недостатками является то, не учитывается динамический выход устройства из системы, а также децентрализованный подход к доступности ресурсов и взаимодействию между устройствами системы. В связи с чем данная модель подлежит модификации.

Список используемых источников

1. Trevathan J., Hamilton L., Read W. Allocating Sensor Network Resources Using an Auction-Based Protocol // Journal of Theoretical and Applied Electronic Commerce Research. Volume 11. Issue 2. May 2016. Page(s): 41-63. DOI: 10.4067/S0718-18762016000200005.

2. Ostwald J., Lesser V., Abdallah S. Combinatorial auctions for resource allocation in a distributed sensor network // Real-Time Systems Symposium. 2005. DOI: 10.1109/RTSS.2005.12

3. Jin A., Song W., Zhuang W. Auction-Based Resource Allocation for Sharing Cloudlets in Mobile Cloud Computing // IEEE Transactions on Emerging Topics in Computing. Volume: 6. Issue 1. Jan.-March 2018. Page(s): 45–57. DOI: 10.1109/TETC.2015.2487865.

4. Yue Y., Sun W., Liu J. Multi-Task Cross-Server Double Auction for Resource Allocation in Mobile Edge Computing // ICC 2019 – 2019 IEEE International Conference on Communications. DOI: 10.1109/ICC.2019.8761791.

5. Wang G., Yang Z., Yuan C., Liu P. Combinatorial Auction-Based Two-Stage Matching Mechanism for Mobile Data Offloading // KSII Transactions On Internet And Information Systems. Volume 11, NO. 6. June 2017. DOI: 10.3837/tiis.2017.06.001.

6. Xu J., Palanisamy B., Ludwig Y., Zenith Q. Utility-Aware Resource Allocation for Edge Computing // IEEE International Conference on Edge Computing. 2017. DOI: 10.1109/IEEE.EDGE.2017.15

7. Sun W., Liu J., Yue Y., Zhang H. Double Auction-Based Resource Allocation for Mobile Edge Computing in Industrial Internet of Things // IEEE Transactions on Industrial Informatics. Volume: 14. Issue: 10. October 2018. DOI: 10.1109/TII.2018.2855746.

8. Zhao Y., Huang Z., Liu W., Peng J., Zhang Q. A Combinatorial Double Auction Based Resource Allocation Mechanism with Multiple Rounds for Geo-distributed Data Centers // IEEE ICC SAC Cloud Communications and Networking. 2016. DOI: 10.1109/ICC.2016.7510724

9. Sun J., Modiano E., Zheng L., Wireless channel allocation using an auction algorithm // IEEE Journal on Selected Areas in Communications. Volume: 24. Issue: 5. May 2006. Page(s): 1085–1096. DOI: 10.1109/JSAC.2006.872890.

10. Nezarat A., Dastghaibifard GH. Efficient Nash Equilibrium Resource Allocation Based on Game Theory Mechanismin Cloud Computing by Using Auction // Cheng-YiXia, Tianjin University of Technology. October 2015. DOI: 10.1371/journal.pone.0138424

11. Zhang Y., Niyato D., Wang P. An auction mechanism for resource allocation in mobile cloud computing systems // Proceedings of the 8th international conference on Wireless Algorithms, Systems, and Applications. August 2013. Page(s) 76–87. DOI: 10.1007/978-3-642-39701-1_7.

12. Wang X., Chen X., Wu W., An N., Wang L. Cooperative Application Execution in Mobile Cloud Computing: A Stackelberg Game Approach // IEEE Communications Letters. Volume: 20. Issue: 5. May 2016. Page(s): 946–949. DOI: 10.1109/LCOMM.2015.2506580.

13. Zhou B., Buyya R., Srirama S. An auction-based incentive mechanism for heterogeneous mobile clouds // The Journal of Systems and Software. 152 (2019). Page(s): 151–164. DOI: 10.1016/j.jss.2019.03.003.

14. Ding L., Chang L., Wang L. Online auction-based resource scheduling in grid computing networks // International Journal of Distributed Sensor Networks. 2016. Volume 12(10). DOI: 10.1177/1550147716673930.

15. Luong N., Xiong Z., Wang P., Niyato D. Optimal Auction for Edge Computing Resource Management in Mobile Blockchain Networks: A Deep Learning Approach // IEEE International Conference on Communications. 2018. DOI: 10.1109/ICC.2018.8422743

16. Голубев И. А. Планирование задач в распределённых вычислительных системах на основе метаданных : дис. … канд. техн. наук : 05.13.11 / Голубев Иван Алексеевич. Санкт-Петербург, 2014. 135 с.

17. Баранов А. В., Тихомиров А. И. Планирование заданий в территориально распределенной системе с абсолютными приоритетами // Вычислительные технологии. 2017. Том 22. Специальный выпуск 1. URL: cyberleninka.ru/article/n/planirovanie-zadaniy-v-territorialno-raspredelennoy-sisteme-s-absolyutnymi-prioritetami.

18. Майоров И. В. Мультиагентные модели и технологии ситуационного управления ресурсами предприятий в условиях неопределенности : дис. … канд. техн. наук : 05.13.01 / Майоров Игорь Владимирович. Самара, 2017. 177 с.

19. Wang X., Sui Y., Wang J., Yuen C., Wu W. A Distributed Truthful Auction Mechanism for Task Allocation in Mobile Cloud Computing // IEEE Transactions on Services Computing. Page(s): 1–1. DOI: 10.1109/TSC.2018.2818147.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Е. В. Лебеденко.

УДК 629.7
ГРНТИ 28.19.27

К ВОПРОСУ О ПОСТРОЕНИИ СИСТЕМЫ УПРАВЛЕНИЯ БЕСПИЛОТНОЙ АВИАЦИОННОЙ СИСТЕМЫ

А. А. Саломатин, Д. В. Сенчук

Институт проблем управления им. В. А. Трапезникова РАН

В настоящей статье проведен анализ существующих подходов к построению системы управления беспилотными авиационными системами (БАС). Предложен сценарий для изучения оптимального алгоритма действий беспилотного летательного аппарата (БЛА).

беспилотные авиационные системы, ограничения эксплуатации, алгоритм взаимосвязи.

В последнее время все чаще в передовых исследованиях технической направленности в научном сообществе рассматривается тема построения эффективной системы управления автономно действующих многокомпонентных беспилотных авиационных систем (БАС), состоящих из различных по своему функциональному назначению аппаратов. Настоящее направление исследований актуально, так как одиночный беспилотный летательный аппарат (БЛА) не всегда обеспечивает успешное выполнение широкого ряда задач. Изучение данного вопроса позволит успешно и оперативно решать широкий круг проблем, в случаях ограниченного ресурса времени, сложных метеоусловиях или местах непригодных для жизни человека. По этой причине одними из первостепенных заказчиков разработки данного оборудования выступают представители силовых структур, министерства по чрезвычайным ситуациям, а также руководители предприятий с вредным производством.

Подходы к построению системы управления БАС

Проектирование системы управления БАС представляет собой сложный технологический процесс. Это обусловлено переменной численностью аппаратов в автономно действующей многокомпонентной БАС, а также динамическим и непредсказуемым характером внешней среды, в которой приходится выполнять поставленные задачи. Таким образом, по мнению исследователя, целесообразно уже на этапе разработки сценариев возможного применения БАС определять структурную организацию системы группового управления (СГУР). Рассмотрим некоторые из возможных вариантов.

Централизованная СГУР (рис. 1) отличается простотой организации и алгоритмизации группового управления, так как в данном случае вся БАС Θ, состоящая из N роботов, рассматривается как единое целое, то есть как единый объект управления со многими степенями свободы. Централизованная СГУР включает центральное устройство управления (ЦУУ) и каналы связи со всеми субъектами БАС. При этом каждый БЛА системы $R_i \in \Theta$ $(i = 1, N)$ должен постоянно передавать в ЦУУ данные о своем текущем состоянии R_i (координаты местоположения, текущее время автономной работы, остаток заряда аккумуляторной батареи), состоянии окружающего его участка внешней среды E_i, то есть информацию о вектор функции $S_i = (R_i, E_i)$.

На основе этой информации СГУР в автоматическом режиме или при задействовании оператора решает для всех БЛА задачу формирования действий A_i $(i = 1, N)$, направленных на оптимальное достижение групповой цели в текущей ситуации.

Следовательно, данный вариант построения системы управления БАС в условиях недетерминированной среды и возможных сбоях прохождения сигналов управления от ЦУУ не позволяет обеспечить максимальную вероятность успешного решения практических задач.

С целью нейтрализации выявленных при построении централизованной СГУР недостатков целесообразно рассмотреть распределенные (децентрализованные) системы группового управления роботами. Примером реализации изучаемой СГУР может служить многокомпонентная БАС состоящая из трех беспилотных летательных аппаратов. Аппараты в группе подразделяются на разведчики и грузовой, поэтому различаются между собой по своей крейсерской скорости движения ν_k, емкости аккумуляторных батарей b_k, и набору предустановленного бортового оборудования χ{y,u}, где y – полезная нагрузка робота-разведчика, а u – транспортного робота.

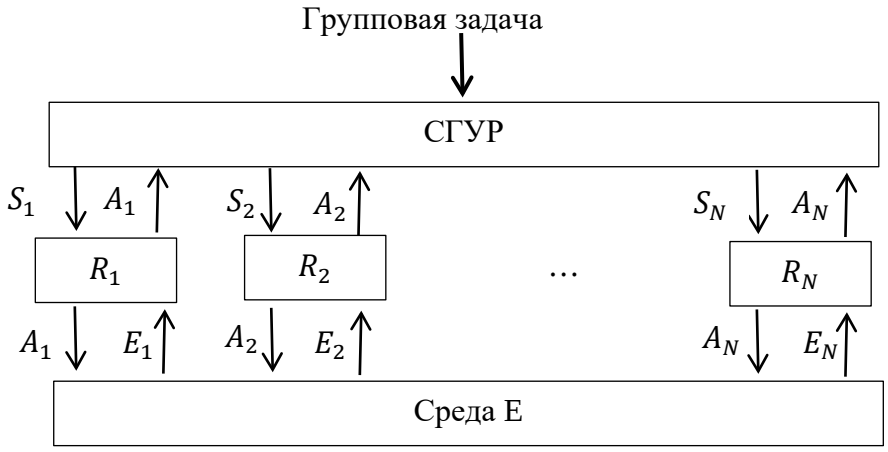


Рис. 1. Централизованная система группового управления.

В настоящей модели допускается, что все разведчики рассматриваемой БАС перемещаются к пострадавшему с увеличенной по сравнению с транспортным роботом крейсерской скоростью. Емкость аккумуляторов для наибольшей наглядности допускается измерять не в единицах энергии, а в средней длительности функционирования. В процессе полета в условиях чрезвычайных ситуаций данная группировка может столкнуться с рядом ограничений, которые могут послужить причиной выхода из строя ряда аппаратов. Задача исследователей на этапе разработки автоматического алгоритма действий БЛА проанализировать влияние данных факторов внешних воздействий и исключить возможность вывода из строя всей группировки. К таким ограничениям можно отнести: критическое повышение (понижение) температуры окружающей среды, в случае применения в условиях пожара или крайнего севера; повышение скорости порывов ветра, в случае применения при шквалистом ветре, бурях в пустыне, смерчах; повышение влажности в случае применения при возникновении обильных осадков (ливня, града). Стоит обратить внимание, что некоторые ограничения накладываются исходя из внутренних параметров БЛА, например: наличие или отсутствие тепловизионной ветви наблюдения для успешного поиска пострадавших в загазованных областях; параметры шумности аппарата, что может положительно сказываться для привлечения внимание пострадавших, о местонахождении которых неизвестно при проведении поисковых мероприятий; масса полезной нагрузки грузового аппарата; время работы в активном режиме и дальность полета; возможность возврата какой-либо полезной нагрузки к пульту оператора оперативной группы МЧС.

Среди систем с распределённым управлением можно выделить системы, реализующие стратегии коллективного либо стайного управления.

Структура децентрализованной СГУР, реализующей стратегию коллективного управления, приведена на рис. 2. Здесь каждый робот R_j группы обладает своей системой управления СУ$_j$. Эти системы объединены с помощью информационного канала связи, но каждая СУ$_j$ отвечает за выбор действий A$_j$ робота R_j в составе группы. Информация о действии A_j, выбранном СУ$_j$, сообщается всем остальным СУ$_i$ ($i = \overline{1,N}, i \neq j$), на основании чего последние могут скорректировать действия «своих» роботов R$_i$ с учетом действия робота R_j для оптимизации достижения групповой цели.

Организационная структура распределённой СГУР, реализующей стайный принцип управления предполагает, что каждый робот R$_j$ группы также имеет свою систему управления СУ$_j$ ($j = \overline{1,N}$), но в отличие от схемы на рис. 2 СУ$_j$ ($j = \overline{1,N}$) не имеют канала обмена информацией. Следовательно, в соответствии со стратегией стайного управления, координацию своих групповых действий роботы осуществляют на основании анализа реакции среды E на суммарное действие всех роботов группы.

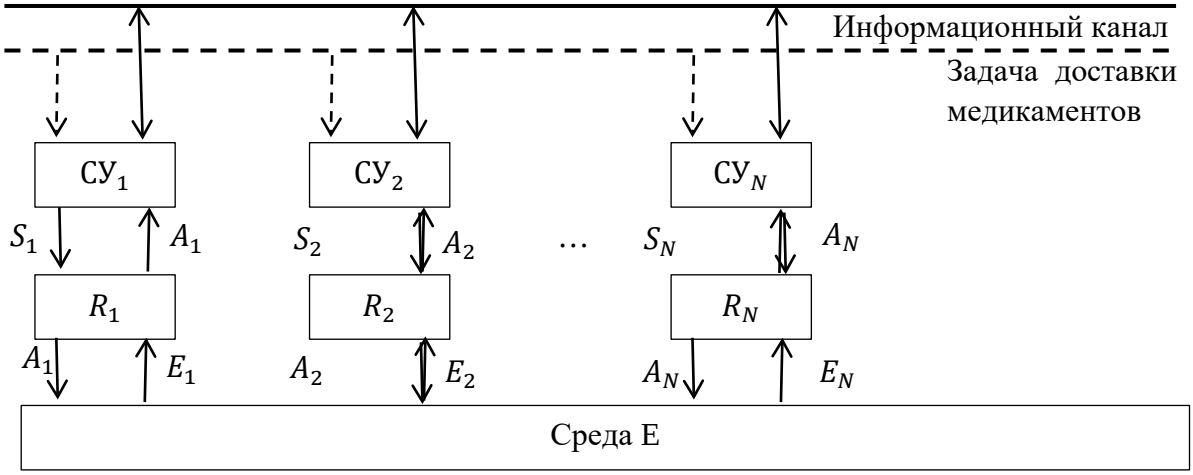


Рис. 2. Распределенная система коллективного управления роботами

Таким образом, к важным преимуществам децентрализованных СГУР можно отнести высокую надежность и живучесть, вследствие высокой вероятности приспособления к окружающей среде – изменениям ситуации в системе «беспилотная авиационная система – среда», к потере связи (выходу из строя) одного из беспилотных летательных аппаратов.

Список используемых источников

1. Каляев И. А., Гайдук А. Р., Капустян С. Г. Модели и алгоритмы коллективного управления в группах роботов. М. : Физматлит, 2009. 280 с.

2. Моисеев В. С. Групповое применение беспилотных летательных аппаратов: монография. Казань: Редакционно-издательский центр «Школа», 2017. 572 с.

3. Бутковский А. Г. Теория оптимального управления системами с распределенными параметрами. М. : Наука, 1965. 476 с.

4. Миляков Д. А. Об управлении большой группой беспилотных летательных аппаратов как системой с распределенными параметрами // Труды Десятой международной конференции (3–6 сентября 2018 г. Самара, Россия). Самара: ООО «Офорт», 2018. С. 176–181

5. Кутахов В. П., Пляскота С. И. Информационное взаимодействие в крупномасштабных робототехнических авиационных системах // Материалы Десятой международной конференции: в 2-х т. Институт проблем управления им. В. А. Трапезникова; Российская академия наук, 2017. С. 93–96

6. Кутахов В. П., Мещеряков Р. В. Принципы формирования модели оптимизации системы роботизированных авиационных средств // XIII Всероссийское совещание по проблемам управления ВСПУ-2019. Сборник трудов XIII Всероссийского совещания по проблемам управления ВСПУ-2019. Институт проблем управления им. В.А. Трапезникова РАН. 2019. С. 1211–1214.

7. Hadad, Meirav; Kraus, Sarit et al. Group planning with time constraints // Annals of mathematics and artificial intelligence. 2013, Vol. 69. PP. 243–291.

8. Tisdale J., Zuwhan K., Hendrick J. K. Autonomous UAV path planning and estimation // IEEE Robotics & Automation magazine. 2009. Vol. 16. Iss. 2. PP. 35–42.

9. Tomic T.; Schmid K.; Lutz P.; Domel A. Toward a Fully Autonomous UAV: Research Platform for Indoor and Outdoor Urban Search and Rescue // IEEE Robotics & Automation magazine. 2012. Vol. 19. Iss. 3. PP. 46–56.

10. Liu, Y., & Nejat, G. (2013). Robotic Urban Search and Rescue: A Survey from the Control Perspective // Journal of Intelligent & Robotic Systems, 72(2). PP. 147–165.

11. Macwan, A., Vilela, J., Nejat, G., & Benhabib, B. (2015). A Multirobot Path-Planning Strategy for Autonomous Wilderness Search and Rescue // IEEE Transactions on Cybernetics, 45(9). PP. 1784–1797.

12. Liu, Y., & Nejat, G. (2015). Multirobot Cooperative Learning for Semiautonomous Control in Urban Search and Rescue Applications // Journal of Field Robotics, 33(4), PP. 512–536.

13. Macwan, A., Nejat, G., & Benhabib, B. (2011). Optimal deployment of robotic teams for autonomous wilderness search and rescue // 2011 IEEE/RSJ International Conference on Intelligent Robots and Systems.

14. Niroui, F., Sprenger, B., & Nejat, G. (2017). Robot exploration in unknown cluttered environments when dealing with uncertainty // 2017 IEEE International Symposium on Robotics and Intelligent Sensors (IRIS).

15. Zhang, K., Niroui, F., Ficocelli, M., & Nejat, G. (2018). Robot Navigation of Environments with Unknown Rough Terrain Using deep Reinforcement Learning // 2018 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR).

Статья представлена научным руководителем,
доктором технических наук, профессором РАН Р. В. Мещеряковым

УДК 004.942
ГРНТИ 49.33.35

ИСКУССТВЕННАЯ НЕЙРОННАЯ СЕТЬ В ЗАДАЧЕ ОБНАРУЖЕНИЯ МНОГОВЕКТОРНОЙ DDOS-АТАКИ

К. Ф. Слесарчик

Академия ФСО России

В статье рассматривается метод обнаружения многовекторных распределенных атак на отказ в обслуживании, направленных на сетевой и прикладной уровень инфокоммуникационной сети. Рассмотрены особенности применения искусственных нейронных сетей в задаче обнаружения многовекторных DDoS-атак прикладного и сетевого уровня. Представлены результаты экспериментальных исследований характеристик вероятности ошибок идентификации состояния атаки искусственной нейронной сетью и ошибок «ложного» срабатывания.

многовекторная DDoS-атака, искусственная нейронная сеть, сетевой прикладной уровень, инфокоммуникационная сеть, деструктивное информационное кибернетическое воздействие.

Введение

Анализ статистики деструктивных информационных кибернетических воздействий (ДИКВ) за 2019 года показал, что в стремительно выросла доля атак на протоколы прикладного уровня инфокоммуникационных сетей (рис. 1).

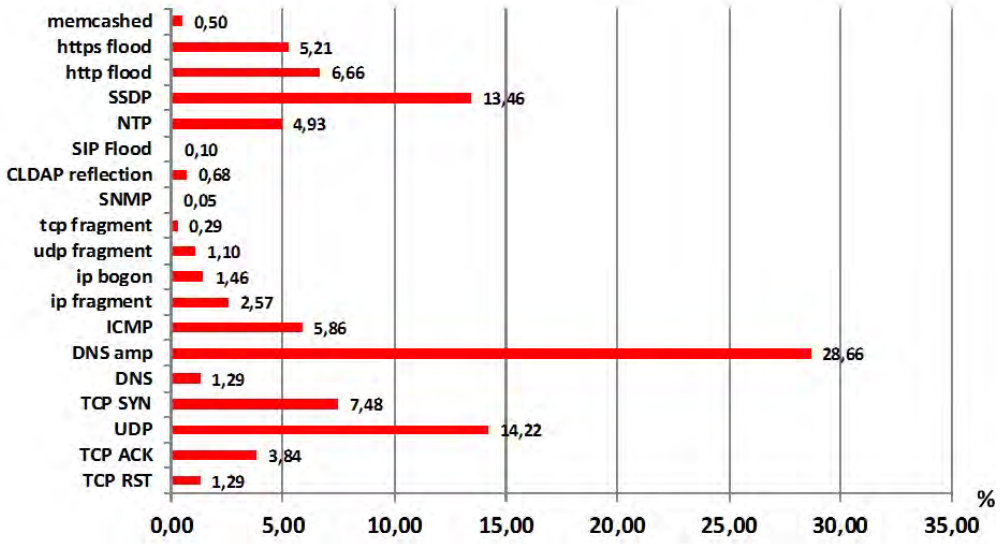


Рис. 1. Соотношение по видам DDoS-атак на протоколы инфокоммуникационных сетей в 2019 году

Структура DDoS-атак стала многовекторной, комплексное использование уязвимостей протоколов инфокоммуникационных сетей в 2019 году сформировало своеобразный тренд – атаки на протоколы сетевого уровня проводятся для маскировки атак на протоколы прикладного, что затрудняет идентификацию последних. Анализ направленности DDoS-атак показал, что в 38,12 % случаев проводились многовекторные DDoS-атаки, из них 29,46 % составили двух и трех векторные (рис. 2).

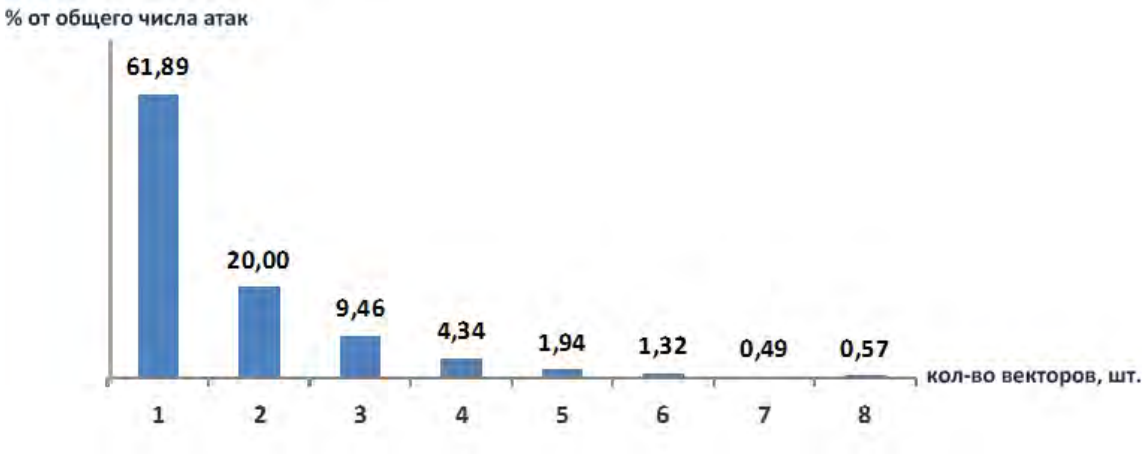


Рис. 2. Статистика DDoS-атак по количеству векторов атак в 2019 году

Наибольшее распространение получили атаки, комплексно использующие уязвимости протоколов сетевого, сеансового и прикладного уровней: UDP, ICMP, NTP, DNS и HTTP(S).

Обнаружение многовекторных DDoS-атак с помощью искусственных нейронных сетей

Наиболее часто используемые методы обнаружения и идентификации DDoS-атак представлены в [2]. Они обладают рядом недостатков, усложняющих их применение для обнаружения многовекторных DDoS-атак. Альтернативой является использование метода анализа динамики градиента характеристик трафика [3]. Задача обнаружения многовекторной DDoS-атаки формулируется следующим образом:

$$(\forall\{a_i\} \supset A)\exists \arg\max_{m_j \in M} grad\big(m_j[a_i]\big),\ i = 1..n, j = 1..k,$$

где $A\{a_i\}$ – множество векторов характеристик типов атак; m_j – вектор метрик соответствующих i типу атаки; $M\{m_j\}$ – множество векторов метрик соответствующих атаке.

Метод анализа динамики градиента характеристик трафика позволяет, используя показатели тревоги [4], идентифицировать вектора атаки посредством совокупности нейро-узлов, объединенных по выходным нейронам. На рис. 3 представлена схема устройства обнаружения многовекторной атаки вида ICMP-TCP_{flood}-$LowDDOS_{HTTP}$, на основе искусственной нейронной сети (ИНС).

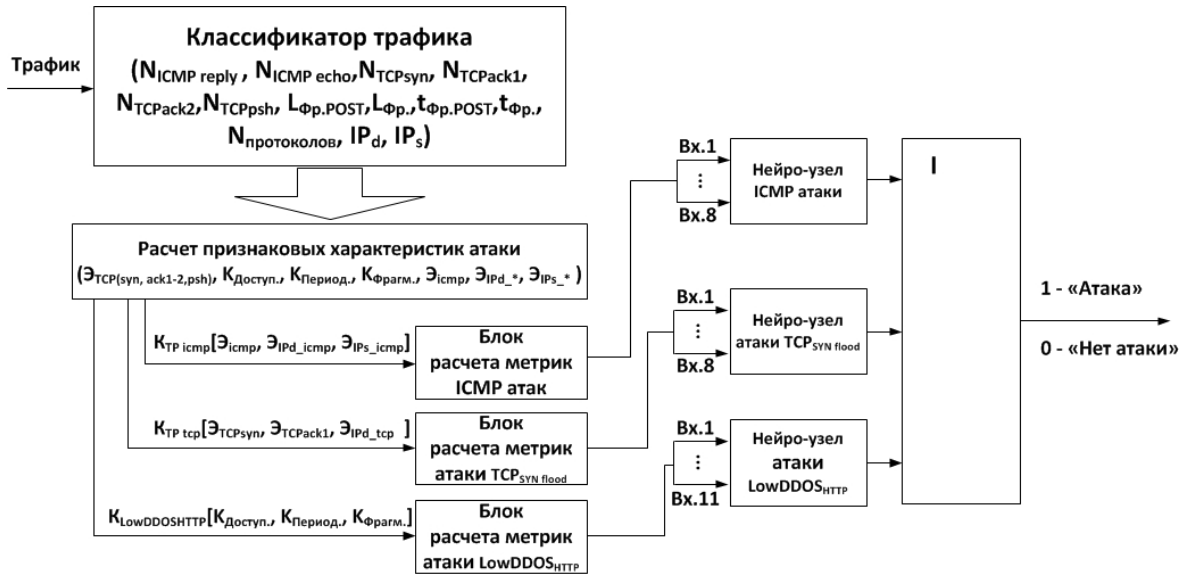


Рис. 3. Схема обнаружения многовекторной DDoS-атаки с помощью нейро-узлов

В работе [4] показаны примеры построения нейро-узлов для идентификации DDoS-атак сетевого и прикладных уровней на основе метода анализа динамики градиента показателя тревоги (рис. 4, 5). Нейро-узел для идентификации атак на протоколы сетевого представляет собой четырехслойную искусственную нейронную сеть (ИНС) по 8 нейронов в слое, с восьмью входами и двумя выходами (рис. 4). Нейро-узел используется как универсальный анализатор динамики градиента показателя тревоги одновекторной DDoS-атаки. Структура нейро-узла не требует изменения при увеличении размерности ортонормированного базиса показателя тревоги, так как изменяться будет только алгоритм вычисления значений элементов показателя тревоги.

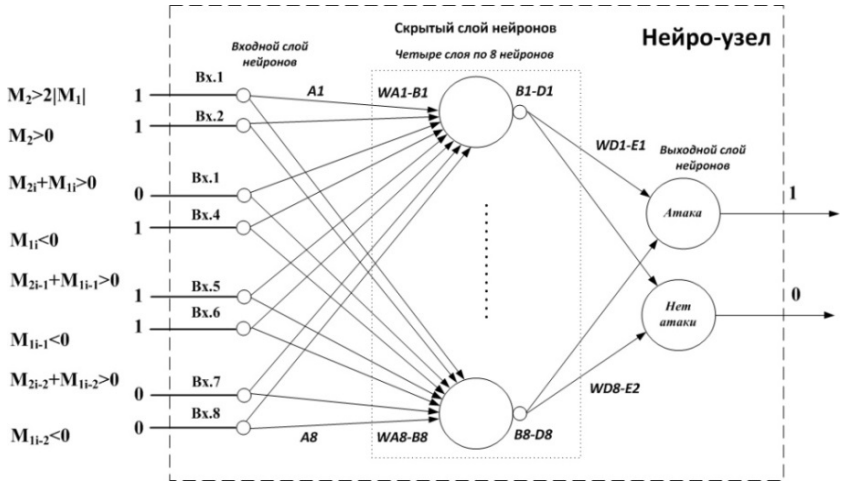


Рис. 4. Узел обнаружения DDoS-атаки
на протоколы сетевого уровня инфокоммуникационной сети

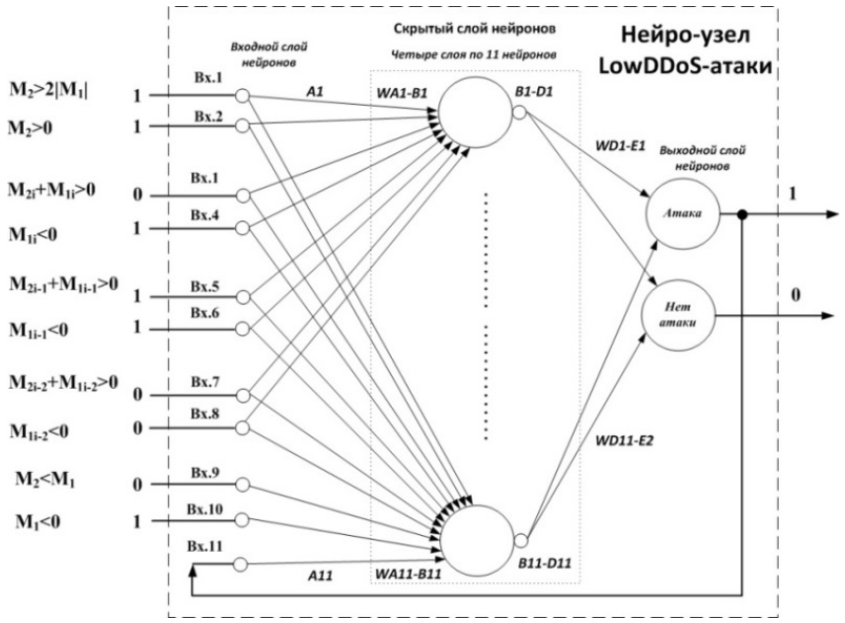


Рис. 5. Узел обнаружения низкоинтенсивной DDoS-атаки прикладного уровня
на протокол HTTP(S) инфокоммуникационной сети

Обучение ИНС осуществлялось модифицированным генетическим алгоритмом (ГА) вещественного кодирования [5]. По окончании обучения среднее значение абсолютной погрешности по всему набору обучающей выборки для узла обнаружения DDoS-атаки на протоколы сетевого уровня – $8{,}881 \cdot 10^{-16}$, а для узал обнаружения низкоинтенсивной DDoS-атаки прикладного уровня на протокол HTTP(S) инфокоммуникационной сети – $7{,}329 \cdot 10^{-15}$.

Результаты и условия экспериментальных исследований по определению значений ошибки 1 рода для предложенного метода обнаружения многовекторных DDoS-атак при различных значениях размера окна анализа представлены в [4].

В ходе экспериментов значение максимальной ошибки первого рода (ложное срабатывание) при минимальном значении окна анализа (30 пакетов): для одновекторной атаки не превысило 0,79 %; двух векторной $3{,}95 \cdot 10^{-4}$ % (рис. 6), а при максимальном значении окна анализа (15 000 пакетов) ошибка обнаружения: одновекторной атаки не превысила 0,112 %; двух векторной 0,0146 % [4].

Рис. 6. Зависимость значений ошибок первого рода от размера окна анализа

Заключение

На примере DDoS-атак сетевого и прикладного уровней показана возможность применения метода анализа динамики градиента характеристик трафика для обнаружения многовекторных атак. Перспективным направлением аппаратной реализации предложенного способа является использование ПЛИС, что позволит оставлять неизменной вычислительную ёмкость при разрастании архитектуры ИНС в случае увеличения количества нейроузлов обнаруживаемых типов DDoS-атак. Применение ПЛИС обеспечивает параллельность выполнения операций по расчету отклика ИНС, количество определяемых типов атак зависит только от объема логических элементов микросхемы.

К ограничениям предложенного способа следует отнести необходимость выбора таких признаковых характеристик атак, значения которых монотонно устремляются к нулевым значениям при появлении DDoS-

элементов в анализируемом трафике, что не всегда возможно при рассмотрении атак прикладного уровня.

Предложенный алгоритм обнаружения многовекторных распределенных атак отказа в обслуживании позволяет решить ряд проблем:

1. Эффективно выявлять принадлежность трафика к распределённой по времени многовекторной атаке с меньшим объемом анализируемых данных по сравнению со статистическими методами.

2. Реализовывать механизм обнаружения DDoS-атак на аппаратной платформе ПЛИС и интегрировать его в инфокоммуникационное оборудование.

Список используемых источников

1. DDoS Threat Landscape Report Q1-Q3 2019. [Электронный ресурс]. URL: https://www.incapsula.com/ (дата обращения: 15.01.2020).

2. Слесарчик К. Ф. Метод обнаружения низкоинтенсивных распределенных атак отказа в обслуживании со случайной динамикой характеристик фрагментации и периодичности // Вопросы кибербезопасности. 2018. № 1 (25). С. 19–27. DOI: 10.21681/2311-3456-2018-1-19-27.

3. Слесарчик К. Ф. Анализатор низкоинтенсивных DDoS-атак со случайной динамикой характеристик периодичности и фрагментации // Техника радиосвязи. 2019. № 1 (40). С. 67–81. DOI: 10.33286/2075-8693-2019-40-67-88.

4. Слесарчик К. Ф. Обнаружение многовекторных DDoS-атак сетевого и прикладного уровней // Техника радиосвязи. 2019. № 4 (43). С. 56–69. DOI 10.33286/2075-8693-2019-43-56-69.

5. Sorsa A., Peltokangas R., Real-coded genetic algorithms and nonlinear parameter identification, University of Oulu, Control Engineering Laboratory, Report A № 34, April 2008. 32 p.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Ю. Б. Ивановым/

УДК 004.414.3
ГРНТИ 20.23.19

АВТОМАТИЗИРОВАННАЯ СИСТЕМА МОНИТОРИНГА ПАРКОВОЧНОГО ПРОСТРАНСТВА

О. К. Суздальцева, В. А. Тарасов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Дана краткая характеристика актуальности существующей проблемы нехватки парковочных мест с учетом растущего количества автомобилей. Автоматизированная

система мониторинга парковочного пространства предназначена для поиска и предоставления парковочных мест для автомобилей. Система обладает программным интерфейсом для взаимодействия с другими информационными системами и является источником информации для подготовки аналитики в целях разработки политики развития парковочного пространства. Проведён обзор методов поиска парковочного места.

парковочное пространство, распознавание, нейронная сеть.

В часы пик водитель мегаполиса тратит 15–20 минут на поиск свободного парковочного места (91 час в год), а более 20 % трафика в центре городов составляют водители, которые ищут парковку. Некоторые мобильные приложения, интегрированные с датчиками геокоординат автомобиля, позволяют водителям получать информацию о свободных (и даже только освобождающихся) парковочных местах в реальном времени.

Для решения поставленной задачи были предложены различные методы. Методы на основе счетчиков, использование датчиков, которые могут быть предварительно установлены на каждом парковочном месте для индикации его состояния занятости, методы, частично основанные на компьютерном зрении. Все они либо недостаточно надежны, либо имеют высокую стоимость и требование постоянного обслуживания. Методы, основанные на компьютерном зрении, являются оптимальным выбором, так как такие системы используют камеры видеонаблюдения, установленные на парковках, и не требуют постоянного наблюдения со стороны человека. Тем не менее, текущая проблема представляет собой сложную задачу по компьютерному зрению из-за изменения освещения, искажений перспективы и различных точек обзора камеры. Чтобы преодолеть эти препятствия, исследователи обращаются к алгоритмам глубокого обучения. Особенно эффективны в задачах компьютерного зрения свёрточные нейронные сети [1, 2, 3].

Распознавание машин на кадре видео является классической задачей распознавания объектов. Существует множество подходов на основе машинного обучения, которые возможно использовать для распознавания.

Вот некоторые из них в порядке от «старой школы» к «новой школе».

Можно обучить детектор на основе HOG (*Histogram of Oriented Gradients*, гистограммы направленных градиентов) и пройтись им по всему изображению, чтобы найти все машины. Этот старый подход, не использующий глубокое обучение, работает относительно быстро, но не очень хорошо справляется с машинами, расположенными по-разному.

Можно обучить детектор на основе CNN (*Convolutional Neural Network,* свёрточная нейронная сеть) и пройтись им по всему изображению, пока не будут найдены все машины. Этот подход работает точно, но не так эффективно, так как нужно просканировать изображение несколько раз с помощью CNN, чтобы найти все машины.

Можно использовать новый подход с глубоким обучением вроде Mask R-CNN, Faster R-CNN или Yolo, который совмещает в себе точность CNN и набор технических хитростей, сильно повышающих скорость распознавания. Такие модели будут работать относительно быстро (на GPU), если есть много данных для обучения модели.

Архитектура, которая будет использоваться, предложена Джозефом Редмоном и называется Yolo. Yolo – это современная система обнаружения объектов. Самое большое преимущество перед другими популярными архитектурами – это скорость. Модели семейства Yolo быстры, гораздо быстрее, чем R-CNN и другие. Это означает, что можно достичь обнаружения объекта в реальном времени.

Yolo переформулировал задачу обнаружения объекта в единую задачу регрессии. Он идет непосредственно от пикселов изображения вплоть до координат ограничительной рамки и вероятностей классов. Следовательно, одна свёрточная сеть предсказывает несколько граничных областей и вероятности классов для этих областей.

Поскольку Yolo работает только с одним взглядом на изображение, раздвижные окна – это неправильный подход. Вместо этого все изображение можно разделить на сетку. Эта сетка будет иметь размеры $S \times S$. Теперь каждая клетка отвечает за предсказание нескольких различных вещей.

Во-первых, каждая ячейка отвечает за предсказание некоторого количества ограничивающих прямоугольников. Кроме того, каждая ячейка будет предсказывать доверительную вероятность для каждого ограничивающего прямоугольника. Другими словами, это вероятность того, что прямоугольник содержит объект. В случае отсутствия объекта в какой-либо ячейке сетки важно, чтобы значение вероятности было очень малым для этой ячейки.

Когда визуализируются все эти прогнозы, то получается карта всех объектов и массив прямоугольников, которые ранжируются по их доверительному значению (рис. 1, см. ниже).

Во-вторых, каждая ячейка отвечает за предсказание вероятностей классов. Это не означает, что какая-то ячейка сетки содержит какой-либо объект, это просто вероятность. Если ячейка сетки предсказывает автомобиль, это не значит, что есть автомобиль, это значит, что если есть объект, то этот объект – автомобиль.

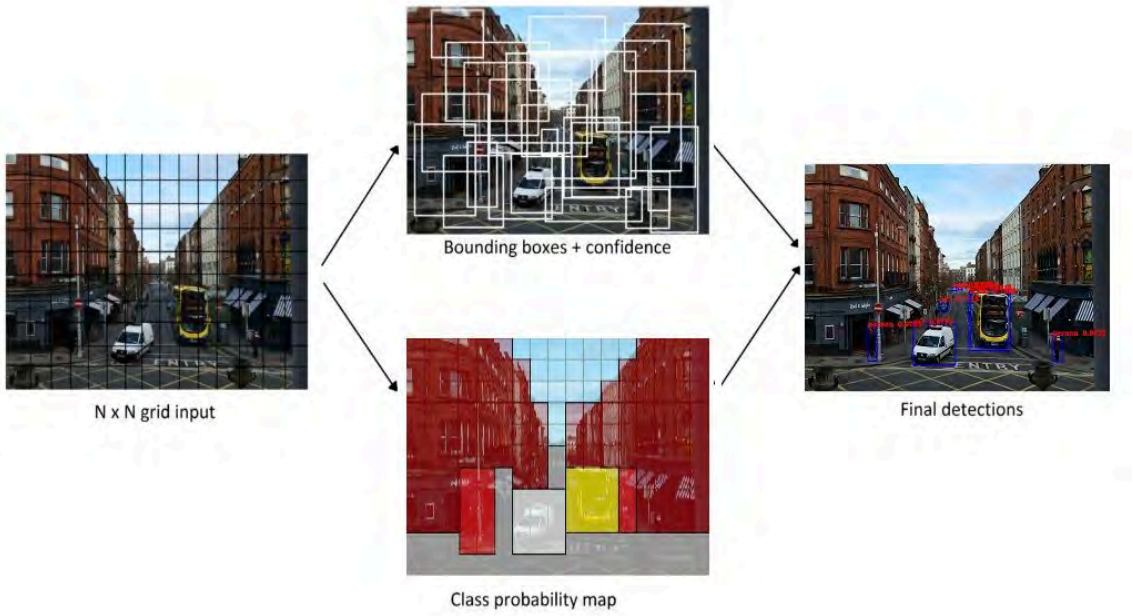


Рис. 1. Процедура Yolo-распознавания объектов

В Yolo закреплённые прямоугольники используются для прогнозирования граничных областей (рис. 2, см. ниже). Основная идея закреплённых прямоугольников заключается в предопределении двух различных форм. Таким образом, можно связать два прогноза с двумя закреплёнными прямоугольниками. Есть возможность использовать больше закреплённых прямоугольников (5 и более).

Есть сетка, и каждая ячейка будет предсказывать:

1. Для каждого закреплённого прямоугольника:
   – 4 координаты (t_x, t_y, t_w, t_h);
   – 1 ошибку, она является показателем вероятности наличия объекта.
2. Некоторое число вероятностей классов.

Если есть некоторое смещение от верхнего левого угла на c_x, c_y, тогда предсказания будут выглядеть следующим образом:

$$b_x = \sigma(t_x) + c_x;$$
$$b_y = \sigma(t_y) + c_y;$$
$$b_w = p_w e^{tw};$$
$$b_h = p_h e^{th},$$

где p_w и p_h соответствуют ширине и высоте ограничивающего прямоугольника соответственно.

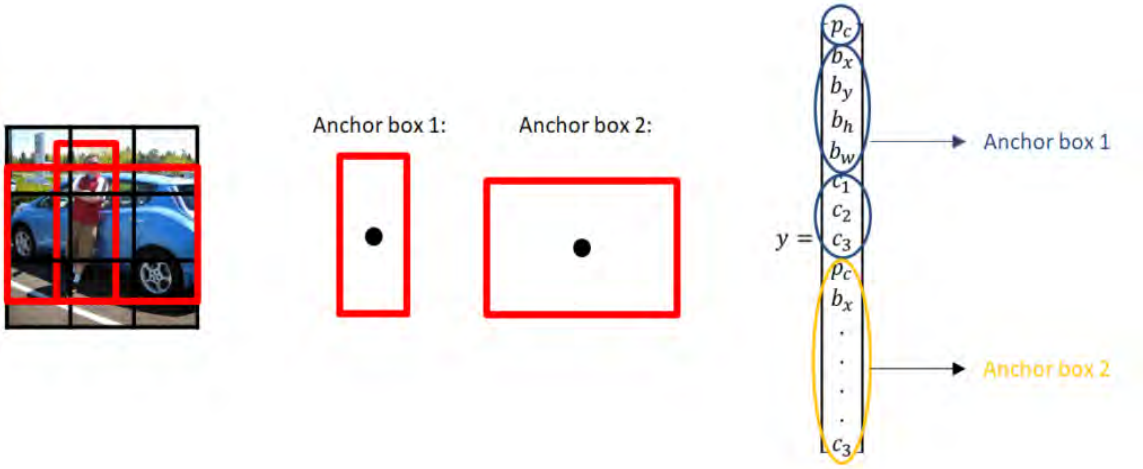


Рис. 2. Закреплённые прямоугольники

Этот выход, это выход данной нейронной сети. В общей сложности, есть $S \times S \times [B*(4+1+C)]$ выходов, где B является количеством граничных полей, предсказанных каждой ячейкой, C – количество классов, 4 для закреплённого прямоугольника и 1 – прогнозирование объектности. За один проход можно перейти от входного изображения к выходному тензору, который соответствует обнаружениям для изображения. Также стоит отметить, что Yolo v3 предсказывает прямоугольники в 3 разных масштабах.

Если вероятности умножить на доверительные значения, получатся все ограничительные прямоугольники, взвешенные по их вероятностям на предмет содержания объекта.

Простое пороговое значение позволит избавиться от всех прогнозов с низким значением вероятности. Для следующего шага важно определить, что такое Intersection Over Union (IoU). Пересечение над объединением вычисляет размер пересечения и делит его на размер объединения (рис. 3).

После этого дубликаты всё ещё могут присутствовать, и чтобы избавиться от них, применяется не максимальное пересечение. Не максимальное пересечение будет принимать ограниченный прямоугольник с наибольшей вероятностью, а затем будет рассмотрена другая ограничивающая рамка, которая близка к первой, и рамки с наибольшим перекрытием с этим (самый высокий IoU) будут пересекаться (рис. 4).

Поскольку всё делается всего за один проход, это почти так же быстро, как классификация. Кроме того, все обнаружения предсказываются одновременно, что означает, что модель неявно включает глобальный контекст. То есть можно узнать, какие объекты, как правило, возникают вместе, относительный размер и расположение объектов и так далее.

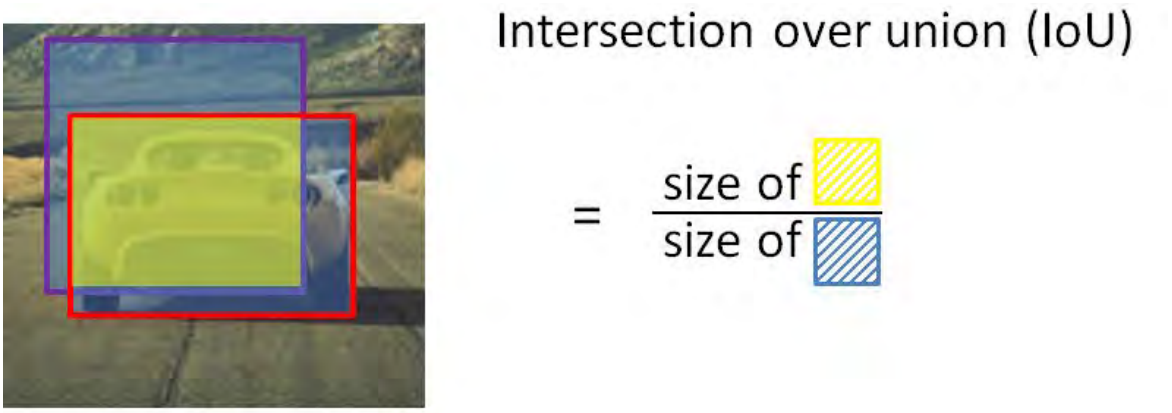


Рис. 3. Intersection Over Union (IoU)

	Type	Filters	Size	Output
	Convolutional	32	3 × 3	256 × 256
	Convolutional	64	3 × 3 / 2	128 × 128
1×	Convolutional	32	1 × 1	
	Convolutional	64	3 × 3	
	Residual			128 × 128
	Convolutional	128	3 × 3 / 2	64 × 64
2×	Convolutional	64	1 × 1	
	Convolutional	128	3 × 3	
	Residual			64 × 64
	Convolutional	256	3 × 3 / 2	32 × 32
8×	Convolutional	128	1 × 1	
	Convolutional	256	3 × 3	
	Residual			32 × 32
	Convolutional	512	3 × 3 / 2	16 × 16
8×	Convolutional	256	1 × 1	
	Convolutional	512	3 × 3	
	Residual			16 × 16
	Convolutional	1024	3 × 3 / 2	8 × 8
4×	Convolutional	512	1 × 1	
	Convolutional	1024	3 × 3	
	Residual			8 × 8
	Avgpool		Global	
	Connected		1000	
	Softmax			

Рис. 4. Yolo v3

Список используемых источников

1. TF YOLO V3 Object Detection in TensorFlow 2.0. [Электронный ресурс]. URL: http://datahacker.rs/tensorflow2-0-yolov3/ (дата обращения: 21.03.2020).

2. Amato G. et al. Deep learning for decentralized parking lot occupancy detection // Expert Systems with Applications. 2017. Vol. 72. PP. 327–334.

3. Зотов С. С., Яковлев А. А., Колчинцев Д. А. Обнаружение объектов в реальном времени с помощью алгоритмов распознавания YOLO // Синергия наук. 2018. № 26. С. 388–404. URL: http://synergy-journal.ru/archive/article2852 (дата обращения: 23.03.2020).

Статья представлена заведующим кафедрой ИУС СПбГУТ, доктором технических наук, профессором Л. К. Птицыной/

УДК 004.415.25
ГРНТИ 50.41.25

ФОРМИРОВАНИЕ ОДНОСТРАНИЧНЫХ ПРИЛОЖЕНИЙ В РЕАКТИВНОМ СТИЛЕ С ИСПОЛЬЗОВАНИЕМ БИБЛИОТЕКИ «VUE.JS»

В. А. Тарасов, Е. А. Фурасьев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются особенности разработки программного обеспечения на основе библиотеки «Vue.js» – прогрессивного JavaScript-фреймворка для создания пользовательского интерфейса и сверхбыстрых, мощных, полностью адаптивных одностраничных Web-приложений (Single Page Application). Благодаря поэтапно наращиваемой системе компонентов библиотека легко интегрируется с другими проектами и библиотеками. Описываются аспекты реализации программной архитектуры.

SPA, JavaScipt, Vue, реактивное программирование, фреймворк.

На сегодняшний день существует два принципиальных подхода к созданию Web-приложений: традиционные Web-приложения, большая часть логики которых выполняется на сервере, а также одностраничные приложения, логика пользовательского интерфейса которых выполняется преимущественно в Web-браузере, а взаимодействие с Web-сервером осуществляется главным образом через Web-API, которыми одна компьютерная программа может взаимодействовать с другой программой. Возможен гибридный подход, при котором в простейшем случае в рамках крупного традиционного Web-приложения размещаются одно или несколько полнофункциональных подчиненных приложений, построенных на основе одностраничной модели. Для работы с платформой одностраничных приложений требуется гораздо больший опыт в построении архитектуры и обеспечении безопасности. Они характеризуются большей частотой обновления и появления новых платформ по сравнению с традиционными Web-приложениями. Кроме того, по сравнению с традиционными Web-приложениями при работе с одностраничными приложениями может усложняться настройка процессов автоматизированного построения и развертывания, а также использование таких вариантов развертывания как контейнеры – технология упаковки и запуска приложений Windows и Linux в различных локальных средах и в облаке. Они предоставляют нетребовательную к ресурсам изолированную среду, которая упрощает разработку, развертывание и управление приложениями. Контейнеры быстро запускаются и останавливаются, что делает их идеальными для приложений, которые нужно быстро

адаптировать в условиях изменяющегося спроса. Упрощенная природа контейнеров также делает их полезным инструментом для повышения плотности и использования инфраструктуры. Эти моменты необходимо учитывать, оценивая улучшения взаимодействия с пользователем, которые могут дать одностраничные приложения.

Необходимо рассмотреть особенности библиотеки Vue.js и разработать одностраничное приложение (SPA) её использованием [1, 2, 3]. Она используется для создания пользовательских интерфейсов и содержит некоторые из лучших концепций React и Angular, но, по сравнению с ними, более доступна. Библиотека не уступает этим фреймворкам в мощности и предоставляет все необходимые функции для создания современных фронтенд-приложений. SPA-приложения очень специфичны, и перед разработкой необходимо проанализировать требования к приложению. Такие приложения могут поддерживать функции на стороне клиента, которые не требуют перезагрузки страницы при выполнении пользователем действий или навигации по различным разделам приложения. Преимущество такого решения заключается в том, что они быстрее загружаются, осуществляя выборку данных в фоновом режиме. Поскольку полная перезагрузка страницы выполняется редко, скорость реагирования на действия пользователя возрастает. Одностраничные приложения поддерживают добавочные обновления, обеспечивая сохранение частично заполненных форм или документов и не требуя при этом от пользователя нажимать кнопку для отправки формы, реализуют полнофункциональное поведение на стороне клиента, в том числе возможности перетаскивания и вставки, что гораздо проще по сравнению с традиционными Web-приложениями. Также они могут быть настроены для работы при отсутствии подключения, позволяя обновлять модель на стороне клиента и впоследствии синхронизировать её с сервером при восстановлении подключения. Одностраничные приложения следует выбирать в тех случаях, когда в приложении требуется реализовать расширенные функции помимо стандартных возможностей HTML-форм.

В приложениях часто требуется реализовать возможности, встроенные в традиционные Web-приложения, например, отображать в адресной строке URL-адрес, отражающий текущую операцию (благодаря чему пользователь может добавлять такой URL-адрес в закладки или задавать прямую ссылку для последующего возврата к нему). Пользователи одностраничных приложений также должны иметь возможность использовать кнопки «Назад» и «Вперед» браузера с предсказуемыми результатами. Если использование Web-API другими клиентами уже поддерживается, может быть проще создать реализацию одностраничного приложения, которое использует эти API вместо воспроизведения логики на стороне сервера. Одностраничные приложения позволяют активно использовать Web-API для запроса и обновления данных во время работы пользователя с приложением.

Однако стоит упомянуть и недостатки разработки таких приложений. На стороне клиента к приложению применяются минимальные требования, например, используются только функции чтения.

Большинство пользователей многих Web-приложений могут работать только с функциями чтения.

Приложения, предназначенные исключительно или преимущественно для чтения, обычно гораздо проще тех, в которых реализуется управление состояниями. Например, в поисковой системе вполне достаточно реализовать одну точку входа с текстовым полем и вторую страницу для отображения результатов поиска. Запросы могут выполнять анонимные пользователи, в связи с чем, на стороне клиента практически не требуется реализовывать логику. Аналогичным образом публичные приложения блогов или систем управления содержимым работают преимущественно с содержимым и практически не имеют функций, реализуемых на стороне клиента. Такие приложения легко создавать в формате традиционных серверных Web-приложений, которые выполняют логику на Web-сервере и преобразовывают HTML-код для отображения в браузере. Тот факт, что каждая уникальная страница сайта имеет собственный URL-адрес, который может добавляться в закладки или индексироваться поисковыми системами (такое поведение реализуется по умолчанию и не требует добавления в приложение отдельной функции), также является очевидным преимуществом такого сценария.

Приложение должно работать в браузерах без поддержки JavaScript.

Web-приложения, которые должны работать в браузерах с отсутствующей или ограниченной поддержкой JavaScript, следует создавать с применением рабочих процессов традиционных Web-приложений (или, как минимум, реализовать возможность переключения на такое поведение). Для работы одностраничного приложения требуется реализация JavaScript на стороне клиента, и, если такой возможности нет, выбирать эту модель не рекомендуется.

После анализа и выбора разработки SPA-приложения, прежде чем приступать, необходимо установить Node.js. Node.js – это среда выполнения JavaScript, которая выполняет код JS без браузера. Однако Vue.js может быть как библиотекой, так и полноценным фреймворком для разработки реактивных приложений. Реактивное программирование – это парадигма программирования с асинхронными потоками данных. Иными словами, реактивность – это способность реагировать на какие-либо изменения.

Необходимо установить Vue.js как библиотеку. Подключение в HTML-файле представлено на рис. 1.

```
<!-- версия для разработки, отображает полезные предупреждения в консоли -->
<script src="https://cdn.jsdelivr.net/npm/vue/dist/vue.js"></script>
```

Рис. 1. Подключение библиотеки Vue.js

В ядре Vue.js находится система, которая позволяет декларативно отображать данные в DOM с помощью простых шаблонов (рис. 2).

```
<div id="app">
  {{ message }}
</div>
```

```
var app = new Vue({
  el: '#app',
  data: {
    message: 'Привет, Vue!'
  }
})
```

Рис. 2. Простое приложение «Hello World» на Vue.js

Каждое приложение начинается с создания нового экземпляра Vue с помощью функции Vue (рис. 3).

```
var vm = new Vue({
  // опции
})
```

Рис. 3. Создание экземпляра Vue

Когда экземпляр Vue создан, он добавляет все свойства, найденные в опции data, в систему реактивности Vue. Поэтому представление будет «реагировать» на их изменения, обновляясь в соответствии с новыми значениями. У каждого компонента есть свой жизненный цикл, за ходом которого можно наблюдать и использовать в своих нуждах при разработки приложения.

Одна из наиболее примечательных возможностей Vue – это ненавязчивая реактивность. Модели представляют собой простые JavaScript-объекты. По мере их изменения обновляется и представление данных, благодаря чему управление состоянием приложения становится простым и очевидным. Когда простой JavaScript-объект передаётся в экземпляр Vue в качестве опции data, Vue обходит все его поля и превращает их в пары геттер/сеттер, используя Object.defineProperty. Эта возможность появилась в JavaScript только начиная с версии ES5, и в более ранних версиях её эмулировать не получится – по этой-то причине Vue и не поддерживает IE8 и ниже (рис. 4).

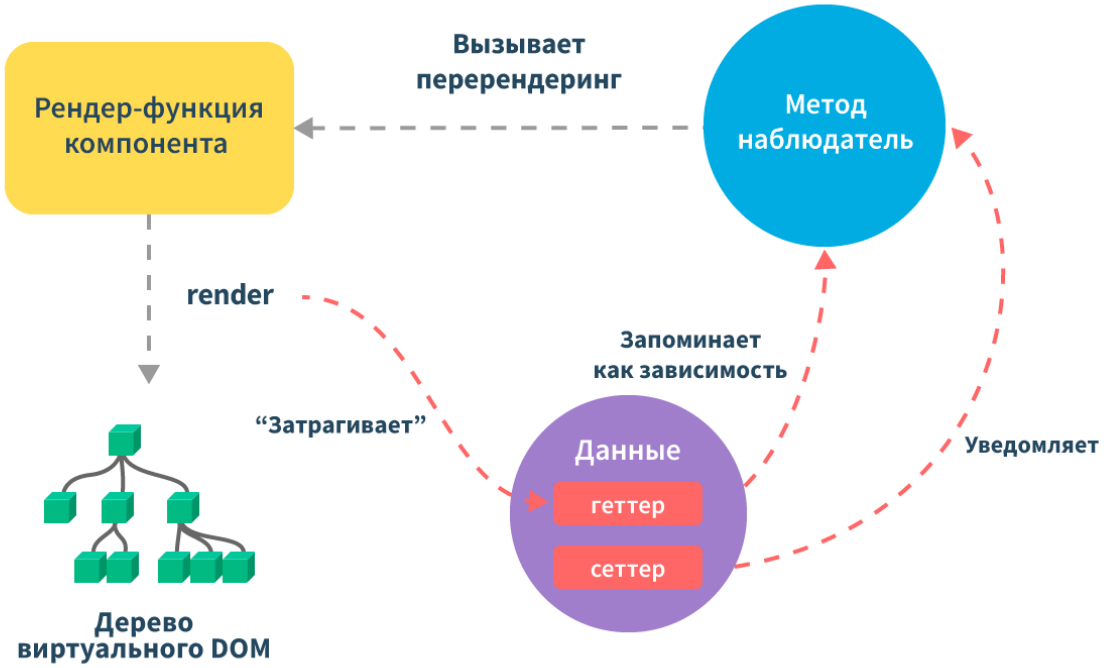


Рис. 4. Этапы работы реактивности во Vue.js

Используя такую парадигму как реактивное программирование и библиотеку Vue.js при актуальности её использования в разрабатываемом приложении и знании устройства её среды, можно разработать комплексное одностраничное приложение, которое будет реагировать и отображать изменения данных без перезагрузки браузера.

Список используемых источников

1. Хэнчетт Э., Листоун Б. Vue.js в действии, СПб. : Питер, 2019. 304 с. ISBN: 978-5-4461-1098-8.

2. The Progressive JavaScript Framework. [Электронный ресурс]. URL: https://vuejs.org/ (дата обращения: 20.03.2020).

3. Getting Started with VueJS [Электронный ресурс]. URL: https://medium.com/js-dojo/getting-started-with-vuejs-for-web-and-native-285dc64f0f0d (дата обращения: 20.03.2020).

Статья представлена заведующим кафедрой ИУС СПбГУТ, доктором технических наук, профессором Л. К. Птицыной/

УДК 004.418
ГРНТИ 20.51.19

АВТОМАТИЗАЦИЯ ВЗАИМОДЕЙСТВИЯ С ЗАКАЗЧИКОМ СТУДИИ ДИЗАЙНА ИНТЕРЬЕРОВ

В. А. Тарасов, П. М. Шаповалов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Приведено обоснование необходимости разработки автоматизированной системы управления бизнес-процессами. Рассмотрены преимущества использования средств автоматизации взаимодействия с заказчиками посредством применения корпоративного Web-ресурса. Представлены требования к составу программной структуры системы и её функционалу. Приведены сложившиеся к настоящему времени концепции Web-проектирования применительно к решению прикладных задач.

автоматизация, бизнес-процесс, Frontend, Backend.

Темпы технического прогресса требуют современных инструментов, эффективных коммуникаций, постоянного обновления информации, стратегий и методологий. Скорость связи, предлагаемая Интернетом, и неограниченный доступ ко всем компьютерам, подключенным к сети, делают его идеальным средством для удовлетворения этих потребностей. Интернет дает возможность всегда быть доступным в любом месте и в любое время [1]. Интернет сегодня предоставляет частным лицам, правительствам, некоммерческим организациям и предприятиям возможность охватить миллиарды людей. Web-ресурсы, связанные группы Web-страниц, являются наиболее широко используемым средством охвата аудитории в Интернете. В определенных правовых рамках владельцы Web-сайтов могут публиковать на сайте практически любую информацию.

Наличие автоматизированной системы взаимодействия с заказчиком, открытой в сеть Интернет посредством Web-ресурса, дает организации целый набор преимуществ, в числе которых, следующие.

Доступность круглые сутки для клиентов. Наличие такой системы означает, что клиенты всегда могут завести или утвердить заявку, оставить комментарий, в любое время и в любом месте. Даже в нерабочее время система продолжает работать. Она предлагает пользователям удобство, поскольку они могут получить доступ к информации, которая им нужна, не выходя из собственного дома. Кроме того, поскольку в настоящее время большинство дизайнерский студий уже имеют свой собственный Web-сайт, есть шансы, что такая автоматизированная система может выгодно выделяться на фоне конкурентов, использующих статичные Web-ресурсы.

Эффективный обмен информацией. Web-сервис обеспечивает быстрый и простой способ передачи информации между компанией и клиентами. Можно оперативно информировать клиентов студии об изменениях в их заказах, предоставить выполненную работу на утверждение, показать примеры выполненных работ, а также вести анкетирование и обратную связь.

Расширение охвата аудитории. Поскольку такая система доступна для всех пользователей Интернета, есть возможность преодолеть географические барьеры. Исполнителю нет необходимости находиться в одном регионе с заказчиком. Клиент может получить готовый качественный дизайн-проект, находясь в нескольких тысячах километрах от дизайнера.

Подключение аналитических инструментов. Аналитические инструменты позволяют определить вкус клиента, его гаммовые предпочтения, предложить типовые виды планировок и сочетаний цветов.

Возможность роста функционала ресурса. По мере необходимости можно легко добавлять новые информационные блоки и дополнительные функциональные возможности.

Предлагается рассмотреть набор функциональных требований к реализации данной автоматизированной системы и некоторые особенности её реализации.

Разрабатываемая автоматизированная система на базе Web-ресурса должна обладать следующими особенностями.

Круглосуточной доступностью из любой точки мира, где есть доступ к сети Интернет.

Отказоустойчивостью. Ресурс должен обеспечивать возможность одновременной обработки заявок от множества заказчиков и их взаимодействия с дизайнерами.

Расширяемостью. Ресурс должен иметь возможность гибкого и малозатратного функционального расширения, добавления дополнительных модулей.

Удобным, информативным, не перегруженным интерфейсом, не отталкивающим клиента, а наоборот, привлекающим его своей простотой и функциональностью.

Ресурс должен содержать следующие функциональные блоки.

Статичная информационная страница (главная страница ресурса, содержащая информацию о студии, сотрудниках, контактные данные, примеры работ, примерные расценки).

Блок оформления заявки с формой анкетирования для сбора первоначальной информации о заказчике и объекте, для которого будет создаваться дизайн-проект.

Блок формирования стоимости работ на основе заявки и анкеты.

Блок взаимодействия заказчика и исполнителя, содержащий функциональные возможности для дизайнера предоставлять промежуточные результаты работы, а для клиента их оценивать и утверждать или отправлять на доработку в соответствии с оставленными комментариями.

Блок утверждения готовой работы со стороны дизайнера и со стороны заказчика.

Финансовый блок, через который осуществляется предоплата перед началом работ и итоговая оплата после утверждения.

Разрабатываемая автоматизированная система должна иметь следующие возможности для администратора системы.

Добавлять и удалять информационные страницы в существующей структуре ресурса.

Добавлять на страницы текстовую информацию.

Добавлять на страницы графическую информацию.

Обеспечить возможность добавления, изменения и удаления со страниц ресурса форм и функциональных блоков.

Обеспечить удобный и наглядный интерфейс администратора, который не имеет навыков работы с базами данных и навыков верстки.

Обеспечить надежное хранение информации.

Обеспечить защиту от несанкционированного доступа.

Контролировать избыточность, непротиворечивость, сохранность и достоверность хранимой в базе данных информации.

Для создания автоматизированной системы на базе Web-ресурса предполагается использовать архитектуру «Клиент-сервер», при которой ресурс хранится на некотором сервере (локально или с использованием хостинга) и доступен по IP-адресу, получаемому из URL посредством системы доменных имен DNS. Множество клиентов могут подключаться к серверу и обмениваться с ним информацией, посылая HTTP-запросы и получая на них ответы (рис. 1).

На стороне сервера происходит формирование HTML-страниц посредством обращений к базе данных, а на стороне клиента – непосредственно взаимодействие системы с пользователем.

Поскольку Web-разработка претерпела существенные изменения, то в настоящее время принято выделять такие области разработки Web-ресурсов как Фронтэнд (*Frontend*) и Бэкэнд (*Backend*) [2].

Frontend и Backend – это два самых популярных термина, используемых в Web-индустрии, но разница между ними довольно существенная. Это две фундаментальные части разработки программного обеспечения, которые играют важную роль в Web-разработке.

Внешний интерфейс может ссылаться на графический интерфейс пользователя, тогда как внутренний интерфейс – это та часть Web-ресурса, которую пользователь не может видеть или с которой не может взаимодействовать.

Рис. 1. Клиент-серверная архитектура

Web-интерфейс – часть Web-ресурса, с которой пользователь может напрямую взаимодействовать, чтобы получить бэкэнд-возможности системы. Он включает в себя все, что пользователь может увидеть и испытать.

Frontend – это все дизайнерские и оформительские решения, которые пользователь видит на Web-ресурсе, такие как графический пользовательский интерфейс, включая яркие кнопки, красочные изображения, навигационные меню и т. д. Frontend также называют «клиентской», поскольку действие происходит на стороне информационного обмена, которая в этом случае является пользовательской. Как правило, клиент относится к компьютерному приложению, такому как Web-браузер, который его просматривает.

Frontend – это в основном Web-браузер, и всё, что пользователь видит и с чем взаимодействует на Web-ресурсе, является частью разработки Web-интерфейса.

Следует отметить, что Web-дизайнер не имеет дел с кодом, а отвечает за все аспекты создания и перепроектирования Web-ресурсов, которые будут содержать как визуально привлекательные элементы, так и удобный дизайн. Роль разработчика Web-интерфейса заключается в создании среды, которую пользователь может видеть и изменять с помощью комбинации нескольких инструментов, включая HTML, CSS и JavaScript [3].

Бэкэнд представляет собой серверную часть, также называемую «серверной стороной», является частью Web-сайта, с которой пользователь не может взаимодействовать напрямую. Всё, что происходит за пределами

форм пользовательского интерфейса, можно отнести к серверной Web-разработке.

Это часть системы, которая не вступает в прямой контакт с пользователями. В отличие от внешнего интерфейса, он работает на стороне сервера, но взаимодействует с внешним интерфейсом, чтобы гарантировать, что система предоставляет нужный пользователю функционал. В каждом приложении есть значительная часть кода не пользовательского интерфейса, который имеет дело со всеми сложными системами, которые работают в фоновом режиме.

Бэкэнд-разработчики обрабатывают всё, что не связано с созданием пользовательского интерфейса, например, написание API, создание библиотек или добавление утилит ко всему, что создает Web-дизайнер. Они облегчают связь между уровнем представления и уровнем бизнес-логики. Они играют решающую роль в Web-разработке, и их роль тесно связана с Web-дизайнерами. Бэкэнд-Web-разработка – это сочетание разработки и поддержки основной функциональной логики программного приложения. Связь бэкэнда и фронтэнда представлена на рис. 2.

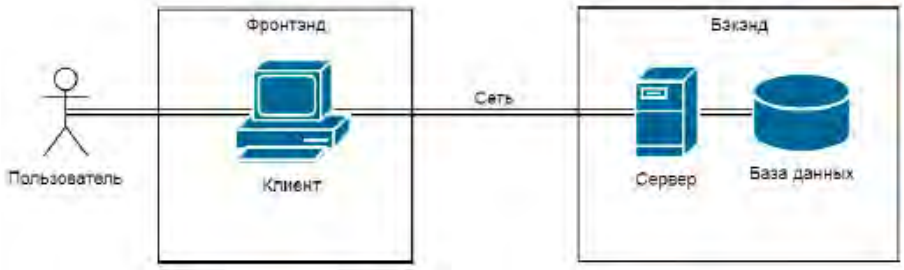


Рис. 2. Связь бэкэнда и фронтэнда

Таким образом, чтобы обеспечить студию дизайна интерьеров конкурентным преимуществом, необходимо создать автоматизированную систему взаимодействия с заказчиком и привлечь к ее разработке Web-разработчика для формирования бэкэнд-логики, Web-дизайнера для формирования фронтенд-логики и подготовить серверную часть для формирования клиент-серверной архитектуры.

Список используемых источников

1. Макконнелл С. Профессиональная разработка программного обеспечения : пер. с англ. СПб. : Символ&Плюс. 2006. 240 с.

2. Бабаев А. Создание сайтов. СПб. : Питер. 2013. 304 с.

3. Дронов В. HTML5, CSS3 и Web 2.0. Разработка современных Web-сайтов. СПб. : БХВ-Петербург. 2011. 416 с.

Статья представлена заведующим кафедрой ИУС СПбГУТ, доктором технических наук, профессором Л. К. Птицыной.

УДК 004.896
ГРНТИ 20.19.29

АЛГОРИТМ РАСПОЗНАВАНИЯ РЕЧИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ НЕЙРОННЫХ СЕТЕЙ И ЕГО ПРИМЕНЕНИЕ В ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

В. Г. Трубицын, В. А. Чеусов

Академия ФСО России

Авторы статьи раскрывают аспекты технологии нейронных сетей, а также подробно описывает применение этой технологии в решении современных прикладных задач в информационно-аналитической деятельности. В качестве примера приводится внедрение автоматизированной системы по вводу и дальнейшей обработке первичных результатов социологических опросов. Авторы приводят результаты функционального моделирования в нотации IDEF0 исследуемого процесса без внедрения автоматизированной системы и с ее внедрением, подчеркивая то, как именно улучшится процесс, если внедрить автоматизированную систему. Описывается алгоритм обработки речевой информации и преобразования ее в текст. Также автор обращает внимание на предъявляемые требования к значениям показателей эффективности функционирования автоматизированной системы – оперативность и безошибочность.

Данная статья представляет интерес и практическую ценность для специалистов в области аналитической деятельности и систем искусственного интеллекта.

нейронная сеть, автоматизированная система, распознавание речи, социологический опрос, оперативность, безошибочность.

На сегодняшний день, очень ярко наблюдается высокий темп развития и активного использования искусственного интеллекта, в частности голосовых помощников.

Роль голосовых помощников безусловно велика, ибо их использование значительно сокращает количество рутинных операций, которые до внедрения голосовых помощников выполнял человек. Стоит с уверенностью сказать, что голосовые помощники отлично справляются с поставленными задачами, основная из которых это прием, обработка и выдача результатов на поступающие в систему различного рода голосовые запросы от пользователей. Как же работают голосовые помощники?

Алгоритм распознавания речи проходит в несколько этапов:

1. Предварительная звуковая обработка сигнала и формирование массива исходных данных для нейронной сети.

2. Обучение нейронной сети и получение набора весовых коэффициентов нейронной сети обеспечивающих требуемую точность распознавания.

3. Распознавание тестовых данных нейронной сетью.

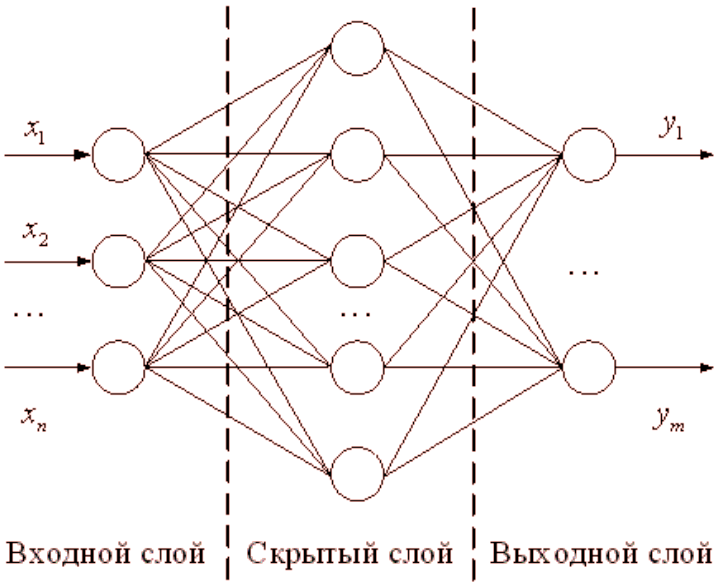


Рис. 1. Нейронная сеть для решения задачи классификации объектов

Простейшая нейронная сеть, представленная на рис. 1, состоит из:

– входного слоя, на который подаются исходный массив данных о гармониках спектра звукового сигнала;

– скрытого слоя, в котором происходят промежуточные расчеты;

– выходного слоя, который отвечает за выдачу результата нейронной сетью;

– связей между слоями. Связи, которые входят в нейрон скрытого слоя, называются синапсами. Связь, которая выходит из нейрона, называется аксоном.

На входной слой нейронной сети подается массив из фиксированного числа гармоник спектрального представления звукового сигнала. Далее производится присваивание предварительных весовых коэффициентов для синапсов между входным и скрытым слоем нейронной сети, а также между скрытым слоем и выходным слоем нейронной сети. Далее значения нейронов входного слоя умножаются на соответствующие весовые коэффициенты синапсов скрытого слоя и суммируются. После этого происходит вычисление значения функции активации нейрона. Как правило, используется сигмоидальная функция активации (рис. 2) [1].

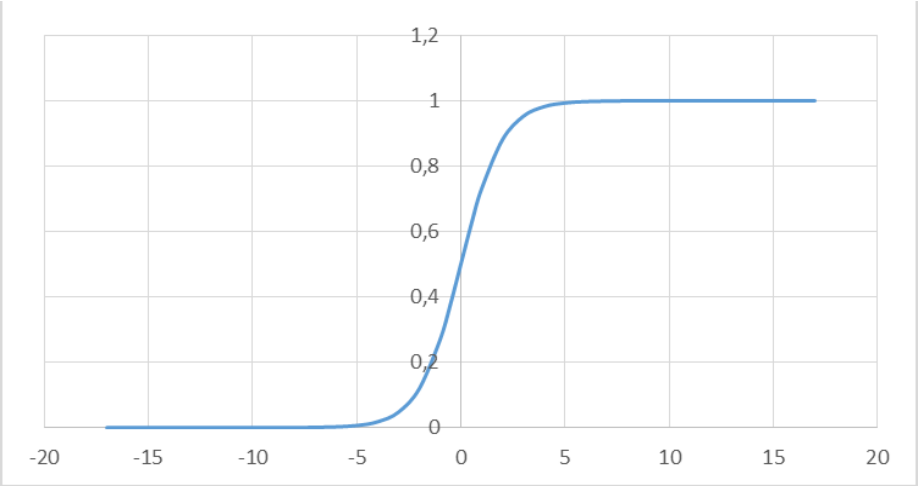


Рис. 2. График сигмоидальной функции активации нейрона

Основная проблема заключается в том, что для эффективного решения задачи классификации объектов нейронной сетью, необходимо эмпирически подбирать наиболее пригодное количество скрытых слоев нейронной сети и количество нейронов в каждом из них, а это в свою очередь сильно увеличивает время на разработку нейронной сети, тестирование и ее последующую отладку [2, 3].

Данный алгоритм распознавания речи может применяться для решения задачи голосового ввода первичных результатов социологических опросов в информационно-аналитических подразделениях.

Учет результатов проведенного социологического опроса представляет собой сложный процесс. Как правило, для учета результатов опроса и составления по нему отчёта исполнителю требуется обработать большое количество опросных листов в зависимости от того, какое количество респондентов принимало участие в социологическом опросе. Для осуществления данной процедуры исполнитель затрачивает большое количество времени. Также не исключается вероятность появления в процессе обработки информации вычислительных или иных возможных ошибок.

Одним из эффективных методов решения данного вопроса является автоматизация анализируемого процесса путём создания автоматизированной информационной системы. Процесс учета результатов социологического опроса, представленный на рис. 3 в нотации IDEF0, необходим для сбора социально-экономической, общественно-политической и другой информации о субъекте РФ, аналитической ее обработке и дальнейшей оценки перспективы развития ситуации в субъекте РФ на основе обработанных данных.

Рис. 3. Диаграмма декомпозиции процесса в нотации IDEF0
«Учет первичных результатов социологического опроса» (AS-IS)

ТАБЛИЦА. Система критериев эффективности для процесса
«Учет первичныхрезультатов социологического опроса»

Свойство	Показатель	Критерий
Оперативность	$P(t_{рп}<t^{тр}_{рп})>P^{тр}$ вероятность того, что время ввода кодов ответов одного опросного листа не превысит требуемого значения	$P(t_{рп}< 60с)> 0,95$ (значение критерия выбрано исходя из требований заказчика)
Безошибочность	$P(K_{общ}<K_{тробщ})>P^{тр}$ вероятность того, что количество ошибок в процессе ввода и проверки кодов ответов одного опросного листа не превысит требуемого значения	$P(K_{общ} =0)>0,95$ (значение критерия выбрано исходя из требований заказчика)

После анализа составляющих исследуемого процесса и составляющих его процессов был выявлен ряд показателей, представленных в табл.

На основании этих показателей, были определены критерии эффективности, при помощи которых можно произвести дальнейшее улучшение системы по свойствам оперативности и безошибочности.

Рис. 4. Функциональная модель автоматизированного процесса в нотации IDEF0 «Учет первичных результатов социологического опроса» (TO-BE)

Согласно схеме, представленной на рис. 4, этап голосового ввода кодов ответов проведенного социологического опроса, проверки данных на предмет безошибочности и вывода значений кодов ответов в результирующий файл данных будут осуществляться с использованием ресурсов автоматизированной системы. Данное решение способствует повышению оперативности учета первичных результатов социологического опроса приблизительно в 3–4 раза.

Пример программного интерфейса прототипа автоматизированной системы, реализующей алгоритм распознавания речи с использованием нейронной сети со 100%-ной точностью, представлен на рис. 5 [4].

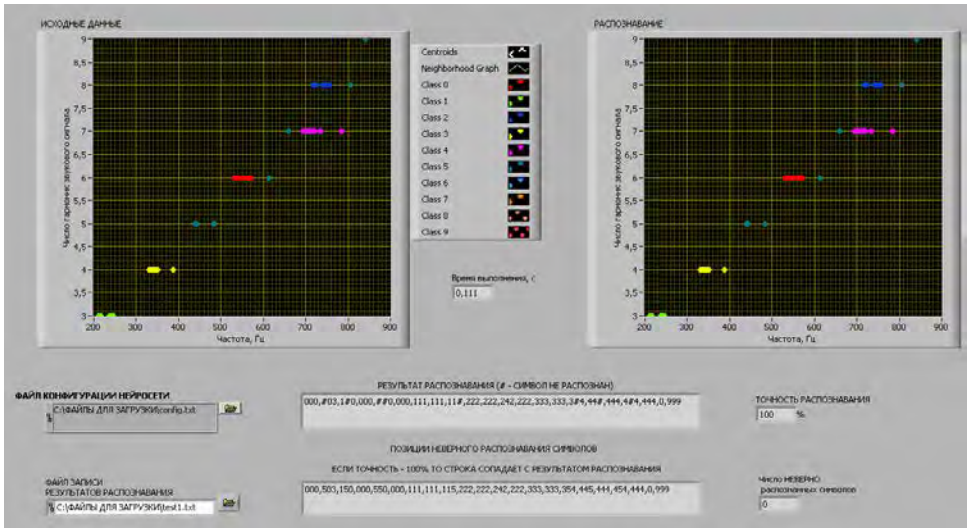


Рис. 5. Программная реализация алгоритма распознавания речи

Список используемых источников

1. Барский А. Б. Введение в нейронные сети. М. : Интуит, 2016. 359 с. ISBN: 978-5-97060-387-1.
2. Гудфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение: пер. с англ. М. : ДМК Пресс, 2018. 652 с. ISBN: 978-5-97060-618-6.
3. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. СПб. : Питер, 2018. 480 с. ISBN: 978-5-496-02536-2.
4. Trubitsyn V. G., Cheusov V. A. Application of algorithm speech definition using technology of neural networks in activity of informational-analytic unions // Modern informatization problems in economics and safety (MIP-2020'ES): Proceeding of the XXV-th International Open Science Conference (Yelm, WA, USA, January 2020) / Editor in Chief Dr. Sci., Prof. O. Ja. Kravets – Yelm, WA, USA: Science Book Publishing House, 2020. 100 p. PP.71–76. ISBN: 978-1-62174-129-9.

УДК 550.34.013.2
ГРНТИ 20.23.29

ИССЛЕДОВАНИЕ ИФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ СОПРОВОЖДЕНИЯ НАУЧНЫХ ЗНАНИЙ

А. И. Ходанович, Е. Д. Шибаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обоснована актуальность развития систем и технологий сопровождения научных знаний. Определена цель исследования информационных систем и технологий сопровождения научных знаний. Выбран профиль качества функционирования систем в целях сопровождения научных знаний. Поставлена задача расширения версий технологий по сопровождению научных знаний. Описан типовой фрагмент расширения версий технологий сопровождения научных знаний. Выбрана оптимальная структура взаимодействия «человек – компьютер» в научной деятельности. Представлены результаты исследования информационных систем и технологий сопровождения научных знаний.

информационная система, информационная технология, научные знания.

Интеграция в мировое информационное пространство, помимо существования надежно функционирующей телекоммуникационной среды, предполагает в первую очередь предоставление, как для мирового сообщества, так и для внутреннего использования собственных информационных

ресурсов. Развитие собственных информационных ресурсов повышает оперативность и является неотъемлемой частью развития сети. Информационные ресурсы могут использоваться для решения разнообразных научных и прикладных задач: от поиска необходимой информации до задач принятия управленческих решений.

Что касаемо научной деятельности, IT-технологии перевернули и по сей день модернизируют все механизмы взаимодействия средств информации. Данные преобразования приведены в табл. [6, 7].

ТАБЛИЦА. Формализация технологий

Прежнее правило	Новое правило	Нынешние технологии
Информация способна появляться в одном месте, в одно и то же время	Информация способна рождаться и быть востребованной, когда угодно	Распределенные базы, технологии поиска данных, поисковые системы
Работу по оценке происходящего способны выполнять эксперты	Работу эксперта способен выполнить специалист любой предметной области	Экспертные системы
Необходимо выбирать между децентрализацией и централизацией	Возможность получения преимуществ от взаимосвязи управления и организации наук	Работа в организованных группах, посредством телекоммуникаций
Решение за высшим руководством	Принятие решения зависит от каждого сотрудника, отвечающего за свой участок	Средства принятия решений, доступ к базам и хранилищам знаний
Для обработки информации требуются оборудованные ЭВМ помещения	Научный работник способен передавать и принимать информацию со своего рабочего места	Спутниковые системы связи, Интернет/Интранет, оптоволокно
Контакт в научной среде, ограниченный местом	Свободный контакт в научной среде	Базы данных, интерактив
Для получения научной информации нужна информация нахождения	Научная информация содержит информацию, где ее найти	Поиск публикаций, цитирований, агентные системы
Принятое решение пересматривается только под давлением ЧС	Планы корректируются оперативно, по мере необходимости	Управления рисками, мощные компьютеры, системы гибкого планирования

Структура технологий сопровождения научных знаний, соответствующей современным тенденциям используемых технологий представлена на рис.

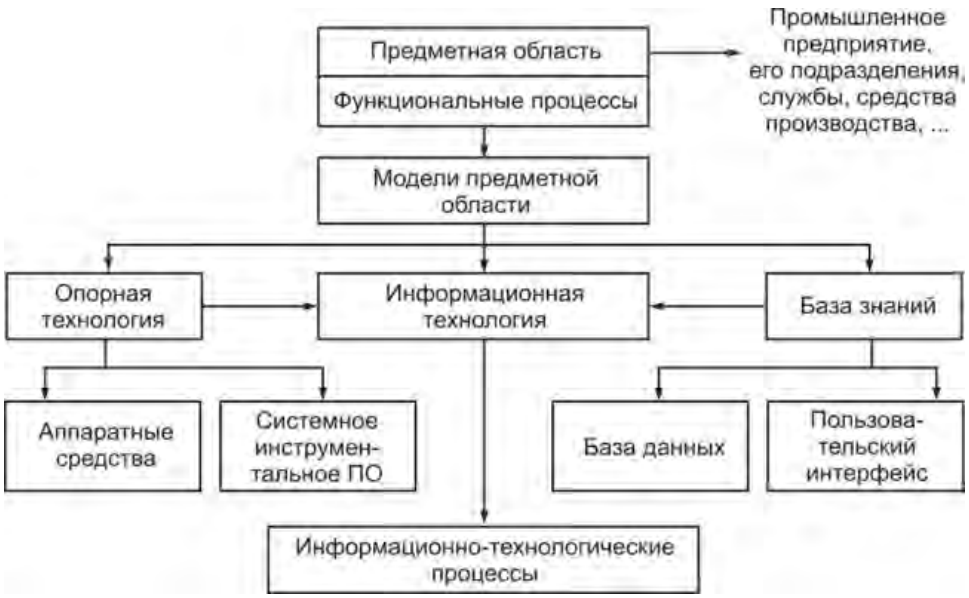


Рис. Структура технологий для сопровождения научных знаний

Компания «БАРС Груп» стала одним из первых отечественных ИТ-производителей, которые стали создавать государственные информационные системы на основе облачных технологий.

«БАРС Груп» специализируется на комплексных проектах для федеральных ведомств, региональных структур, крупных государственных и коммерческих компаний.

Alpha BI – BI-платформа для создания прикладных аналитических систем компании. Возможности: комплексный многомерный анализ данных, интеграция информации, визуализация экспериментов, построение отчётов.

Единое информационное пространство для работы исследователей

В процессе реализации нового научного учреждения или портала в обязательном порядке ключевой задачей является обеспечение бесперебойной работы сети при работе наибольшего числа исследователей и научных сотрудников сервиса. Также, несомненным преимуществом является способность портала в общении или обмене мультимедийной информацией исследователей между собой в рамках этого самого портала.

Поиск научной информации

Поиск необходимой информации, тем более связанной с научной сферой, часто сталкивается с проблемой ее доступа в сети Internet, поэтому существует всего несколько путей реализации наиболее обширного поиска: физический поиск адреса, с помощью поискового сервера [12].

Электронные публикации

Любая изданная публикация должна быть доступной для создания, внесения и удаления любым автором в сети ЭБ, также целесообразно обеспечить хранение публикации на сервере библиотеки, что позволило бы автору иметь постоянный и свободный доступ к любому изданию, выпущенному в рамках данной ЭБ. Причем данный доступ должен быть в доступности вне зависимости от местонахождения исследователя или простого пользователя [13].

Электронная доска объявлений

Реализация данного сервиса смогла бы повлиять на наглядность разнообразной информации о проводимых мероприятиях, по типу конференций, симпозиумов, защит диссертаций и прочего. А также, такая доска объявлений, размещенная на ресурсе ЭБ, могла бы оповещать пользователей не только о чисто научных новостях, но и о приглашении учебными учреждениями на конференции или о приглашении специалистов на совещание, работу и т. п.

Библиотечные информационные системы

При вышеупомянутом достаточном финансировании проекта заказчиком, в рамках направления разработки, допустима и необходима покупка собственного сервера для реализации научной ЭБ, с последующим созданием электронного каталога ЭБ и ИС удаленного библиографического обслуживания пользователя.

Список используемых источников

1. Аксюхин А. А., Вицен А. А., Мекшенева Ж. В. Информационные технологии в образовании и науке // Современные наукоемкие технологии. 2009. № 11. С. 50–52.

2. Андреев Г. И., Смирнов С. А., Тихомиров В. А. Основы научной работы и оформление результатов научной деятельности: учеб, пособие. М., 2004.

3. Василевич Л.И. Научно-методическое сопровождение профессиональной деятельности педагогических работников на основе кластерного подхода: проблемы, опыт перспективы // Реализация идей В. А. Сухомлинского в теории и практике современного образования (к 100-летию со дня рождения) Международная научно-практическая конференция. Сб. ст. в 2-х т. / Научный редактор В. Г. Рындак. 2018. С. 153–156.

4. Венделева М. А., Вертакова Ю. В. Информационные технологии в управлении: учеб. пособие. М. : Юрайт, 2013. 462 с.

5. Цибульский Г. М., Носков М. В., Барышев Р. А. и др. Активная информационная система вуза в информационно-образовательной среде // Педагогика : журнал. 2017. № 3. С. 28–33.

6. Гончарик Н. Г. Цифровые мультимедийные технологии – смысловые средства передачи информационного содержания // Проблемы создания информационных технологий : сб. науч. тр. 2012. Вып. 21. С. 74–76.

7. Гушул Ю. В., Тесля Е. В. Информационно-аналитическое сопровождение: современные задачи и траектории развития // Научные и технические библиотеки. 2020. № 1. С. 24–44.

8. Козилова Л. В., Чвякин В. А. Динамика показателей системы ценностей в структуре инновационного обеспечения педагогической деятельности // Педагогическое образование и наука : журнал. 2017. № 1. С. 34–38.

9. Рабинович П. Д., Баграмян Э. Р. Практикум по интерактивным технологиям: методическое пособие. М: . БИНОМ. Лаборатория знаний, 2012. 96 с.

10. Перегоедова Н. В., Бусыгина Т. В., Балуткина Н. А. Проблемы и перспективы оптимизации структуры и методологии формирования информационных ресурсов по гуманитарным отраслям знания для сопровождения научных исследований СО РАН // Библиосфера. 2010. № 4. С. 37–44.

11. Садырин В. В., Потапова М. В., Татьянченко Д. В. Сетевое взаимодействие педагогических вузов: механизмы формирования и развития // Педагогическое образование и наука : журнал. 2017. № 1. С. 19–25.

12. Тихонов А. Н. Информационные технологии и телекоммуникации в образовании и науке (IT&T ES'2007) // Материалы международной научной конференции, ФГУ ГНИИ ИТТ «Информика». М. : ЭГРИ, 2007. 222 с.;

13. Холин А. Н. Ситуационные центры: перспективы цифровых технологий. Площадка для апробации цифровых технологи // Науч. периодика: проблемы и решения. 2011. № 6. С. 6–9.

УДК 004.413.2
ГРНТИ 82.05.02

АНАЛИЗ МЕТОДОЛОГИЙ РАЗРАБОТКИ IT-ПРОЕКТОВ И РАЗРАБОТКА AGILE-КОНЦЕПЦИИ ДЛЯ НАЧИНАЮЩЕЙ КОМАНДЫ РАЗРАБОТЧИКОВ ПРОГРАММНЫХ СРЕДСТВ

В. В. Черномырдин, А. А. Шиян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Управление IT-проектами подразумевает под собой большое количество различных методологий и концепций. Для начинающей команды существующие методологии могут казаться сложными и непонятными. Рассмотрены наиболее популярные «гибкие» методологии разработки IT-проектов, проведен сравнительный анализ с другими методологиями, предложены варианты интеграции элементов нескольких подходов в одну методологию, актуальную для небольшой, начинающей команды разработчиков программных средств.

разработка, управление проектами, agile, начинающие разработчики, методологии.

Мир IT-разработки многообразен и постоянно развивается, каждый день появляются новые инструменты и методологии разработки продуктов. Одним из актуальных трендов на сегодняшний день являются гибкие методологии разработки проектов (*Agile*) [1]. Agile возник в сфере IT, но на сегодняшний день проник уже во многие сферы деятельности людей, от промышленности до искусственного интеллекта. Философия Agile изложена в манифесте разработки ПО: «Люди и взаимодействие важнее процессов и инструментов. Работающий продукт важнее исчерпывающей документации. Сотрудничество с заказчиком важнее согласования условий контракта. Готовность к изменениям важнее следования первоначальному плану» [6]. Из манифеста ясно то, что упор делается на взаимодействие людей друг с другом и работа на результат. Кроме того, подчеркивается отличительная черта Agile – это постоянная динамика, ориентация на изменения в рынке, плотная обратная связь между заказчиком и разработчиками.

Одними из представителей Agile-семейства методологий являются Scrum и Kanban [2]. Каждая из методологий обладает рядом недостатков и преимуществ. Однако, подобные методологии часто используют только в больших IT-компаниях и командах. Для начинающих разработчиков и развивающейся команды крайне сложно соблюдать все алгоритмы или, например, «церемонии» методологий. Каждой команде приходится адаптировать принципы и подходы к разработке продукта, для наибольшей оптимизации процессов в каждом отдельном взятом случае. На данный момент, молодым командам приходится тратить очень много сил и времени, на то, чтобы адаптировать под себя методологию, что ведет к финансовым и временным потерям.

Scrum – это по сути «подход структуры». Данная методология регламентирует то, что над любым проектом работает универсальная и самоорганизующаяся команда разработчиков, а также специалист контроля (scrum-мастер) и владелец продукта. Владелец продукта в разных случаях является либо заказчиком, либо менеджером, который выступает буфером между командой и заказчиком. По своей сути владельца продукта можно сравнить с куратором. Специалист контроля же выступает ментором, он следит за исполнением «церемоний», проводит собрания, решает бытовые проблемы и мотивирует команду. Сейчас на рынке труда даже появилась отдельная должность scrum-мастер, правда, как можно понять, для небольшой команды разработчиков это недопустимая роскошь.

Рабочий процесс Scrum делит на равноценные спринты – это периоды от недели до месяца. В начале спринта формируются задачи на спринт из общего списка задач, в конце обсуждаются результаты, а команда начинает готовится к новому спринту. Данный подход позволяет постоянно анализировать прогресс работы над продуктом, вовремя вносить коррективы,

что позволяет повысить эффективность команды, схема работы методологии представлена на рис. 1.

Рис. 1. Схема работы методологии Scrum

Kanban – это подход баланса. Его задача оптимизировать процесс разработки так, чтобы все участники процесса находились в равной трудовой загрузке, и никто никого не ждал [3]. В Kanban нет отдельных ролей, как в Scrum. Все задачи делятся не на спринты, а на статусы этих самых задач: «Планируется», «Разрабатывается», «Тестируется», «Завершено». Главный показатель эффективности в Kanban – это среднее время прохода задачи по доске. Для визуализации часто используют и физически доски. Однако, в чистом виде Kanban обладает недостатком в виде отсутствия обратной связи и сложным внесением корректировок. К тому же, визуально Kanban доски могут быть огромными, что мешает восприятию. Схема работы Kanban-доски представлена на рис. 2.

Рис. 2. Схема работы Kanban-доски

В условиях изменчивого рынка, для разработки больших и сложных проектов используют подход реализации MVP. Наиболее часто, данный термин можно услышать в стартап-сообществах, так как для инвесторов важно снижение рисков и проверка способностей команды разработчиков. MVP – это минимальный рабочий прототип, который должен содержать в себе функционал, отличающий систему от других и необходимый для корректного решения задач пользователей [4]. Кроме того, тестировать гипотезы UI/UX дизайнеров на MVP гораздо проще, нежели чем на полностью реализованном продукте. В данном случае, внесение корректив по итогам тестирования будет гораздо проще, нежели чем уже на готовом. Можно сказать, что использование MVP позволяет оптимизировать разработку, снизить риски инвесторов и получить результат быстрее и качественнее.

Исходя из этого, можно предположить, что начинающая команда разработчиков, приступая к реализации проектов должна учитывать промежуточный итог в виде MVP или даже нескольких версий, так как его реализации позволит повысить доверие со стороны инвесторов или заказчиков, а также помогает протестировать и проверить гипотезы самих разработчиков. Запускать MVP стоит как на тестовую аудиторию, так и на самих разработчиках и заказчиках [5]. Чем больше разных взглядов и мнений соберет команда, тем более точно их проект сможет попасть в целевую аудиторию. В условиях того, что каждый день придумываются новые идеи и проекты, особенно мелкого масштаба, начинающей команде разработчиков нужно быть уверенными в том, что их продукт смогут оценить по достоинству.

Исходя из всей изложенный информации, а также опираясь на опыт работы молодых команд разработчиков можно сказать, что для реализации собственных проектов, а тем более стартапов, необходимо придерживаться следующих принципов из нескольких методологий, позволяющих оптимизировать работы и повысить эффективность команды:

1. Разработку необходимо вести итерациями в несколько недель (лучше всего по 2), на каждую из которых команда выбирает задачи и не меняет их в ходе итерации. По итогам одного спринта команда должна получать рабочий функционал программного средства, либо его часть, который можно было бы продемонстрировать заказчикам.

2. При реализации больших проектов, стоит учитывать реализацию MVP, вынося в него основные и отличающие от других систем функции, поэтому задачи на спринты стоит ориентировать на наиболее скорейшее получение результатов и проверки гипотез.

3. В ходе разработки, наиболее удачной визуализацией задач может стать Kanban-доска в электронной системе управления проектами YouTrack, стоимость которой для небольших команд небольшая и зависит от выбранного тарифа.

4. Для правильного восприятия важности задач необходимо использовать принцип расстановки приоритетов MoSCoW, который разделяет любые задачи на: Must (обязательные), Should (нужно сделать, если возможно), Could (можно сделать, если этого не влияет на результат отрицательно), Would (хотелось бы в будущем). Пересматривать приоритеты для задач необходимо каждый спринт, так как некоторые задачи могут быть не реализованы за текущий спринт.

5. В условиях дистанционной работы команды, либо не постоянного рабочего графика крайне сложно будет соблюдать «ежедневные встречи» из Scrum, однако простым решением может быть 3-х разовые встречи в неделю, либо использование видеоконференций. Отказаться от подобных встреч нельзя, так как позволяют постоянно контролировать процесс разработки проекта и вовремя устранять преграды и сложности.

6. Небольшая команда разработчиков не может себе позволить много сотрудников, поэтому необходимо использовать следующие роли: project manage – объединяющий в себе Scrum-мастера и владельца продукта, так как по сути может являться буфером между командой и заказчиком, проводить презентации результатов итераций; team leader – им может быть самый опытный представитель команды разработчиков, необходим для формирования списка задач по проекту и помощи в работе других специалистов, так как начинающие разработчики не могут быть универсальными и самоорганизующимися единицами, как от нас требует Scrum.

В ходе анализа популярных на сегодняшний день подходов к разработке IT-проектов выявлено то, что они не предназначены для молодых и начинающих команд разработчиков. Использование их в чистом виде будет приносить команде лишние сложности. Исходя из этого, было необходимо адаптировать несколько методологий под нужды начинающей команды и свести всё в один список принципов. Предложенные принципы взяты из разных методологий, но именно такая комбинация позволяет начинающей команде разработчиков быть эффективной с самого начала. Конечно, многие моменты команда подстраивает под себя на основе своего опыта и особенностей, но для формирования «собственной» философии еще нужно время и опыт. Кроме того, использование этого подхода позволяет снизить вероятность провала проекта (особенно в рамках стартапа), тем самым увеличивая шансы команды на успешную карьеру и развитие.

Список используемых источников

1. Перерва Андрей. Путь IT-менеджера. Управление проектной средой и IT-проектами. М. : Питер, 2016. 647 с.

2. Partogi Joshua. Certified Scrum Master vs Professional Scrum Master // Lean Agile Institute. July 7, 2013. Retrieved May 10, 2017.

3. Sutherland Jeff. Scrum: The Art of Doing Twice the Work in Half the Time. Crown Publishing Group, 2014.

4. Вольфсон Борис. Гибкое управление проектами и продуктами. М. : Питер, 2014. 137 с.

5. Ловина В. В., Шиян А. А. Использование возможностей облачного сервиса Битрикс24 для совместной работы команды веб-разработчиков // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научнометодическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 2. С. 474–477.

6. Официальный сайт «Agile Alliance». URL: https://www.agilealliance.org/agile101/the-agile-manifesto.

ЦИФРОВАЯ ЭКОНОМИКА, УПРАВЛЕНИЕ И БИЗНЕС-ИНФОРМАТИКА

УДК 37.02
ГРНТИ 14.15.07

ИСПОЛЬЗОВАНИЕ КОЛИЧЕСТВЕННЫХ МЕТОДОВ АНАЛИЗА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Ю. В. Арзуманян, М. Б. Вольфсон, А. А. Захаров, А. Д. Сотников

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Описывается метод количественной оценки взаимосвязи курсов образовательной программы на основе характеристик ключевых понятий. Рассматривается алгоритм формирования количественных характеристик ключевых понятий с учётом когнитивной ментальности преподавателя. Формулируются принципы построения образовательной траектории по ключевым понятиям для требуемой специальности. Приводятся сценарии использования полученных результатов для гармонизации как отдельных дисциплин, так и образовательной программы в целом.

образовательная программа, ключевое понятие, количественная характеристика ключевого понятия, мера взаимосвязи дисциплин, образовательная траектория.

Существующие методы количественной оценки дидактических материалов, к которым можно отнести анализ учебных текстов по количеству «семантической» информации [1, 2], тезаурусный анализ [3, 4], анализ на базе понятий сложности [5, 6], контент-анализ [7] и пр., используют математические инструменты обработки исходных данных, полученных без заметного учёта когнитивной ментальности задействованного в программе обучения конкретного педагога. В тоже время, ментальность лектора, его индивидуальный взгляд на предмет, подчас, играют весьма важную, а иногда и решающую роль в результате обучения. Предлагаемый подход в значительной степени учитывает персональные особенности путём формирования исходных данных на основе представлений преподавателей о месте их дисциплин в образовательной программе в целом.

В дальнейшем изложении будет использован термин «ключевое понятие» (КП), отличающийся от общепринятого «ключевого слова» только тем, что представляет собой не одно слово или словосочетание, но может быть целым выражением из нескольких слов в контексте конкретной дисциплины или образовательной программы.

В соответствии с традиционным построением любая образовательная программа (ОП) представляет собой совокупность взаимосвязанных дисциплин (Д). В свою очередь, каждая дисциплина состоит из совокупности взаимосвязанных дидактических единиц, или тем. На каждом уровне этой иерархической структуры можно выделить множества КП, характеризующих как отдельные Д, как и всю ОП. Рис. 1 иллюстрирует иерархию структуры ОП в её временном развитии. Пунктирные стрелки обозначают связи изучаемых Д с ОП, а непрерывные – междисциплинарные связи. Как в первом, так и во втором случае связи устанавливаются через КП конкретных Д в конкретной ОП.

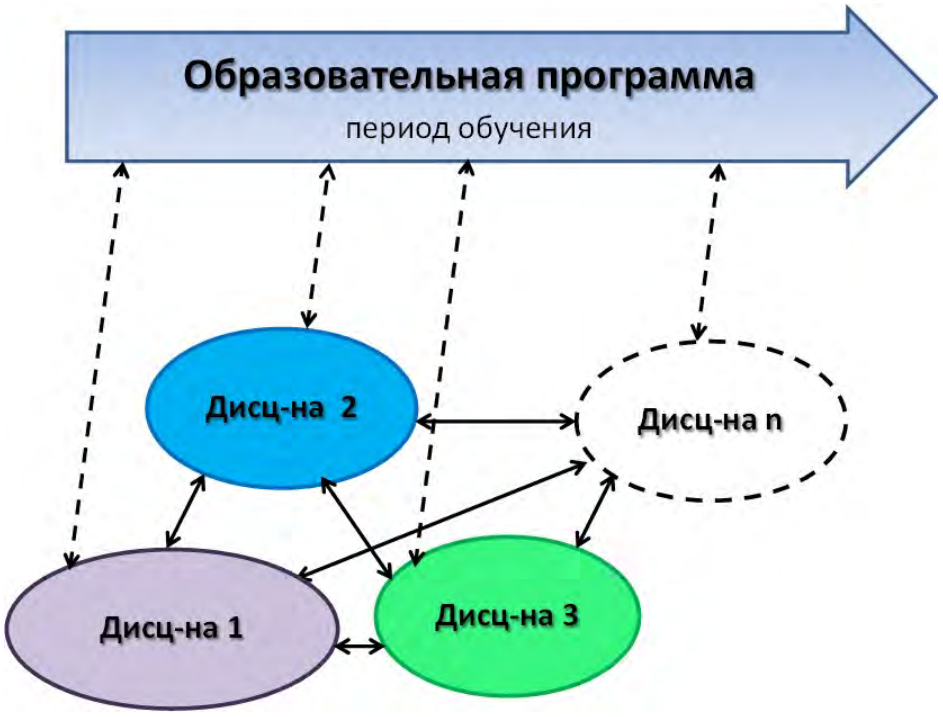


Рис. 1. Структура образовательной программы

Центральное место рассматриваемого метода состоит в определении КП и их количественных характеристик самими ведущими дисциплины преподавателями.

В ходе учебного процесса любой преподаватель при изложении конкретной темы своего предмета раскрывает несколько КП. Каждое КП он сам может охарактеризовать некоторой количественной величиной (мерой). В качестве меры конкретного КП допустимо использовать любую характе-

ристику, связанную с временем учебного процесса и удовлетворяющую аксиомам меры [8]. Например, это может быть аудиторное время, или количество страниц учебника (методического пособия), или время записи в видеокурсе и т. п.

Ведущий дисциплину преподаватель для всех тем формирует список КП с их количественными характеристиками. Некоторые из КП в разных темах могут повторяться, тогда, учитывая разнесённость изучения тем во времени, в рамках всей дисциплины характеристики таких КП суммируются так, что общая мера D всех КП совпадает со всем аудиторным временем или объёмом изучаемого материала. Таким образом, результатом анализа преподавателем своей дисциплины с общей мерой D является совокупность тем со списками КП, а также общий список КП $S = \{S_1, S_2, \ldots, S_n, .., S_N\}$ с их совокупными мерами $q(S_n)$, $n = 1, .., N$. (рис. 2).

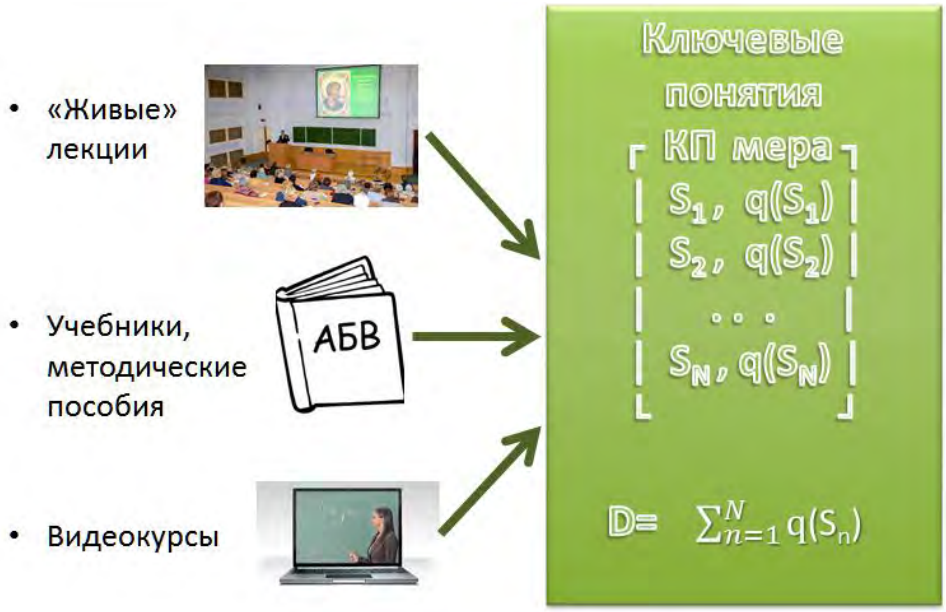


Рис. 2. Источники мер ключевых понятий

Поскольку в образовательную программу обычно входит ряд дисциплин и может быть задействовано несколько преподавателей необходимо установить следующие общие требования к формированию КП и вычислению мер:

1. Используются одинаковые меры для всех дисциплин (например, аудиторное время).

2. Соблюдается количественная сопоставимость КП (примерно одинаковое количество КП на единицу учебного времени, например, около 10 КП на академический час).

3. Применяется принцип семантической сопоставимости (синонимы и близкие по значению понятия отождествляются и рассматриваются как одно КП).

Определение величин междисциплинарных связей выполняется путём попарного сравнения. Для этого преподаватель дисциплины $Д_1$ анализирует темы дисциплины $Д_2$ и выделяет КП $Д_1$, которые, по его мнению, относятся к темам $Д_2$. Количество выделенных КП и их суммарная мера характеризует величину связи дисциплины $Д_1$ с дисциплиной $Д_2$ $q(Д_1 \rightarrow Д_2)$. Аналогичным образом преподавателем дисциплины $Д_2$ определяется величина $q(Д_2 \rightarrow Д_1)$ связи $Д_2$ с $Д_1$. Общая мера $q(Д_1 \leftrightarrow Д_2)$ связи пары $Д_1$ и $Д_2$ вычисляется как сумма $q(Д_1 \rightarrow Д_2)$ и $q(Д_2 \rightarrow Д_1)$, т. е. $q(Д_1 \leftrightarrow Д_2) = q(Д_1, Д_2) + q(Д_2, Д_1)$.

Помимо междисциплинарных связей преподаватели определяют совокупную меру $q(Д, ОП)$ совпадений КП своих дисциплин с ключевыми понятиями всей образовательной программы (КПОП). Сами КПОП могут задаваться государственными стандартами, министерствами, общественными организациями, работодателями, учащимися, наконец.

При наличии перечисленных характеристик можно сформулировать регулярную процедуру формирования образовательной программы с требуемыми КПОП, в том числе в рамках индивидуальных образовательных траекторий.

На первом этапе все дисциплины ОП выстраиваются в убывающий по значению $q(Д, ОП)$ вариационный ряд. Формирование порядка следования дисциплин в образовательной программе начинается с выбора дисциплин в начале вариационного ряда, т. е. дисциплин, завершающих обучение. Количество таких дисциплин определяется физическими возможностями учебного заведения (аудиторный фонд, санитарные нормы, расписание преподавателей и т. п.). Затем, последовательно выбираются дисциплины с наибольшими связями с уже выбранными и далее аналогичным образом. Вполне возможно, что у дисциплин в конце вариационного ряда (дисциплин, с которых начинается образовательная программа) может отсутствовать связь с КПОП и они целиком служат необходимым базисом для завершающих обучение предметов (рис. 3, см. ниже)).

Помимо формирования новых образовательных программ предлагаемый подход может быть использован для анализа существующих программ обучения с целью гармонизации следования дисциплин в их равномерной взаимоувязанности. Кроме того, появляется возможность преподавателям создавать или корректировать свои курсы, акцентировать внимание учащихся на ключевых понятиях, имеющих важное значение для всей программы в целом, выравнивать дидактическую сложность материала тем внутри дисциплины, обоснованно менять её объём.

В заключение необходимо выразить благодарность сотрудникам кафедры бизнес-информатики нашего университета Е. П. Охинченко и Е. В. Стригиной за предоставленные материалы по своим дисциплинам, во многом определившие появление этой работы.

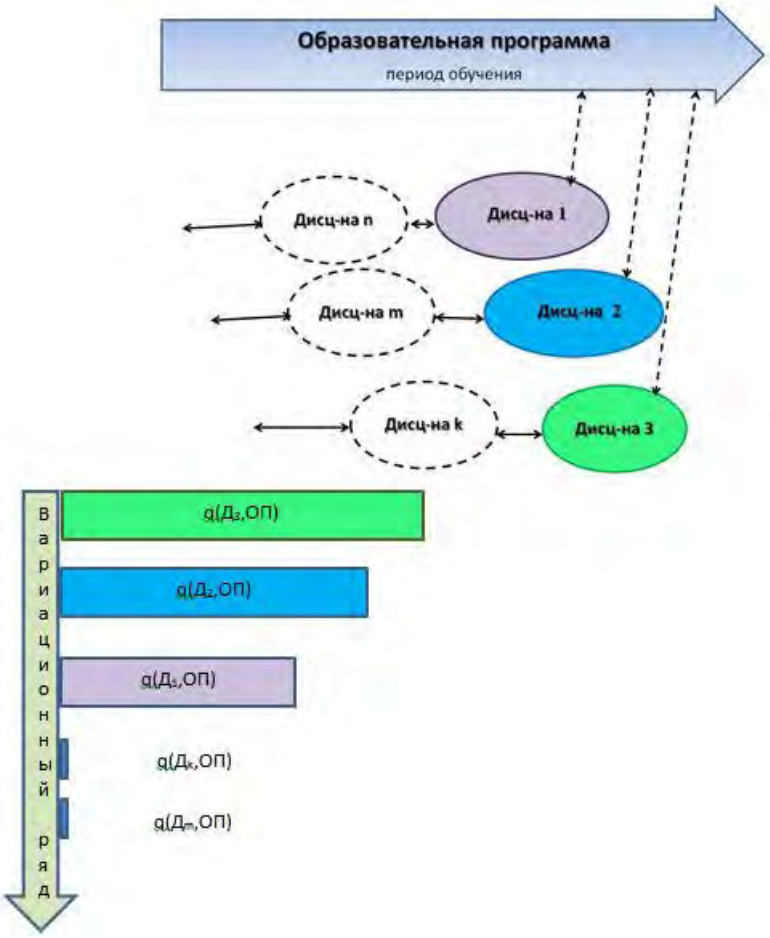


Рис. 3. Построение образовательной программы

Список используемых источников

1. Виткин В. Б, Синергетическая теория информации: пояснения и терминологические замечания // Научный журнал КубГАУ. 2012. № 80 (06).

2. Зеркалъ О. В. Семантическая информация и подходы к ее оценке. Часть 1. Семантико-прагматическая информация и логико-семантическая концепция // Философия пауки. 2014. № 1. С. 53–69.

3. Лукашевич Н. В. Тезаурусы в задачах информационного поиска. М., 2010. 396 с.

4. Луков Вал. А., Луков Вл. А. Методология тезаурусного подхода: стратегия понимания // Знание. Понимание. Умение. 2014. № 1. С. 18–35.

5. Майер Р. В. Проблема оценки сложности дидактических объектов и её решение// Азимут научных исследований: педагогика и психология. 2019. Т. 8. № 4 (29). С. 126–128.

6. Невдах М. М. Исследование информационных характеристик учебного текста методами многомерного статистического анализа // Прикладная информатика. 2008. № 4. С. 117–130.

7. White M. D., Marsh E. E. Content analysis: A flexible methodology // Lihraty trends. 2006, Vol. 55, No 7. PP. 22–45.

8. Колмогоров А. Н., Фомин С. В. Элементы теории функций и функционального анализа. М. : Наука, 1976. 543 с.

УДК 37.02
ГРНТИ 14.15.07

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИНФОРМАЦИОННЫХ ХАРАКТЕРИСТИК УЧЕБНЫХ ДИСЦИПЛИН

Ю. В. Арзуманян, А. А. Захаров, Я. В. Соколова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Учебные дисциплины представляются источниками информации, в которых сообщениями выступают ключевые понятия дидактических единиц. Используемая модель позволяет получить оценки различных характеристик классической теории информации. В частности, по величине взаимной информации метод даёт возможность оценить близость лекций к материалам выбранного учебника. Приводится пример сравнения лекции с соответствующим материалом учебника дисциплины «Архитектура предприятия».

ключевое понятие, информационная характеристика дидактической единицы, взаимная информация.

В классической теории информации Клода Шеннона [1] появление сообщений на выходе источника суть случайные и независимые события с известными вероятностями. Такая модель плохо подходит для анализа осмысленных текстов, в которых условие независимости входит в принципиальное противоречие с весьма существенной связью между следующими друг за другом словами. Это обстоятельство привело появлению понятия «семантическая» информация [2, 2, 4, 5, 6 и др.], где делается попытка учесть смысловое содержание. К сожалению, значительные вычислительные трудности, связанные с необходимостью формализации всего многообразия отражающих результаты человеческой деятельности связей, существенно затрудняют практическое использование такого подхода.

Центральное место предлагаемого метода занимает модель учебной дисциплины, представляющей собой последовательность дидактических единиц в виде аудиторных занятий или текста учебника (учебного пособия). Как в первом, так и во втором случае дидактическая единица обозначается названием темы и описывает некоторое количество ключевых понятий. Применительно к учебнику в качестве темы чаще всего выступает название главы, а ключевое понятие содержится в названии параграфа этой главы.

На рис. изображена модель учебной дисциплины в процессе её изучения. На этом рисунке в качестве примера показано, что в теме 1 раскрываются ключевые понятия S_1, S_2 и S_3, в теме 2 – S_4, S_2 и S_5 и так далее. Размер

овалов с соответствующими надписями отображает время, затраченное на лекции (количество произнесённых слов), или количество слов в тексте учебника.

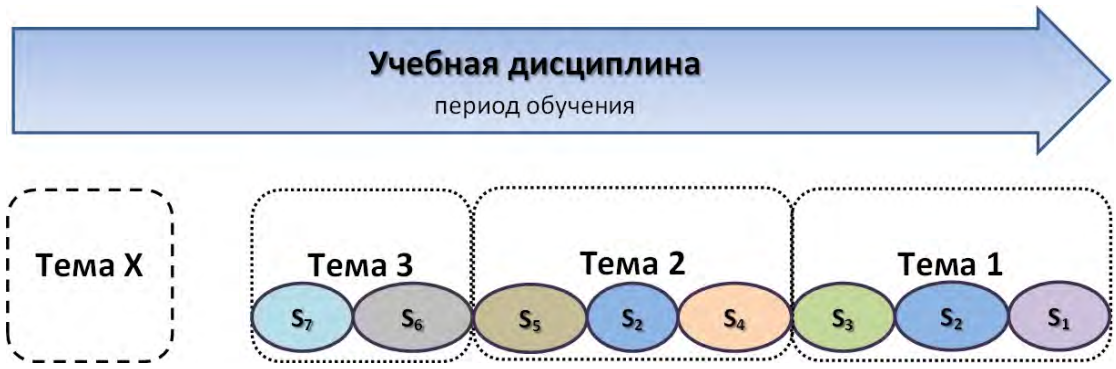


Рис. Модель учебной дисциплины

В предлагаемой модели все слова, использованные при описании конкретного ключевого понятия, отождествляются с ним самим. Таким образом, выполняется своеобразное «квантование» или «огрубление» всей дисциплины до списка выделенных ключевых понятий с их суммарными характеристиками затраченного в аудитории времени или количества слов. Следует заметить, что весьма важной в такой трактовке является временна́я независимость изучения ключевых понятий и, следовательно, выбранные характеристики обладают свойством аддитивности. Например, на рис. ключевое понятие S_2 изучается в двух первых темах и характеристика этого понятия равна сумме соответствующих значений при условии, что в других дидактических единицах S_2 не встречается. В результате вся учебная дисциплина может быть описана списком различных ключевых понятий $S = \{S_1, S_2, \ldots, S_n, .., S_N\}$ с их совокупными мерами $\{q(S_n), n = 1, .., N\}$, причём сумма всех $q(S_n)$ равна $Q(S)$ – периоду обучения дисциплине или объёму учебного материала в словах.

В представленной модели значительно снижена присущая семантической информации роль связи между сообщениями источника и достаточно обоснованным становиться использование информационных характеристик в соответствии с теорией Клода Шеннона, где в качестве оценки значений вероятности $p(S_n)$ появления сообщения S_n используется частость этого ключевого понятия в дисциплине в целом, т. е. $p(S_n) = q(S_n)/Q$ ($n = 1, .., N$).

В качестве примера рассмотрим результат сравнительного анализа информационных характеристик лекции по дисциплине «Архитектура предприятия» и соответствующих разделов учебника [7].

В таблице 1 приведен список раскрытых на лекции ключевых понятий, частость их появления и количество соответствующей информации. Указанные в таблице значения были получены путём преобразования аудиозаписи лекции в текст с последующим выделением S_n.

ТАБЛИЦА 1. Ансамбль *S* ключевых понятия лекции

n	Ключевое понятие (S_n)	$q(S_n)$	$i(S_n)$
1	Системный подход	217	3,804027
2	Стратегический подход	255	3,571225
3	Процессный подход	725	2,063741
4	Бизнес-аналитика	538	2,494116
5	Архитектурный подход	131	4,532155
6	Управление ЖЦ ИС	61	5,634841
7	Сервисный подход	89	5,089845
8	Проектный подход	488	2,634841
9	Проект	114	4,732688
10	ИТ-сервис	48	5,980616
11	Бизнес-сервис	146	4,375754
12	Цифровизация	58	5,707597
13	Электронный бизнес	46	6,042016
14	Прочее	115	4,720088
	$Q(S)=$	**3031**	

В таблице 2 приводятся аналогичные результаты анализа разделов учебника.

ТАБЛИЦА 2. Ансамбль *Z* ключевых понятий материалов учебника

n	Ключевое понятие (Z_n)	$q(Z_n)$	$i(Z_n)$
1	Системный подход	3177	3,0584032
2	Стратегический подход	3377	2,9703261
3	Процессный подход	2702	3,2920406
4	Бизнес-аналитика	1523	4,1191523
5	Архитектурный подход	2083	3,6674054
6	Управление ЖЦ ИС	1194	4,4702654
7	Сервисный подход	2973	3,1541488
8	Проектный подход	3340	2,9862202
9	Проект	979	4,7566875
10	ИТ-сервис	0	0
11	Бизнес-сервис	0	0
12	Цифровизация	0	0
13	Электронный бизнес	0	0
14	Прочее	5118	2,3704881
	$Q(S)=$	**26466**	

Используя в таблицах значения количества информации в ключевых понятиях, нетрудно подсчитать величины энтропий $H(S)$= 3,255578436 бит и $H(Z)$ = 3,175123481 бит ансамблей S и Z соответственно.

Представляет интерес в качестве меры информационной «близости» рассчитать количество взаимной информации $I(S, Z)$ лекции и учебника. Эта характеристика может быть получена с помощью известного соотношения – $I(S,Z)= H(S) + H(Z) – H(S\cup Z)$, где $H(S\cup Z)$ – энтропия объединённого ансамбля. Суммируя значения в третьих столбцах таблиц 1 и 1 нетрудно получить значение $H(S\cup Z)$ = 3,259785435 бит и значение взаимной информации $I(S, Z)$= 3,170916482 бит.

С помощью условных энтропий нетрудно подсчитать величину информационных «потерь» в лекции $H(S/Z) = H(S) – I(S, Z)$ = 0,084661955 бит (2,67 % от $I(S, Z)$) и в материалах учебника $H(Z/S) = H(Z) – I(S, Z)$ = = 0,004206999 бит (0,13 % от $I(S, Z)$) соответственно.

В заключение необходимо отметить, что предложенный метод оценки информационных характеристик отличается вычислительной простотой и естественностью, в значительной степени в выборе ключевых понятий учитывает когнитивную ментальность ведущего предмет преподавателя. Авторы надеются продолжить начатые исследования для выработки апробированных метрик оценки качества учебного процесса в различных образовательных организациях.

Список используемых источников

1. Шеннон К. Э. Работы по теории информации и кибернетике; перев. с англ. Под ред. Р. Л. Добрушина и О. Б. Лупанова. С предисловием А. Н. Колмогорова. М. : Издательство иностранной литературы, 1963. 829 с.

2. Bar-Hillel Y., Carnap R. An Outline of a Theory of Semantic Information. Technical Report No. 247, 1952 October 27, Research Laboratory of Electronics. 49 p.

3. Шрейдер Ю. А. Об одной модели семантической теории информации // Проблемы кибернетики. 1965. Вып. 13. С. 233–240.

4. Floridi L. Outline of a Theory of Strongly Semantic Information // Minds and Machines. 2004, 14(2). 197–222.

5. Floridi L. Semantic Conception of Information. The Stanford Encyclopedia of Philosophy, ed. Edward N. Zalta. 2011

6. Ruurik Holm. Non-Zero Probabilities for Universal Generalizations. 2013, Synthese 190 (18). p. 4001–4007

7. Зараменских Е. П. Основы бизнес-информатики. Новосибирск : Издательство ЦРНС, 2014. 380 с.

УДК 338.001.36
ГРНТИ 06.52.45

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ГЛОБАЛЬНЫХ ИНДЕКСОВ ИННОВАЦИЙ И СВЯЗНОСТИ ДЛЯ ОЦЕНКИ ПЕРСПЕКТИВ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ

А. М. Атаян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Для измерения уровня цифровизации в странах международными организациями были разработаны различные индексы. Особый интерес для анализа рейтинга представляет Глобальный индекс связности, используемый для анализа индикаторов инфраструктуры ИКТ и цифровой трансформации, и Глобальный инновационный индекс. Несмотря на то, что Россия не входит в группу лидеров по цифровой экономике, сравнительный анализ показателей этих индексов с показателями лидеров рейтинга, позволит выделить стратегически важные направления развития.

цифровизация; международные индексы развития; рейтинг; глобальный индекс связности GCI, глобальный инновационный индекс GII.

В развитии большинства современных стран цифровые технологии являются драйвером экономического роста и трансформации бизнеса, социальных институтов и даже коммуникаций разного уровня. Цифровая трансформация носит глобальный характер, в том числе, и потому, что получаемые выгоды и риски носят инновационный характер, далеко не всегда предсказуемый. Интенсивное развитие телекоммуникаций и средств связи опережает в своей динамике осмысление и понимание применения их возможностей в различных отраслях экономики. Но ясно одно – ни одна страна в одиночку не сможет достичь безусловного успеха, так как совокупный экономический результат проявится только при относительном выравнивании ряда показателей национальных экономик. Поэтому большинство развитых стран приняли национальные программы перехода к цифровой экономике, и рассчитывают, что цифровизация обеспечит долгосрочный экономический рост.

В условиях высокой социально-экономической и технологической турбулентности трудно принимать адекватные управленческие решения стратегического характера без понимания общей картины и тенденций мирового

развития. С этой целью разными Международными организациями проводятся исследования и составляются различные индексы, отражающие уровень развития разных аспектов цифровой экономики. Это, например, Индекс развития ИКТ (ICT *Development Index*), Индекс развития электронного правительства (E-*Government Development Index*), Глобальный индекс кибербезопасности (*Global Cybersecurity Index*), Глобальный инновационный индекс (*The Global Innovation Index* (GII)), Глобальный индекс связности (*Global Connectivity Index* – GCI) [1].

Очевидно, технологической базой построения и развития цифровой экономики являются информационно-коммуникационные технологии, чье дальнейшее развитие возможно только при наличии мощного инновационного потенциала и его своевременной реализации. Поэтому был проведен сравнительный анализ данных за 2019 г. Глобального инновационного индекса (GII) и Глобального индекса связности (GCI).

Глобальный индекс связности (GCI) «был создан для анализа широкого спектра индикаторов инфраструктуры ИКТ и цифровой трансформации, чтобы обеспечить всеобъемлющую карту глобальной цифровой экономики» [2]. GCI основан на базовых экономических категориях: поставка (предложение), спрос, опыт, потенциал, которые охватывают всю цепочку развития ИКТ и цифровой трансформации, обеспечивая 360-градусный обзор цифровой экономики. GCI анализирует цифровое преобразование в направлении передовых технологий, таких как широкополосная связь, центры обработки данных, облачные сервисы, большие данные, интернет вещей (IoT). GCI – это уникальная количественная оценка для 40 показателей цифрового развития, которые можно анализировать по вертикали (базовые категории) либо по горизонтали (технологические возможности). Этот индекс можно использовать для анализа перспектив развития цифровой экономики [3]. В GCI 2019 были внесены два других заметных изменения в методологию: объединение периметра центров обработки данных в облако и включение больших данных в недавно созданный периметр ИИ. Новый периметр ИИ включает в себя: создание данных, инвестиции в ИИ, робототехнику с поддержкой ИИ и потенциал ИИ. Структура портала расчета Глобального индекса связности [3] дает возможность не только увидеть таблицу рейтинга GCI по 79-ти странам мира, но и рассмотреть подробный профиль каждой страны, а также сравнить интересующую страну с выбранными тремя по 40 показателям в онлайн режим.

Например, на рис. 1–4 приведено наглядное сравнение индекса GTI России (41 место из 79) с индексом GTI США (1 место из 79).

Рис. 1. Сравнение GCI России и США за 2019 г. по категории ПОСТАВКА

Рис. 2. Сравнение GCI России и США за 2019 г. по категории ПОТРЕБНОСТЬ

Рис. 3. Сравнение GCI России и США за 2019 г. по категории ОПЫТ

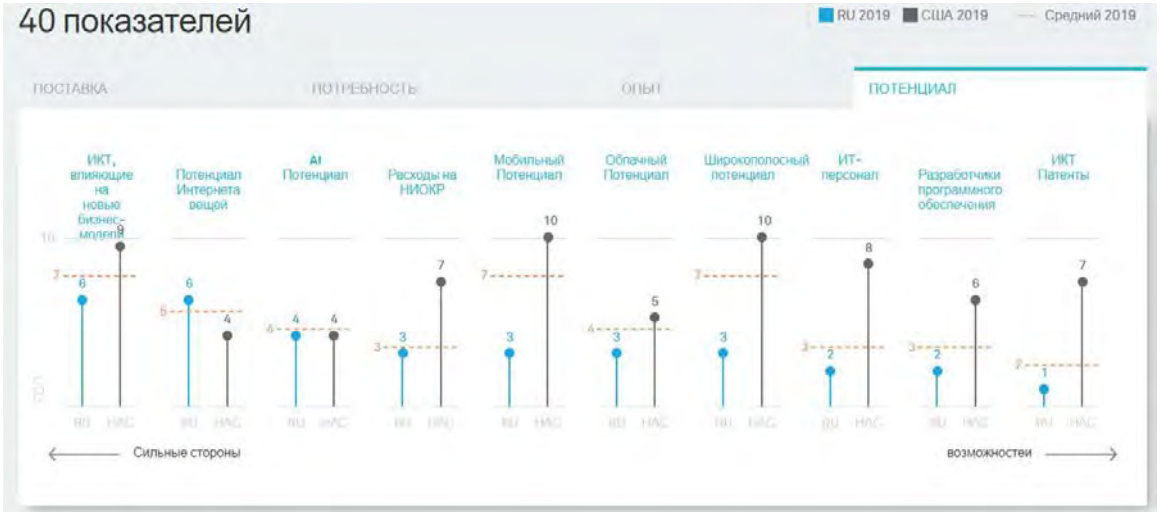


Рис. 4. Сравнение GCI России и США за 2019 г. по категории ПОТЕНЦИАЛ

Глобальный инновационный индекс (GII), структура которого приведена на рис. 5, призван охватить многогранные аспекты инноваций и предоставить инструменты, которые могут помочь в разработке политики, способствующей долгосрочному росту производства, повышению производительности и росту рабочих мест. GII помогает создать среду, в которой постоянно оцениваются инновационные факторы. Он предоставляет ключевой инструмент и обширную базу данных подробных показателей для экономик, которая в 2019 году охватывает 129 стран. Пять входных столбов охватывают элементы национальной экономики, которые обеспечивают инновационную деятельность: (1) институты, (2) человеческий капитал и исследования, (3) инфраструктура, (4) изощренность рынка и (5) изощренность бизнеса. Два столбца результатов отражают фактические результаты инноваций: (6) знания и технологии и (7) творческие результаты [4].

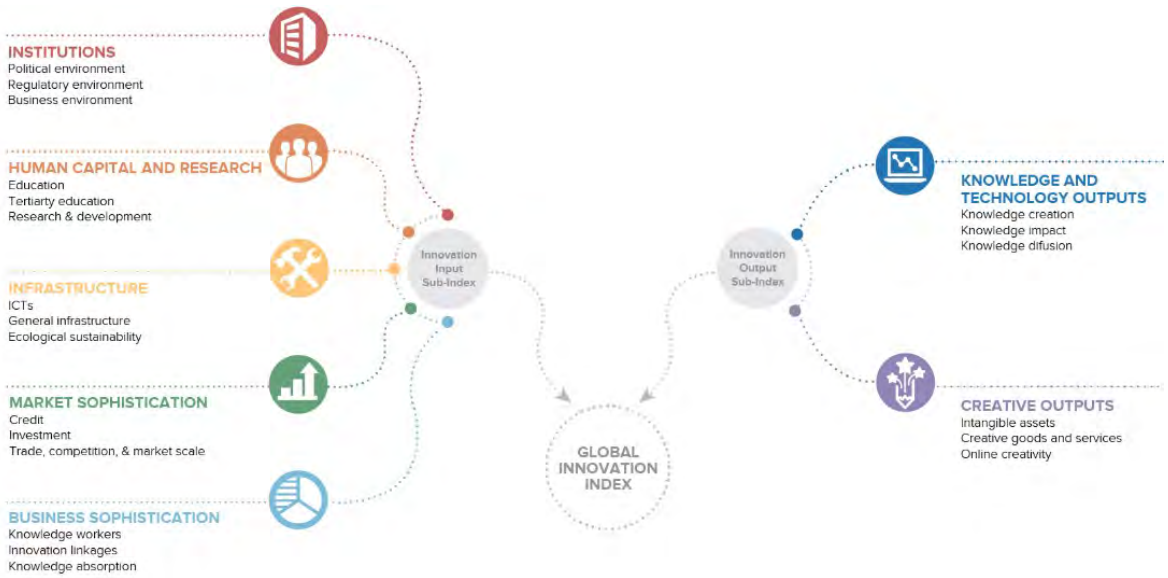


Рис. 5. Структура индекса GII

Россия по индексу GII в 2019 г занимает 29 место, и входит в тройку лидеров среди стран со средним уровнем дохода (Китай, Индия, РФ, Бразилия, Малайзия и пр.)

Рассмотрим на рис. 6 и рис. 7 первую десятку лидеров по GCI и GII за 2019 г.

RANK	ID	COUNTRY	GCI SCORE
1	US	United States	85
2	CH	Switzerland	83
3	SE	Sweden	81
4	SG	Singapore	81
5	DK	Denmark	78
6	JP	Japan	75
7	FI	Finland	75
8	NO	Norway	75
9	GB	United Kingdom	74
10	NL	Netherlands	74

Рис. 6. Десятка лидеров по GCI за 2019 г.

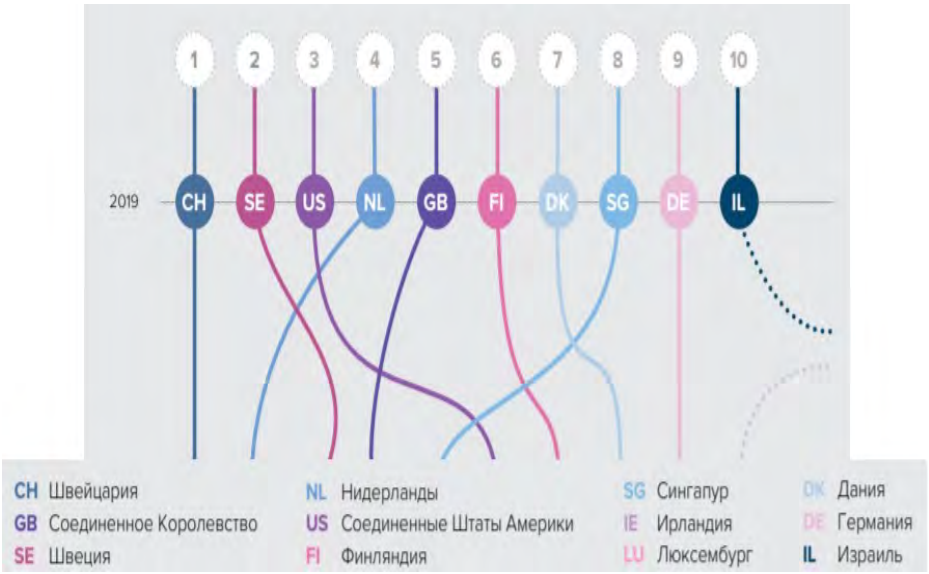


Рис. 7. Десятка лидеров по GII за 2019 г.

Очевидным является то, что состав десятки лидеров по обоим индексам не сильно отличается. Однако, нужно понимать, что страны повышающие

свой рейтинг по GII в перспективе будут подниматься и в рейтинг GCI, ведь реализация инновационного потенциала в современных условиях неизбежно приведет к улучшению интегральных показателей цифровой экономики.

Подробное изучение и сравнительный анализ результатов лидеров со своими собственными показателями индексов GCI и GII позволит Российской Федерации четче ставить целевые показатели и приоритеты в развитии цифровой экономики на ближайшую перспективу.

Список используемых источников

1. Индикаторы цифровой экономики: 2018 [Электронный ресурс]. URL: https://issek.hse.ru/mirror/pubs/ share/222291432. (дата обращения: 30.03.2020).

2. Глобальный индекс связности GCI [Электронный ресурс]. URL: https://www.huawei.com/minisite/gci/en/country-profile-ru.html (дата обращения: 30.03.2020).

3. Атаян А. М., Гурьева Т. Н., Шарабаева Л. Ю. Использование глобального индекса связности для анализа перспектив развития цифровой экономики России // Государство и бизнес. Экосистема цифровой экономики: мат-лы XI междунар. конф. СПб. : РАНХиГС, 2019. С. 94–98.

4. Глобальный инновационный индекс GII [Электронный ресурс]. URL: https://www.globalinnovationindex.org/about-gii#keyfindings (дата обращения: 30.03.2020).

УДК 378.16
ГРНТИ 14.35.07

ТЕНДЕНЦИИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ В ОБРАЗОВАНИИ

Т. А. Блатова, В. В. Макаров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Быстрое развитие цифровых технологий оказывает значительное влияние на отрасли промышленности и служит для обеспечения новых возможностей, снижения затрат и максимизации эффективности. Поскольку сектор образования становится все более конкурентоспособным, цифровая трансформация в настоящее время является необходимым средством выживания вуза, так как новый цифровой мир требует от преподавателей адаптации, принятия цифровых технологий, методологий и умонастроений. Цифровая трансформация в высшей школе оказывает свое влияние на два основных направления информатизации образования. Во-первых, это трансформация

услуг, которая направлена на создание новых образовательных продуктов и преобразование существующих продуктов в цифровые. Кроме того, сюда входит и предоставление цифровых средств связи между учащимися и преподавателями. Во-вторых, это цифровизация всех имеющих место в образовательных учреждениях общих операций, таких как планирование обучения, прием студентов, составление расписания, разработка рабочих учебных программ и обеспечение их качества.

образование, цифровая трансформация, технологии, преподаватели, обучение.

Образование как отрасль социальной сферы является приоритетной отраслью народного хозяйства, занимающей особое место в системе общественного производства. В современном мире образование становится важнейшим фактором, обеспечивающим развитие общества [1]. При этом образование, часто придерживаясь устаревших методов и практик, претерпевает значительные изменения в числе одной из последних отраслей экономики. Но благодаря цифровым преобразованиям и росту образовательных технологий преподаватели начали вносить радикальные изменения в образовательный процесс, причем гораздо более быстрыми темпами, чем ожидалось. Кроме того, «прослеживается явная взаимосвязь между информацией, новыми технологиями и эффективностью обучения с экономическими показателями развития общества» [2].

Можно выделить восемь основных тенденций цифровой трансформации в высшем образовании, основанных на новых технологиях. Менеджеры высшего образования уже сейчас делают серьезные инвестиции в Интернет вещей (IoT). «Умные классы» отслеживают и измеряют производительность и эффективность с помощью различных подключенных устройств IoT (планшеты и электронные книги с образовательным программным обеспечением и приложениями, интеллектуальные доски, и т. д.). Технология дает возможность отслеживания посещаемости студентов. А мозговая активность может быть проанализирована специальным гаджетом, работающим по технологии EEG (electroencephalography), определяющим затраты когнитивной энергии обучаемого. Эта информация может передаваться преподавателю для анализа работы студента на занятии. Кроме того, IoT помогает автоматизировать множество полезных процессов. Например, интеллектуальные термостаты могут сбалансировать температуру внутри здания, а интеллектуальная система освещения позволит значительно сэкономить на оплате электроэнергии. Также на основе интернета вещей могут быть реализованы решения для обеспечения безопасности, включая удаленный мониторинг и биометрическую аутентификацию.

Следующая современная технология – блокчейн. Она используется для хранения и передачи информации распределенным, безопасным и эффективным способом. Образовательные учреждения могут использовать блокчейн для хранения данных учащихся, таких как личные данные и ре-

зультаты обучения. Преимуществом такой технологии, в частности, является безопасность. С помощью блокчейн реально избежать манипуляций с сертификатами, дипломами, научными работами и статьями.

С ростом внедрения ИТ-технологий и устройств Интернета вещей возникла необходимость защитить сеть от киберугроз. Высшие учебные заведения должны внедрить новые инструменты, повышающие кибербезопасность, такие как системы поведенческого анализа (UEBA – User and Entity Behavioral Analytics), который обнаруживает подозрительные действия в типичном поведении пользователей.

Дополненная AR (augmented reality) и виртуальная реальность VR (virtual reality) уже используются для создания более информативных занятий. VR все еще имеет ограничения с точки зрения затрат и контента. AR – более доступная технология, поскольку требуется только мобильный телефон (дополнение к повышению знаний в области медицины, инженерии и т. п.).

Большие данные в образовании – это, в основном, информация о производительности и способностях каждого отдельного студента, которая может улучшить их учебный опыт путем его персонализации. Стремление обеспечить возможность персонализированного обучения является одним из основных драйверов внедрения цифровых технологий в образовании [3]. Новые инструменты и приложения помогают преподавателям настраивать учебные планы для отдельных студентов на основе их сильных и слабых сторон.

В то время как персонализированное обучение фокусируется на потребностях отдельных студентов, большие данные могут помочь преподавателям улучшить занятия в более широком масштабе. Поскольку информация собирается с помощью устройств IoT и интерфейсов AI (artificial intelligence), эти данные могут быть проанализированы, чтобы понять тенденции, демонстрирующие, где учащиеся наиболее вовлечены или области, где могут быть сделаны улучшения. Кроме того, большие данные используются для лучшего анализа учебных программ и являются базой для машинного обучения и искусственного интеллекта.

Искусственный интеллект (ИИ) и его основа, машинное обучение, являются частью глобальной цифровой трансформации. Искусственный интеллект может быть использован в системах управления контентом и обучением для создания дополнительных средств обучения с поддержкой искусственного интеллекта, которые не только генерируют задание учащимся, но и предоставляют им четкое объяснение и пошаговое руководство. Такой подход к обучению повысит эффективность студентов, так как они смогут учиться в любом месте и в любое время.

ИИ может облегчить персонализированное обучение, учитывая потребности каждого студента, чтобы гарантировать обеспеченность необходимым материалом, который нужен для успешного прохождения курса. Это может быть сделано с помощью платформ обучения с поддержкой ИИ (AI-*enabled tutoring)*, которые обеспечивают обратную связь в реальном масштабе времени. Кроме того, ИИ может быть использован для ускорения процесса оценивания выполненных заданий, давая преподавателям больше времени, чтобы сосредоточиться на потребностях студентов. Это привело к созданию смешанных учебных программ, которые сочетают очное обучение с интерактивными мероприятиями, а также к более широкому использованию ИИ в образовании.

Сферой использования ИИ является также университетское обслуживание клиентов, чтобы помочь быстро решить некоторые из более простых вопросов, которые есть у студентов, и уменьшить нагрузку на телефонные линии. Помимо всех преимуществ, которые предлагают чат-боты, их могут использовать те, кто не может общаться по телефону.

Университеты стараются сделать образование доступным для людей с ограниченными возможностями. Университеты внедряют современные технологии, такие как распознавание речи и транскрипция для студентов, которые являются глухими или слабослышащими. ИТ-решения обеспечивают равное и доступное образование для каждого студента. Транскрипция лекций не только помогает студентам с ограниченными возможностями, но и может быть использована другими учащимися для поиска лекций и просмотра их после занятий.

Цифровые технологии радикально меняют содержание преподаваемых дисциплин и форму их подачи, делая возможным прямые подключения к электронным базам данных и использование социальных сетей в проведении практических занятий [4].

Для цифровой трансформации существуют потенциальные проблемы. Во-первых, это нежелание приспосабливаться. Обычно люди неохотно выходят за пределы своей зоны комфорта, что приводит к замедленному росту и прогрессу. При адаптации к новой технологии, культуре или менталитету многие в секторе образования боятся неудачи. Недостаточные знания или навыки в области цифровых технологий также служат определенным препятствием цифровизации образовательного сектора. Для стимулирования инновационной деятельности необходим адекватный уровень доверия, знаний и навыков в масштабах всей организации. Отсутствие направления или стратегии цифровой трансформации является серьезной проблемой, требующей первоочередного решения. Успешная цифровая трансформация в сфере образования предполагает комплексную технологическую, кадровую и бюджетную стратегию. Еще одна неотъемлемая проблема цифровой

трансформации заключается в том, что многие системы, которые используют образовательные учреждения, не совместимы с новыми цифровыми инновациями, необходимыми для их развития.

Любая трансформация – это кардинальное изменение. Разрушить хорошо известные, удобные подходы и заменить их чем-то новым и неизвестным всегда достаточно сложно. Но цифровая трансформация в образовании – это скорее необходимость, чем самоцель. Можно начать с небольших шагов, таких как создание платформы электронного обучения, и перейти к чему-то более сложному, например, IoT и AI.

Новые технологии и новые модели обучения предлагают ранее немыслимые возможности для преподавателей и студентов, но они требуют постоянной ИТ-поддержки. По мере роста ожиданий от новых форм обучения должна также возрастать и способность реагировать на эти потребности.

Список используемых источников

1. Гордеева Д. С. Экономика образования : учебное пособие. Челябинск : Цицеро, 2017. 95 с.

2. Макаров В. В., Блатова Т. А. Инновации в информационно-коммутационных технологиях как атрибут экономики знаний // Информационные технологии и телекоммуникации. 2013. № 4. С. 65–71.

3. Блатова Т. А., Макаров В. В. Персонализированная модель образования на базе технологии цифровых двойников // Национальная концепция качества: государственная и общественная защита прав потребителей. Сборник тезисов докладов международной научно-практической конференции. Под редакцией Е. А. Горбашко. 2019. С. 9–13.

4. Тульчинский Г. Л. Цифровая трансформация образования: вызовы высшей школе // Философские науки. 2017. № 6. С. 121–136.

УДК 336.26; 657. 01
ГРНТИ 06.35

БУХГАЛТЕРСКИЙ УЧЕТ ПРИ ИСПОЛЬЗОВАНИИ BITCOIN КАК ЕДИНОЙ МИРОВОЙ КРИПТОВАЛЮТЫ

Н. Н. Васильева, А. А. Степаненко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Использование криптовалюты BitCoin как единые международные цифровые деньги может обеспечить существенный экономический эффект национальным экономикам и мировой экономике в целом. Объективно возникнут проблемы единого бухгалтерского учета и соответственно в вопросах налогообложения. В отдельных развитых

странах с рыночной экономикой с целью легализации BitCoin и решения вопроса национального бухгалтерского учета и налогообложения в настоящее время этот вопрос постепенно решается. Однако вопросы учета и налогообложения в условиях использования BitCoin как мировых цифровых денег и связанные с этим трудности в настоящее время не рассматриваются. В статье приводятся предложения по преодолению объективных трудностей достижения поставленной цели, что делает такую работу актуальной и своевременной, в том числе для реализации программы «Цифровая экономика РФ». Рассмотрены пути организации бухучета и налогообложения в новых условиях и приводится перечень вопросов, требующих решения в будущем.

бухгалтерский учет, налоги, финансовая система, криптовалюта BitCoin, транзакция, инфокоммуникации, цифровая экономика.

Развитие мировой цивилизации сопровождалось открытиями в различных областях научной или инженерной деятельности людей. Эти открытия давали новые знания, а их реализация на практике часто предлагала огромные преимущества по сравнению с существующей действительностью, принципиально меняя ее. Естественно, что это не могло не затронуть интересы тех, кто профессионально освоили, владели понятными им приемами и навыками и не желали их менять. Поэтому появление и развитие всего нового не проходило без сопротивления консервативных, чаще некомпетентных сил, что создавало трудности их реализации, замедляло, а иногда и откладывало новые возможности на долгие годы. Это замедляло в конечном итоге развитие мировой экономики и рост уровня жизни людей.

При этом важно отметить, что темпы развития цифровых инфокоммуникаций и увеличение скорости распространения новых знаний происходит в геометрической прогрессии, создавая новые блага потребления меньше чем за период жизни одного поколения. Поэтому, своевременность преодоления проблем – актуально.

Использование **BitCoin** как мировых цифровых денег является сложной инновационной задачей и объективно не может проходить без множества проблем, которые необходимо решать [1, 2, 3].

Неизбежные трудности при реализации идеи BitCoin в мировой цифровой экономике можно разделить на следующие основные группы:

1. Организационные, административные.
2. Юридические.
3. Экономические, налогообложение.
4. Образование, обучение.
5. Психологеские.
5. Технические, сети связи.

Среди экономических трудностей – это преобразование электронной финансовой системы, важнейшими направлениями которой являются бухгалтерский учет, аудит и налогообложение [4, 5, 6]. Естественно, что это

многогранная задача и в конечном счете не может быть решена без сочетания с вопросами юридическими [7] и экономической психологи. Поэтому, исследования в данной статье сужены до принципов ведения бухгалтерского учета (БУ) и налогообложения (Н) в электронном виде при условии постепенной замены в обращении фиатных денег на криптовалюту BitCoin.

Кроме того, так как любое государство заинтересовано в росте денежных средств в казне, которая пополняется тем успешнее, при прочих условиях, чем лучше состояние экономики и выше темпы ее роста. В этом случае логична всесторонняя поддержка государства в лице власти любых новаций, которые могут обеспечить этот рост. Практическим действиями в этом направлении в РФ является программа «Цифровая экономика РФ» (ЦЭ) и в ее развитие исследования в области бухгалтерского учета [8]. Однако в работе не рассматривается стратегическое развитие ЦЭ на основе перспективной технологии криптовалюты BitCoin и Blockchain [9]. Необходимость рассмотрения принципа налогообложения доходов в этом случае очевидна.

Известно, что на основе криптовалют транзакции (операция денежного оборота, купля – продажа) исключают в деловой последовательности (цепочке) посреднические услуги [10, 11]. Это позволит существенно сократить издержки обращения, стимулировать экономический рост. Даже на качественном уровне анализа понятно, что внедрение BitCoin как единого мирового платежного средства, позволит снизить расходы бизнеса, существенно снизить потери в экономиках отдельных стран и в мировой экономике. Как следствие – государство сможет собрать больше налогов, Однако, для реализации этой возможности необходимо создать новые принципы учета и налогообложения и научится в новых условиях собирать налоги.

Определение выгоды с целью налогообложения возможно только при определении статуса BitCoin, как нового явления в финансовой сфере, принципиально отличающегося от фиатных денег, даже электронных. С точки зрения теории денег это – самый сложный вопрос. Чем является криптовалюта BitCoin сегодня? Рассматриваются разные представления – финансовым инструментом, товаром, платежным средством, предметом коллекционирования или чем-то другим, что не вписывается в существующую классификацию активов [12, 13]. По мнению Председателя ассоциации «Электронные деньги» Виктора Достова, если BitCoin как актив, например, ценная бумага, платишь налог с курсовой разницы. Если как товар, поменял его на фиатные деньги и платишь налог с продажи.

Преодолеть эту проблему можно постепенно, например, в два этапа.

Первый – промежуточный, когда криптовалюта BitCoin выступает как вид фиатных денег, оцениваемых относительно доллара США. Принцип бухгалтерского учета и налогообложения в этом случае остается традиционным для отдельной страны при конвертации BitCoin в конечном итоге в национальную валюту на рынке Forex.

В настоящее время реальные шаги по налогообложению BitCoin предприняли с США. Ещё в марте 2014 американское налоговое управление (IRS) признала Bitcoin подходящим для целей налогообложения. При этом, криптовалюта рассматривается, как собственность, но не как «валюта».

По закону о налоговой реформе, подписанному президентом США Трампом, все операции с криптовалютами с 1 января 2018 года будут облагаться налогом [CNews]. Будет облагаться налогом во время операции даже обмен одной криптовалюты на другую при получении выгоды. Кроме того, криптовалюты в собственности будут облагаться подоходным налогом после их реализации (от 10 до 37 %) [14].

В 2015 году European Court of Justice, ECJ (Европейский суд) законодательно закрепил налоговые льготы, стимулирующие использование BitCoin в финансовой системе Евросоюза. Операции обмена BitCoin на фиатные валюты освобождаются от НДС. Транзакции в BitCoin были отнесены к платёжным операциям с валютами и не подлежат обложению НДС. ECJ рекомендовал всем странам-членам Евросоюза исключить криптовалюты из числа активов, подлежащих налогообложению [15].

Шведская налоговая служба – Skatteverket определила, что Биткоин является товаром, и все операции с ним должны облагаться НДС. Однако Европейский суд ECJ вынес решение в пользу отмены НДС, которое обязательны теперь для членов ЕС, в том числе Швеции [15].

Опережая полное признание BitCoin в РФ, учитывая растущий интерес к новому платежному средству разработана «Объектная структура данных крипто-валюты Bitcoin в базе данных 1С, демонстрационная версия [16]. Блоки данных, которые содержат транзакции между адресами (кошельками) – это и есть все данные Bitcoin. Конфигурация представляет собой объектную структуру данных Bitcoin. База данных содержит информацию, сформированную на основе данных сети Bitcoin. Предложенная модель БУ отличается от тем, что хеш значение (уникальный секретный код) задается. В действительности это секредный ключ исключающий доступ к базе данных пользователей в сети BitCoin.

Второй – конечный этап, когда BitCoin будет признан как единое мировое платежное средство, единой мировой валютой. В этот период его можно оценить единственным способом, рыночным – на основе спроса и предложения. Психологической базой у пользователей должно быть доверие к новому платежному средству, полученного при согласии всех заинтересованных субъектов рынка. Например, как договаривались в Бретен-Вуде (1963 г.) об отмене золотого стандарта и оценки всех валют относительно доллара США.

Однако для организации бухгалтерского учета (БУ) с целью налогообложения операций с BitCoin потребуется решить вопрос доступа к базе данных транзакций пользователя в его сети. База данных транзакций скрывает необходимую информацию: сумму платежа, место назначения, участников транзакций, время. По мнению авторов [12, 17], даже существующая публичная децентрализованной база данных (бухгалтерская книга) сети BitCoin недостаточно защищена. Применение метода Zerocoin (Miers etЭл., IEEE S&P 2013) решает некоторые из вопросов подмены данных, вывода проводок от источника платежа. Например, позволить пользователю доказать, что он уплатил причитающиеся налоги со всех транзакций, не раскрывая эти транзакции, их суммы или даже сумма уплаченных налогов [18].

Таким образом, в условиях использования криптовалюты BitCoin как единой мировой валюты с функцией платежного средства вопросы организации бухгалтерского учета и налогообложения можно решить в два этапа:

Первый, при использовании BitCoin с ограниченными функциями совместно с фиатными деньгами и валютами. На уровне национальных экономик существующий учет осложнится операциями конвертации.

Второй, как стратегический в части БУ и налогообложения может быть реализован только при выполнении обязательных условий. Учитывая новизну и уже понятные в настоящее время проблемы, необходимо определиться и принять:

– статус BitCoin, с учетом его многофункциональности;

– методику получения доступа к базе данных транзакций (цифровой бухгалтерской книге) налогоплательщика в сети BitCoin для планового контроля;

– универсальное международное законодательство (упрощение процесса учета; процентные ставки; учет транзакций физических и юридических лиц; благотворительность; коэффициенты, учитывающие уровень развития экономик и другие мотивации платить налоги);

– систему и уровень санкций раздельно за сокрытие и за неуплату налогов;

– методологически доступные, просветительские мероприятия для стимулирования и понимания субъектами экономической деятельности важности и необходимости налогообложения.

Список используемых источников

1. Степаненко А. А. Платежное средство BitCoin – как инновационная стратегия изменений финансовой сферы и инфокоммуникаций // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2015. Т. 2. С. 424–429.

2. Андрюшин С. А., Бурлачков В. К. Биткоин, блокчейн, файл-деньги и особенности эволюции денежного механизма // Финансы и кредит. 2017. Т. 23, № 31. С. 1850–1861. https://doi.org/10.24891/fc.23.31.1850

3. Филиппов Е. Криптовалюта от А до Я [Электронный ресурс]. URL: https://golos.io/@investbox/kniga-kriptovalyuta-ot-a-do-ya-evgenii-filippov, 09.03.2018.

4. Починок А. П. Фискал. М : Наталья Починок, 2016. 304 с.

5. Степаненко А. А. Инфокоммуникации и мировая криптовалюта как внедрение инноваций в экономику // Национальная ассоциация ученых. 2014. № 5. Ч. 1. С. 105–106.

6. Налогообложение Биткоин в США, 2018, [Электронный ресурс]. URL: https://roem.ru/27-12-2017/265908/nalog-na-bitcoin/

7. Архипов В. Bitcoin: основные принципы и отдельные юридически-значимые особенности [Электронный ресурс]. URL: http://protokol.com.ua/ru/ bitcoin_osnovnie_printsipi_i_otdelnie_yuridicheski_znachimie_osobennosti, 19.02.2016.

8. Карпова Т. П. Направления развития бухгалтерского учёта в цифровой экономике. СПб. : СПбГЭУ, 2018 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/napravleniya-razvitiya-buhgalterskogo-uchyota-v-tsifrovoy-ekonomike/viewer.

9. BitCoin – электронные деньги будущего, новости и события [Электронный ресурс]. URL: http://bitcoin-info.net, 19.02.2019.

10. Стефанова Н. А., Осипов А. А. Биткоин как инвестиции: преимущества и риски // Карельский научный журнал. 2018. Т. 7. № 1 (22). С. 181–184.

11. Возможности и перспективы развития криптовалют [Электронный ресурс]. URL: www. scienceforum.ru/2015/1053/9732

12. Правовой режим криптовалюты Биткоин как товара [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Правовой_режим_криптовалют.

13. Многогранная природа Биткоин. [Электронный ресурс]. URL: https://forklog.com/priroda-bitkoina-aktiv-valyuta-tovar-ili-predmet-kollektsionirovaniya/

14. Рецепт налогообложения биткоина от США / TAX-TODAY.COM – налогообложение, Загл. с экрана. – 03.06.2019.

15. Обмен традиционных валют на виртуальную валюту «Биткойн» освобождается от НДС // Пресс-релиз Европейского суда. № 128/15 от 22 октября 2015 (англ.).

16. Объектная структура данных крипто-валюты Bitcoin в базе данных 1С [Электронный ресурс]. URL: https://infostart.ru/public/824120/, 2019.

17. Фергал Рейд, Харриган Мартин. Анализ анонимности в системе Биткойн // 3-я Международная конференция IEEE по вопросам конфиденциальности, безопасности, риска и доверия, а также по социальным вычислениям, SocialCom / PASSAT '11, 2011. С. 1318–1326.

18. Zerocoin (Miers etal., IEEE S&P 2013), Decentralized Anonymous Payments from Bitcoin [Электронный ресурс]. URL: http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf, 10.02.2020.

УДК 334.752
ГРНТИ 82.33.13

ПЕРСПЕКТИВНЫЕ ВАРИАНТЫ ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ УЧАСТНИКОВ ПРОЕКТОВ ВНЕДРЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ

С. Ю. Верединский, В. В. Макаров, Д. О. Стародубов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Внедрение цифровых технологий в отрасли экономики направлено на создание принципиально новых условий их функционирования, при которых становится возможным достижение «прорывных» технологических, организационных и экономических результатов функционирования как отдельных предприятий, так и целых отраслей. Современные условия хозяйствования предприятий реального сектора экономики вынуждают инициаторов проектов внедрения цифровых технологий как совершенствовать существующие способы организации взаимодействия участников проектов, так и разрабатывать новые, ранее не используемые. Примером может служить развитие теории и практики применения так называемых «энергосервисных контрактов», нормативно-правовое и организационно-экономическое содержание которых вполне пригодно для разработки организационно-экономической основы инновационных проектов в сфере внедрения цифровых технологий. Также могут использоваться механизмы взаимодействия, основанные на лизинговых схемах. Такие организационно-экономические механизмы особенно эффективны в условиях недостаточной текущей платежеспособности реципиентов инновационных решений в виде цифровых технологий.

инновации, цифровые технологии, инновационные проекты.

Проект внедрения инновационных разработок, систем и комплексных решений предполагает последовательное выполнение следующих этапов (рис.).

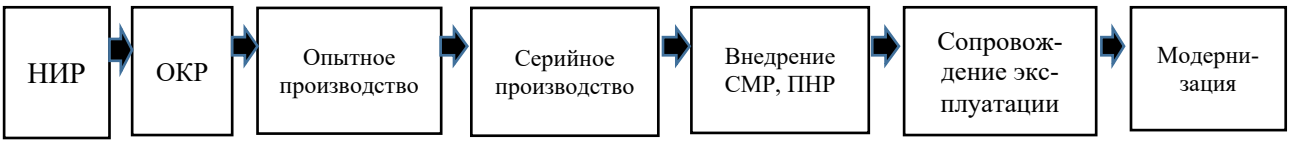


Рис. Этапы разработки

Каждый из этапов проекта (процесса) внедрения инновационных продуктов и услуг может быть реализован разными способами. Компания, реализующая проект, может каждый из этапов выполнять либо сама, либо посредством привлечения организаций-партнеров, имеющих разный статус

в проекте. Одних партнеров компания может привлекать на основе заключения с ними договоров поставки, других – выполнения подрядных работ и т. п. При этом компания не связана с такими партнерами обязательствами раздела прибыли с ними. С другими партнерами компания может выстраивать отношения на принципиально иных условиях, подразумевающих совместное несение затрат, а также долевое участие в прибыли от реализации проекта. Традиционной формой для таких отношений является заключение договора о совместной деятельности, при котором балансодержателем такого договора становится сама компания-инициатор проекта.

Возможны варианты реализации проекта внедрения инновационных разработок, систем и комплексных решений, при которых отдельные этапы проекта реализуются самим заказчиком проекта – фактическим реципиентом инноваций. Такие варианты возможны, когда компания, отвечающая за проект целиком, реализует не все его этапы, а только те, в которых у заказчика (реципиента инноваций) есть необходимость. В состав выполняемых работ и в комплект поставляемого (монтируемого) оборудования, вводимого в эксплуатацию, по такому «усеченному» (с точки зрения всего объема работ и комплектности оборудования) варианту реализации проекта, войдут только те работы и комплектующие, за которые заказчик заплатит. В случае, если существенную часть работ по такому проекту, а также фактическое производство существенной доли оборудования заказчик выполняет сам, то для него экономическая сущность реализуемого таким образом проекта (развития) будет соответствовать схеме, традиционно называемой «хозспособом». В этом случае компания-поставщик выполнит только некоторую часть работ по проекту и обеспечит комплектацию теми аппаратно-программными средствами, которые заказчик либо не будет в состоянии произвести самостоятельно, либо посчитает такой способ более привлекательным для себя с экономической точки зрения.

Таким образом, процесс реализации инновационного проекта может быть осуществлен любым из принципиально возможных способов, каждый из которых представляет собой комбинацию вариантов выполнения каждого этапа посредством: силами и средствами компании-поставщика инновационного решения; партнера компании-поставщика по совместной деятельности; поставщика в лице третьего лица; подрядной организации – третьего лица; реципиента инновационного решения.

Конкретный вариант реализации проекта внедрения инновационного решения представляет собой результат выбора, осуществляемого совместно заказчиком и поставщиком инновационного решения. При таком варианте компания-поставщик инновационного решения реализует такие этапы, как: выполнение НИР и ОКР; непосредственное внедрение, включая выполнение строительно-монтажных и пуско-наладочных работ; модернизацию

системы (предусмотренную договором). Прочие этапы компания-поставщик инновационного решения «передает» на аутсорсинг третьим лицам. Очевидно, что такая «передача» возможна только в том случае, если это заранее оговорено и одобрено заказчиком. Целесообразность «передачи» части функций может быть обусловлена как технологическими возможностями, так и экономическими причинами – более низкими издержками при такой организации выполнения работ по проекту. Необходимо отметить, что экономические мотивы далеко не всегда являются самыми существенными. Часто более существенным фактором является надежность поставок и качество выполнения работ.

На формирование финансовых решений компании-заказчика существенное влияние оказывает не только факт наличия финансовых ресурсов на момент реализации проекта, но также содержание тех полезных для него эффектов, на достижение которых и направлен реализуемый проект. Суть таких полезных для заказчика-реципиента инноваций эффектов может состоять в следующем:

1) в снижении «чистой технологической себестоимости» выпускаемой им продукции (услуг) за счет: сокращения длительности производственно-технологического цикла; снижения норм расходования сырья, материалов, энергии и других ресурсов на производство;

2) в повышении доходов и прибыли за счет: повышения производительности труда; увеличения объемов выпускаемой продукции вследствие эффективной ценовой политики и/ или роста качества продукции;

3) в сокращении общепроизводственных и общехозяйственных расходов за счет перепроектирования бизнес-процессов и оптимизации структуры расходов организации.

При этом важным для выработки финансовой схемы реализации проекта оказывается не только суть получаемого заказчиком-реципиентом инноваций эффекта или эффектов, но также и их численная характеристика, а также временной период, в котором полезный эффект (эффекты) будет фактически материализован. В условиях снижения уровня платежеспособности потенциальных клиентов компании целесообразно рассматривать такие инструменты продвижения инновационной продукции, которые способны стимулировать спрос.

Хозяйственная практика свидетельствует в пользу применения таких традиционных инструментов финансирования поставок технологической продукции, как лизинг и отсрочка платежа. Каждый из этих инструментов имеет как свои преимущества по отношению к другому, так и недостатки. Лизинговая схема предполагает включение в проект дополнительного участника в лице лизинговой компании, которая, как правило, является либо дочерней, либо аффилированной банковской структурой. Считается, что лизинговая схема позволяет получить дополнительную экономию на налогах.

На практике это реализуется далеко не всегда. Неоспоримым достоинством лизинговой схемы является сама возможность финансирования проекта в условиях отсутствия средств у заказчика. Отсрочка платежа представляется менее предпочтительной для компании-поставщика инновационного решения, поскольку финансовая нагрузка в смысле графика финансирования проекта ложится полностью на нее. Неполученные своевременно денежные средства также можно рассматривать как базу для расчета упущенной выгоды, которую рассчитывают путем умножения этих денежных средств на усредненный депозитный процент. Кроме того, финансирование проекта компанией-поставщиком инновационного решения за счет собственных средств или, тем более, за счет привлекаемых дополнительно кредитных ресурсов, приводит к резкому росту совокупного риска такого проекта. Однако лизинговая схема может оказаться неприемлемой для заказчика-реципиента инноваций, так как заказчик часто не готов принять на себя дополнительный риск в виде лизинговых платежей, поэтому ее реализуемость всегда находится под большим вопросом.

В последнее время активный интерес у практиков вызывают так называемые «энергосервисные контракты», а также различные их вариации, которые иногда называют «квазиэнергосервисными» [1]. Их экономическая сущность состоит в том, что заказчик расплачивается с поставщиком инноваций из средств, формирующихся в результате экономии ресурсов (электроэнергии), образующейся в результате внедрения инновационного решения. При этом заранее оговариваются: процент экономии, выплачиваемый поставщику инновационного решения; длительность периода времени, в течение которого осуществляются платежи; механизм расчета экономии, основанный на технической возможности количественного измерения уровня потребления соответствующего ресурса (электроэнергии, газа, горячей/холодной воды) [2]. Некоторые компании пытаются внедрять подобные финансовые схемы в других отраслях. Однако на сегодняшний день такая практика мало изучена и практически никак не освещена в открытых источниках информации. Тем не менее данное направление исследований представляется вполне перспективным для разработки практического инструментария.

Целесообразно выделить перечень вопросов, ответы на которые позволят идентифицировать суть конкретного варианта взаимоотношений между такими ключевыми участниками проекта внедрения инновационной продукции, как поставщик инновационного решения и заказчик-реципиент инноваций:

1) На достижение какого экономического эффекта (эффектов) направлена реализация инновационного проекта?

2) Какие (основные) этапы инновационного цикла реализуются в конкретном инновационном проекте? Какие из них реализуются непосредственно компанией-поставщиком инновационного решения? Если какие-то процессы «передаются» на аутсорсинг, то вследствие каких причин? Есть ли этапы инновационного цикла, которые реализуются самим заказчиком?

3) Какие «обеспечивающие» процессы включены в состав инновационного проекта? Кто их реализует?

В качестве ключевых участников инновационного проекта уже были названы компания-поставщик инновационного решения и заказчик-реципиент инноваций. В случае, если компания-поставщик инновационного решения реализует проект на основе заключенного ею договора о совместной деятельности с третьим лицом, то такое третье лицо также следует рассматривать в качестве одного из ключевых участников проекта.

В качестве нормативно-правовой основы механизма реализации инновационного проекта может выступать комбинация договоров поставки (нового технологического оборудования) и договора о совместной деятельности (простого товарищества). Сочетание таких договоров позволяет реализовать распределение общего дохода от реализуемого проекта (и прибыли) [3]. В качестве еще одного варианта предлагается комбинация договоров о совместной деятельности (простого товарищества) и договора аренды с правом выкупа.

Применение представленного подхода позволит детально структурировать инновационные проекты. Практическая полезность данного подхода тем выше, чем сложнее структура планируемых к реализации инновационных проектов, чем больше количество потенциальных участников, чем разнообразнее полезные эффекты, на достижение которых направлены инновационные проекты [4].

Список используемых источников

1. Назарова Л. Е. Анализ опыта применения энергосервисных контрактов в России // Журнал «Дайджест-финансы». 2017. Т. 22. № 1 (241). С. 50–61.

2. Нефедов В. А. Энергосервисная деятельность: существующие проблемы и некоторые одели организации финансирования // Вестник Томского государственного университета. 2015. № 400. С. 238–244.

3. Макаров В. В., Шувал-Сергеева Н. С. Выбор источника финансирования инновации на разных этапах ее жизненного цикла: объем финансирования и качество инновации // Вопросы радиоэлектроники. 2016. № 1. С. 78–80.

4. Алексеев А. Л., Блатова Т. А., Макаров В. В., Шувал-Сергеева Н. С. Современные тенденции в управлении инновационным развитием отраслей промышленности для обеспечения качества и конкурентоспособности продукции // Вопросы радиоэлектроники. 2016. № 11. С. 66–71.

УДК 659.1
ГРНТИ 19.01.29

ИЛЛЮЗИИ В ДИЗАЙНЕ НАРУЖНОЙ РЕКЛАМЫ

Е. В. Гунина, С. В. Иванова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье приведен анализ примеров оптических иллюзий движения в рекламе. Актуальность и практический аспект выбранной темы определяется рядом ключевых проблем, связанных с актуальностью и эффективностью использования нового подхода в рекламной сфере для увеличения внимания и интереса к рекламе, а также повышения продаж рекламируемых продуктов. Рассмотрена возможность применения новых приемов визуальных решений в процессе создания рекламных баннеров. На примере известных рекламных кампаний представлены приемы создания движения оптических иллюзий.

цвет, иллюзия, реклама, полиграфия, дизайн, изображения, иллюзия движения.

Актуальность проведенного исследования обусловлена становлением рекламы как одного из аспектов современной жизни человека. На данный момент реклама прочно заняла ведущие позиции и выходит на первый план как явление экономическое, информационно-коммуникативное, общекультурное. Негативным фактором распространения такого объема рекламы становится перенасыщение рынка, в связи с чем необходимо проводить постоянные исследования и искать свежие, новые, необычные и нетипичные способы рекламирования, расширения методов продвижения товаров и услуг. Создание уникальной, привлекающей внимание потребителей рекламы становится все более трудным процессом. Рекламный рынок нуждается в более новых и усовершенствованных примерах. Одним из подобных примеров постепенно становятся крайне интересные формы культурной деятельности мира – иллюзии.

Цель работы: анализ применения иллюзий в рекламе и на его основе создание собственного рекламного баннера.

Задачи:

1. Изучение соответствующей теме литературы.
2. Классификация различных видов оптических иллюзий.
3. Выбор наиболее подходящего варианта иллюзии как основы собственного рекламного баннера.
4. На основе подходящего варианта иллюзии создать собственный рекламный баннер.
5. Обобщение и анализ полученных результатов.

Визуальные противоречия уже не первое столетие очаровывают и захватывают людей. Систематические исследования феномена оптических иллюзий начались еще в середине XIX века, однако до сих пор профессионалы не могут объяснить, как многие из них «работают».

Зрительные иллюзии – (обманы зрения), систематические ошибки зрительного восприятия, а также различные искусственно создаваемые зрительные эффекты и виртуальные образы, основанные на использовании особенностей зрительных механизмов [1, 2].

Выделяют несколько распространенных типов иллюзий [3]: иллюзии восприятия размера, искажения геометрии фигур, иллюзии цвета и контраста, иллюзии движения, двойственное изображение, иллюзии соотношения фигуры и фона, иллюзии кажущихся, несуществующих фигур, иллюзии восприятия глубины, иллюзии невозможной фигуры, иллюзии перевёрнутой картинки, эффект перцептивной готовности, парейдолические иллюзии, иллюзия следящего взгляда, иллюзии распознавания образов.

Из вышеперечисленных видов иллюзий наиболее сильно привлекает внимание зрителя иллюзия движения. Учеными доказано, что все неожиданно появляющееся в поле зрения человека способно невольно привлечь его внимание. Например, при интенсивной умственной работе человеку может сильно помешать качающаяся лампа: глаза поневоле фиксируют это движение [1].

Иллюзия движения подразделяется на:

1. Иллюзию вращения и кручения кругов (рис. 1).

Иллюзию вращения кругов взяли на вооружение маркетологи из Shell [4], таким образом, они хотели показать, что компания готова поддерживать шестерёнки в действии, а благодаря магии оптических иллюзий, удалось достичь движения даже на полностью статических печатных страницах.

Принт наглядно иллюстрирует слоган: «Поддерживаем шестеренки в движении».

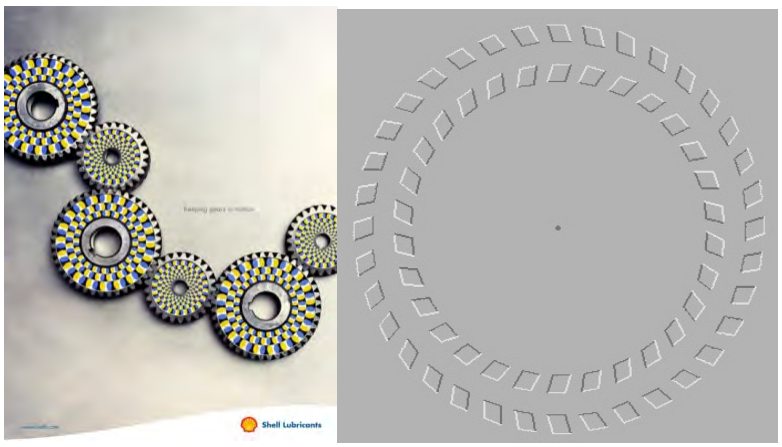


Рис. 1. Реклама компании Shell и иллюзия кручения кругов

2. Иллюзию волн (иллюзия Геринга).

На человека значительное воздействие оказывает иллюзия Геринга, использовалась в логотипе Sonos (рис. 2), представляющая собой муаровый узор, где сетки накладываются друг на друга, порождая ложные движения.

Рис. 2. Логотип Sonos

3. Иллюзию движения по коридору. Если сосредоточить взгляд в центр картинки, то через некоторое время движение останавливается. На данный момент в рекламе не использовалась.

Аналогом иллюзии движения по коридору является фрактальная пульсирующая иллюзия. При рассмотрении картинки заметны пульсирующие изменения в ее форме. Оба вида иллюзий представлены на рис. 3.

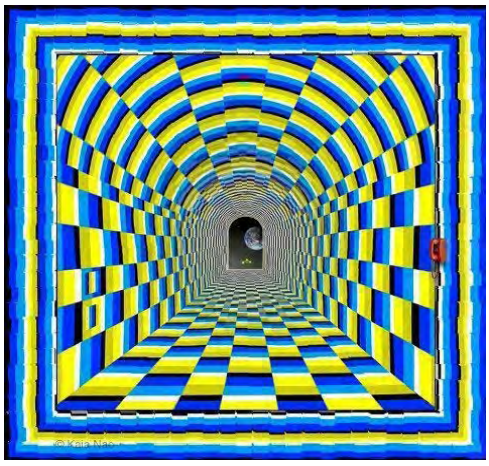
а)  б) 

Рис. 3. Иллюзия движения по коридору (а), фрактальная пульсирующая иллюзия (б)

4. Иллюзию расширения кругов (рис. 4), при сосредоточении взгляда в центре картинки и осуществлении движений головой вперед и назад, будут заметны расширения и сужения кругов, а также изменение цветовых вариаций.

Рис. 4. Иллюзия расширения кругов

5. Иллюзию исчезновения.

Реклама пятновыводителя Hygiene [5] была размещена на остановках Бангкока (Тайланд). Издалека на свитере видно пятно, которое исчезает прямо на глазах по мере приближения к билборду (рис. 5).

Рис. 5. Реклама пятновыводителя Hygiene

В новой рекламной кампании IKEA [6] обещает раскрасить серые бельгийские будни разноцветными товарами для дома (рис. 6). Чтобы рассказать об этом покупателям, рекламное агентство подготовило серию плакатов, которые издалека выглядят как простые цветные прямоугольники с названием товара и ценой, но при приближении человек распознает объект на картинке.

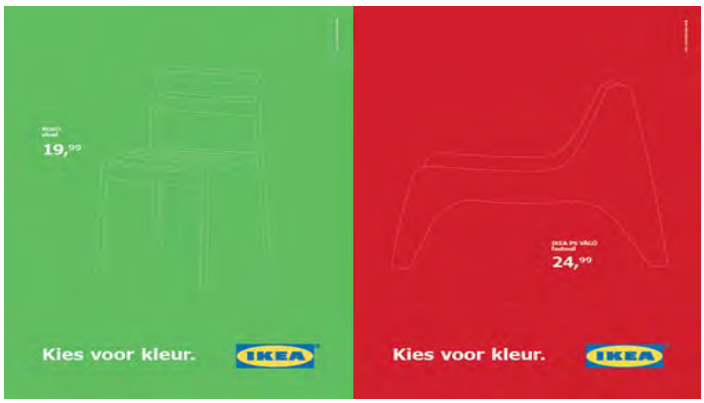


Рис. 6. Реклама IKEA

При создании плакатов были использованы технологии, позволяющие показать контуры товара только тем, кто подошел к плакату поближе. По задумке авторов, реклама должна подстегнуть людей к решительным действиям. Кампания стартовала накануне пасхальных каникул, во время которых намного проще найти время на обустройство дома.

Рассмотрев некоторые виды иллюзий и увидев конкретные примеры их применения в рекламе известных брендов, можно заметить, что из 6 видов иллюзий в рекламе применяются всего 3, то есть только 50 %. Поэтому следует отметить, что возможности применения иллюзий в рекламе на данный момент используются не полностью.

Приведенные иллюзии можно применить и для создания собственного рекламного баннера, например, рекламы компании по ремонту квартир, в том числе по отделки стен (рис. 7). Конкретный пример рекламы, где валики движутся, символизирует полноценный процесс работы.

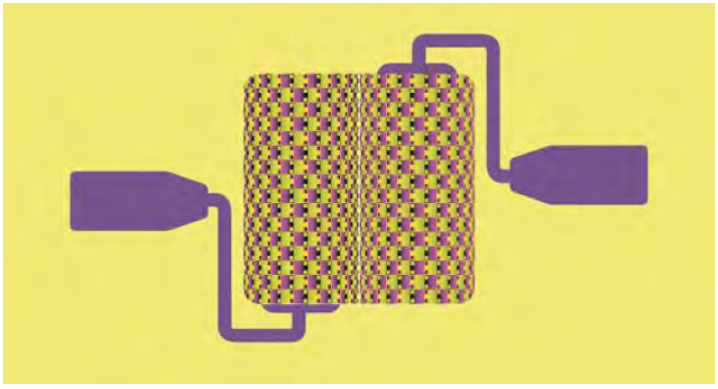


Рис. 7. Рекламный баннер компании по ремонту

Данная реклама не нагромождена лишними элементами, но в свою очередь, привлекает внимание крутящимися элементами. Самое главное поместить эту рекламу на большой баннер, так как в маленьком формате иллюзия не раскрывает своих свойств.

В заключении, на основе проведенного исследования, несмотря на то, что оптические иллюзии уже находят свое применение в сфере рекламы, существует еще большая нераскрытая перспектива их использования в рекламе полиграфической продукции. Отличительной чертой иллюзий является их необычность, которая значительно сильнее привлекает внимание потребителей. Именно такая особенность человеческого мозга, как запоминание нестандартных рекламных кейсов, заставит в будущем маркетологов широко применять данную технику иллюзий в своих рекламных проектах. При этом рассмотренные в данные статье являются лишь небольшой частью всего набора существующих иллюзий, что открывает огромные перспективы их использования в сфере рекламного бизнеса.

Список используемых источников

1. Артамонов И. Иллюзии зрения. М. : Наука, 1964. 112 с.
2. Толанский С. Оптические иллюзии. М. : Мир, 1967. 128 с.
3. Джанни А. Сарконе, Мари-Джо Ваэбер. Рисуем оптические иллюзии. М. : Арт-Родник, 2013. 128 с.
4. Оптические иллюзии в рекламе: как запомниться каждому [Электронный ресурс]. URL: https://read.kj.media/trends/opticheskie-illyuzii-v-reklame-kak-zapomnitsya-kazhdomu/ (дата обращения: 18.02.2020).
5. Оптическая иллюзия в рекламе [Электронный ресурс]. URL: http://promoatlas.ru/opticheskaya-illyuziya-v-reklame/ (дата обращения: 01.02.2020).
6. IKEA использовала в рекламе оптические иллюзии [Электронный ресурс]. URL: http://www.lookatme.ru/mag/live/experience-news/202953-illusion (дата обращения: 15.02.2020).

УДК 004.77
ГРНТИ 20.49.37

РАЗРАБОТКА СТРАТЕГИИ РАЗВИТИЯ ИМПОРТОЗАМЕЩЕНИЯ ВЫСОКОТЕХНОЛОГИЧНОЙ ПРОДУКЦИИ В РФ

Ю. А. Дуболазова, Е. А. Конников, В. В. Макаров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Эффективное функционирование предприятия также является составной частью экономической модели промышленной политики, направленной на защиту внутреннего производителя – то есть политики импортозамещения. При этом замещение импорта промышленных продуктов собственным производством является программой инновационного развития для отечественных предприятий, т.к. замещаемые продукты для предприятий – производителей являются новыми. Критерием экономической эффективности инновационного процесса на предприятии автор предлагает считать эластичность издержек производства продуктов относительно экономии капитальных вложений – коэффициент эластичности издержек производства относительно капитальных вложений меньше единицы.

импортозамещение, эндогенные переменные, экзогенные переменные, высокотехнологичные товары, экспорт, импорт.

В настоящее время тема импортозамещения стала одной из самых обсуждаемых. Драйвером реализации политики импортозамещения стали серьезное обострение международной обстановки и ухудшение экономических отношений со многими зарубежными странами. В связи с этим Правительством РФ было принято решение о создании конкурентоспособного внутреннего производства, способного заменить импортные товары на российском рынке и таким образом сделать экономику менее зависимой от внешних отрицательных воздействий. Изначально воспринимавшееся как одна из необходимых мер для сглаживания негативных конъюнктурных изменений, импортозамещение вскоре стало одной из наиболее приоритетных государственных задач. Внедрение этой политики проводится практически во всех отраслях экономики, в том числе и в высокотехнологичных отраслях промышленности, благодаря чему обеспечивается технологическая независимость и технологическая безопасность.

Теоретической и методологической базой при анализе текущего состояния высокотехнологичных и наукоемких отраслей промышленности, целесообразности государственных мер, а также принятых стратегий развития импортозамещения высокотехнологичной продукции послужили научная

и учебно-методическая литература, статьи в периодических изданиях и нормативно-законодательные акты Российской Федерации.

По результатам анализа были выделены следующие переменные:

Эндогенные переменные:

Y_t^1 – объем производства высокотехнологичных товаров в году *t* (млн рублей);

Y_t^2 – суммарный экспорт высокотехнологичных товаров в году *t* (млн долл. США);

Y_t^3 – суммарный импорт высокотехнологичных товаров в году *t* (млн долл. США);

y_t^4 – выплаты по лицензионным соглашениям с зарубежными странами и роялти (млн долл. США).

Экзогенные переменные, влияющие на каждую эндогенную:

$X_{1,t}^1$ – ВВП на душу населения в году *t* (долл. США);

$X_{2,t}^1$ – число научно-технических статей в году *t* (единиц);

$X_{3,t}^1$ – число исследователей НИОКР в году *t* (на млн человек);

$X_{4,t}^1$ – число патентных заявок резидентов (единиц);

$X_{5,t}^1$ – число организаций, выполнявших научные исследования и разработки (единиц);

$X_{6,t}^1$ – финансирование науки из средств федерального бюджета (млн рублей);

$X_{7,t}^1$ – средняя заработная плата в высокотехнологичных отраслях промышленности (долл. США в год);

$X_{1,t}^2$ – затраты на научные исследования и разработки в году *t* (в % от ВВП);

$X_{2,t}^2$ – глобальный инновационный индекс GII в году *t*;

$X_{3,t}^2$ – поступления по лицензионным соглашениям с зарубежными странами и роялти (млн долл. США);

$X_{4,t}^2$ – чистый приток прямых иностранных инвестиций в Россию (в % от ВВП);

$X_{5,t}^2$ – инвестиции в нематериальные активы (млн рублей);

$X_{1,t}^3$ – среднегодовой курс доллара к рублю;

$X_{2,t}^3$ – среднедушевые денежные доходы (руб.);

$X_{3,t}^3$ – индекс промышленного производства электрооборудования, электронного и оптического оборудования (в % к предыдущему году);

$X_{4,t}^3$ – среднегодовая численность работников организаций по производству электрооборудования, электронного и оптического оборудования (тысяч человек);

$X_{5,t}^3$ – индекс цен производителей электрооборудования, электронного и оптического оборудования;

$X_{6,t}^{3}$ – число предприятий и организаций по производству электрооборудования, электронного и оптического оборудования (единиц);

$X_{1,t}^{4}$ – специалисты с высшим образованием в России (% от общей численности населения);

$X_{2,t}^{4}$ – доля продукции высокотехнологичных и наукоемких отраслей в валовом внутреннем продукте (в процентах);

$X_{3,t}^{4}$ – выдано патентов на изобретение (единиц);

$X_{4,t}^{4}$ – численность занятых в высокотехнологичном секторе (человек).

Были проанализированы статистические данные за период с 2001 по 2018 год [1]. Регрессионный анализ, с последующим исключением незначимых переменных позволил сформировать следящую систему уравнений:

$$\begin{cases} y_t^1 = 200739{,}35 + 24{,}65 \cdot x_{1,t}^1 - 8307{,}61 \cdot x_{3,t}^1 - 12298{,}12 \cdot x_{5,t}^1 + 50{,}14 \cdot x_{6,t}^1 \\ y_t^2 = 1915{,}89 + 0{,}13 \cdot x_{2t}^2 \\ y_t^3 = -972{,}38 + 3{,}42 \cdot x_{1t}^3 + 0{,}01 \cdot x_{2t}^3 \\ y_t^4 = 72{,}44 + 93{,}71 \cdot x_{2t}^4 + 146{,}51 \cdot t \end{cases}$$

Таким образом, драйверами развития высокотехнологичной промышленности РФ являются: число научно-технических статей; среднедушевые денежные доходы, инвестиции в нематериальные активы, ВВП на душу населения; чистый приток прямых иностранных инвестиций в Россию (в % от ВВП) [2]. Именно для данных переменных предложен ряд рекомендаций по разработке государством мер, направленных на их увеличение с целью последующей оптимизации программ импортозамещения в РФ инновационного и наукоёмкого производства, а именно:

– оказание поддержки участия молодых ученых в крупных международных конференциях, по итогам которых могут быть изданы их научные труды;

– создание системы финансовой поддержки российских научных статей, созданных по результатам научно-исследовательских проектов на средства из государственного бюджета, и публикуемых в высокорейтинговых международных журналах;

– создание на базе высших учебных заведений и научных организаций сеть центров повышения квалификации научных и научно-педагогических работников по развитию компетенций работы с информационными ресурсами в базах данных Web of Science и Scopus;

– создание центров языковой подготовки, где российские ученые будут учиться писать научные статьи на английском языке для международных научных журналов [3];

– создание конкурентоспособных рентабельных производств, обеспечивающих высокий уровень оплаты труда;

– снижение уровня издержек в производстве на основе применения оптимальных технико-технологических решений;

– увеличение объемов продаж вследствие роста уровня конкурентоспособности [4];

– снижение налогового бремени для предприятий, ведущих НИОКР;

– разработка систему нематериальных стимулов для занятия научно-исследовательской деятельностью крупными российскими компаниями;

– государственная финансовая поддержка малых инновационных предприятий на приобретение инвестиций в нематериальные активы;

– использование специальной системы налоговых стимулов к вложению бизнесом финансовых средств в инновационные проекты (ускоренная амортизация, налоговые льготы на инвестиции в нематериальные активы, на инвестирование венчурного капитала в инновационную деятельность) [5];

– внедрение мер по упрощению административных барьеров при открытии инновационноёмких предприятий и реализации инвестиционных проектов [6];

– создание особых экономических зон и территорий опережающего развития действительно может стать эффективным инструментом привлечения инвестиций в Россию [7].

Список используемых источников

1. Российские исследователи будут учиться писать статьи в мировые журналы // РИА Новости. URL: https://ria.ru/science/20130227/924965146.html (дата обращения: 04.12.2018).

2. Прохоров А. Ю. Перспективы привлечения инвестиций в нематериальные активы // Вектор науки ТГУ. 2012. № 3. С. 55–57. URL: http://edu.tltsu.ru/sites/sites_content/site1238/html/media70428/14_proxor.pdf (дата обращения: 05.12.2018).

3. Патрикеева В. Е. Привлечение инвестиций в условиях санкций // Научно-исследовательские публикации. Воронеж : Вэлборн, 2015. С. 55–68.

4. Родионов Д. Г., Рудская И. А. Региональные инновационные системы, их роль и место в формах инновационной кооперации // Финансовые решения XXI века: теория и практика: сб. науч. тр. 16-й Международной научно-практической конференции. Санкт-Петербургский политехнический университет Петра Великого. СПб. : СПбПУ, 2015. С. 157–164.

5. Родионов Д. Г., Кошман А. В., Моттаева А. Б. Методический подход к оценке влияния инновационной активности хозяйствующего субъекта нефтегазового комплекса на стоимость бизнеса // Вестник Алтайской академии экономики и права. 2019. № 2–2. С. 319–325.

6. Сомов А. Г., Дуболазов В. А. Исследование зарубежных рынков инновационных продуктов с использованием теории нечетких множеств и нейронных сетей // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. 2019. Т. 12. № 1. С. 191–200.

7. Макаров В. В., Шувал-Сергеева Н. С. Оценка экономической эффективности инвестиций в инновационные проекты с учетом нематериальных активов // Вопросы радиоэлектроники. 2015. № 4. С. 193–198.

УДК 004.77
ГРНТИ 20.49.37

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ОПТИМИЗАЦИИ ПРОЦЕССА ОБУЧЕНИЯ АНАЛИТИКОВ ERP-СИСТЕМ

Ю. А. Дуболазова, В. В. Макаров, А. Д. Окатьева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Для эффективного управления предприятием необходима информационная поддержка процессов управления для своевременного принятия управленческих решений. В конфигурации «1С: ERP Управление предприятием 2» есть инструменты, позволяющие выводить информацию в визуальном представлении в виде наглядных графиков и диаграмм, что позволяет быстро проводить анализ текущих показателей и факторов, влияющих на хозяйственную деятельность предприятия, своевременно и быстро принимать управленческие решения. Но также существуют проблемы: высокая стоимость обучения с профессионалом, разрозненная структура данных для самостоятельного изучения, слишком большой объём информации, нацеленной на средний уровень подготовки специалиста.

ERP-система, корпоративная информационная система, автоматизированная система управления предприятием, программное обеспечение, информационные технологии, аналитика, аналитик ERP, система обучения, оптимизация, систематизация, повышение эффективности.

В статье будут разобраны вопросы актуальности профессии аналитика ERP-систем, проблем процесса обучения стажёров использованию программы и внедрения информационных технологий для их решения.

Планирование ресурсов предприятия (ERP) – это специальное программное обеспечение, предназначенное для управления бизнес-процессами с целью автоматизации многих функций бэк-офиса, связанных с технологиями, услугами и человеческими ресурсами, с помощью использования системы интегрированных приложений [1].

Бэк-офис – это структурное подразделение организации, которое занимается ведением бизнес-процессов, стремясь к повышению производитель-

ности с помощью оптимизации потоков рабочих операций, устранения неэффективных «ручных» операций на протяжении всего жизненного цикла бизнес-процесса [2].

Структура стандартной ERP-системы включает в себя множество элементов, как видно на рис. 1 [3], что позволяет оптимизировать бизнес-процессы предприятия на всех этапах работы.

Рис. 1. Структура стандартной ERP-системы

Доли программного обеспечения (ПО) для бизнеса от различных производителей на рынке РФ по состоянию на 2017 год представлены на рис. 2 [4].

На диаграмме (см. рис. 2, ниже) наглядно видно, что лидером рынка пока является SAP, однако отечественная программа для управления ресурсами 1С уверенно занимает второе место по занимаемой доли рынка. Этому способствовала кризисная ситуация 2014 года, вызванная санкционным режимом со стороны европейских стран и США. В ответ на сложившуюся ситуацию руководство страны призвало к импортозамещению и поддержке отечественных производителей, в том числе и ПО для бизнеса. Российские подразделения таких крупных компаний как Siemens и Ford Motor, а также ПАО «Газпром» и ФГУП «Почта России» стали клиентами 1С, запустив тем самым тренд на переход к 1С среди крупного бизнеса. Именно поэтому в

данной статье рассматривается ситуация на примере «1С: ERP Управление предприятием 2» (1С:ERP).

С развитием внедрения ERP-систем в предприятия по всей России растёт спрос на профессию аналитика в данной сфере. Средняя заработная плата специалиста в Москве колеблется около 100 тыс. рублей в месяц, а аналитик стажёр может получать до 70 тыс. рублей в месяц согласно данным исследовательского центра «Trud.com» [5]. Однако рынок сталкивается с нехваткой квалифицированных кадров, что связано не только с многогранной спецификой работы (специалисты должны разбираться не только в технической работе системе, но и в архитектуре бизнес-процессов), но и со сложностью освоения учебных материалов.

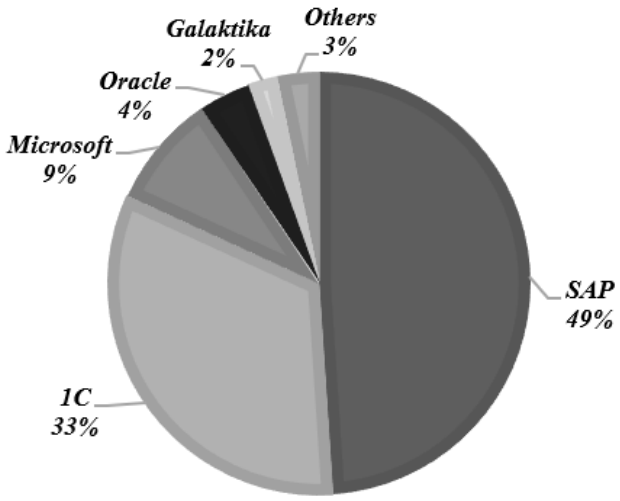


Рис. 2. Доли программного обеспечения для бизнеса на рынке РФ

Не только студенты встречают на своём пути преграды к изучению системы. Поскольку до 2014 года подавляющее большинство клиентов 1С:ERP являлось малым и средним бизнесом, не располагающим достаточными средствами для оплаты квалифицированного подрядчика по внедрению системы управления ресурсами, получила распространение практика самообучения сотрудников пользованию новой программой. Решение новой задачи для работников осложняется рядом трудностей.

Основные проблемы, с которыми сталкиваются обучающиеся:

1. Высокий входной порог для изучения ERP.
2. Разрозненная структура материалов для самостоятельного обучения.
3. Слишком большой объём данных для изучения.

Далее каждая из описанных выше проблем будет рассмотрена более детально [5].

Что подразумевает под собой высокий входной порог для изучения ERP? Большинство материалов для обучения подготовлены с расчётом на то, что изучающий уже знаком с системой и понимает специфику работы с ней. Для освоения программы студенту требуется самостоятельно погрузится в контекст, разбираясь в незнакомых алгоритмах и терминах. Существуют пособия и от компании-разработчика, и от клиентов, что снижает точность информации.

Учебные материалы для новых пользователей программы выпускались хаотично и не зависимо друг от друга, поэтому в поисках информации студент сталкивается с массивом разрозненных данных, имея не только повторения, но также и противоречия между собой, так как устаревшая информация никак не фильтруется и не удаляется из открытых источников. Существует таблица в формате Microsoft Excel, которая учитывает актуальные на данный момент материалы, но не все страждущие познать новый инструмент управления имеют к ней доступ, что рождает непонимания, ошибки при использовании ПО, а они зачастую влекут и финансовые потери для компаний.

К решению сложившейся ситуации необходимо подходить комплексно. Не только корректируя имеющиеся учебные пособия, но также пересматривая методы их представления студентам. Ряд предлагаемых мероприятий по совершенствованию учебного процесса:

1. Разработка материалов для «нулевого» уровня подготовки, адаптирующие человека к специфике работы с ERP-системами, дающие базовые знания, необходимые для дальнейшего более глубокого изучения темы.

2. Создание единой системы хранения материалов для обучения в формате интерактивной площадки.

3. Формирование определённых маршрутов изучения тем с поэтапными инструкциями и ссылками на готовый сборник, подходящий для конкретного уровня. Пример интересующих областей программы в зависимости от уровня подготовки приведён далее.

Для начинающего: Управленческий учёт – Управление продажами и взаимоотношение с клиентами – Управление человеческими ресурсами – Финансовое планирование и бюджетирование – Введение в управление проектами внедрения ERP-систем. Также новичку рекомендуется ознакомиться с обучающими видеороликами из курса «Концепция ERP» на YouTube, которые находятся в открытом доступе, что особенно важно для начального уровня, ведь зачастую у пользователей, только начинающих знакомиться с платформой, нет свободных средств на обучение. Видеокурс решает также другую проблему самостоятельного изучения – новичок рискует затеряться в терминах и забросить начатое дело. Лектор поэтапно будет вводить в мир управления ресурсами, попутно объясняя все незнакомые слова и специфику работы.

Для любительского уровня подойдёт изучение управления производством, особенностей ведения документации при использовании ERP, а также курсы учебного центра по подсистемам ERP. Такая комбинация материалов позволит узнать глубже структуру системы, её возможности и «правила игры» при использовании ERP на предприятии.

Для младших специалистов, желающих повысить свою квалификацию, интересно изучать более сложные кейсы – решение практических задач автоматизации с помощью комплексного управления ресурсами предприятия «1С: ERP», а также изучение методических статей на официальном сайте информационно-технологического сопровождения «1С:ИТС».

Старших специалистов интересуют аспекты презентации технических проектов, доклады сотрудников 1С о проделанной работе на тематических мероприятиях, а также технологии подготовки и автоматизации отчётности по международным стандартам финансовой отчётности. Обычно сотрудники с такими компетенциями занимают лидирующие позиции в команде проекта, что приводит к необходимости представления результатов работы руководству в виде отчётов и презентаций.

Отличным способом оптимизации процесса обучения является применение информационных технологий (IT) и их непосредственная интеграция. Успешный кейс использования IT был у компании 1С, которая применила технологию в тренинге стажёров-аналитиков ERP.

Обновлённый сайт платформы как единая точка входа для новых пользователей позволяет не потеряться новичку в массивном объёме материалов для обучения. На сайте собраны только проверенные материалы от самого разработчика ПО. Во избежание путаницы стажёру присылается приветственное письмо с перечнем полезных ссылок и их кратким описанием. Также прилагается перечень рекомендуемых маршрутов изучения в зависимости от начальной подготовки каждого ученика. Благодаря такому подходу студент не пугается объёмов информации и переходит только на тот раздел, который способен освоить на данный момент, что повышает процент завершаемости курса и способствует повышению имиджа обучающей компании[6]. Сквозные курсы с учётом отраслевой специфики позволяют углубиться в изучение программы сотрудникам различных сфер, что увеличивает долю покрытия образовательного портала среди всех компаний.

Одним из главных преимуществ 1С перед конкурентами является своевременная реакция на поправки в законодательстве РФ и предоставления для клиентов вебинаров по использованию программы с учётом изменений – заявляет Ольга Ускова, президент компании «Cognitive Technologies» [6]. В текущей быстро меняющейся конъектуре рынка «выживают» только те компании, которые используют свой потенциал по максимуму, а также обладают определённой гибкостью для мгновенного изменения под новые потребности общества. Клиенты чувствуют современность взглядов разработчика ПО и доверяют ему, будучи уверенными в актуальности полученного продукта.

Задачей данной статьи являлось выявление способов повышения эффективности процесса обучения с помощью применения информационных технологий на примере стажёров-аналитиков ERP-систем отечественной

компании 1С. Оптимизация работы с помощью внедрения IT делает процесс более прозрачным и понятным пользователю, а значит, повышает привлекательность продукта. Таким образом, постоянное обновление и улучшение структуры подачи даже сопутствующих услуг позволяет компании повысить эффективность и заполучить доверие клиентов.

Список используемых источников

1. Граничин О. Н., Кияев В. И. ERP и управление возможностями бизнеса [Электронный ресурс] // Национальный Открытый Университет «ИНТУИТ». 2008. URL: https://www.intuit.ru/studies/courses/1055/271/lecture/6886?page=1 (дата обращения: 02.02.2020).

2. Граничин О. Н., Кияев В. И. Архитектура предприятия [Электронный ресурс] // Национальный Открытый Университет «ИНТУИТ». 2008. URL: https://www.intuit.ru/studies/courses/995/152/lecture/4222?page=9 (дата обращения: 02.02.2020).

3. Граничин О. Н., Кияев В. И. Информационные системы планирования ресурсов и управления предприятием: ERP-системы [Электронный ресурс] // Национальный Открытый Университет «ИНТУИТ». 2008. URL: https://www.intuit.ru/studies/courses/1055/271/lecture/6886?page=2 (дата обращения: 02.02.2020).

4. Шляхтина С. Обзор российского рынка ПО [Электронный ресурс] // Электронное периодическое издание «КомпьютерПресс». 2017. URL: https://compress.ru/article.aspx?id=146689 (дата обращения: 05.02.2020).

5. Макаров В. В., Синица С. А. Информация как товар на рынке инновационных продуктов и услуг // Журнал правовых и экономических исследований. 2014. № 3. С. 20–22.

6. Макаров В. В., Шувал-Сергеева Н. С. Управление внедрением инноваций на рынке программного продукта / Под редакцией В. В. Макарова ; Федеральное агентство связи, Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича». Санкт-Петербург : СПбГУТ, 2018. 159 с. ISBN 978-5-89160-175-8.

УДК 364.4
ГРНТИ 10.67

ПЕНСИОННЫЕ РЕФОРМЫ И БУДУЩЕЕ РЫНКА ПЕНСИОННЫХ НАКОПЛЕНИЙ

М. А. Егорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Пенсионные изменения с 2002 года происходят постоянно. Низкая доходность накопительной части пенсии ставит под сомнение достижение основной цели пенсионной системы – повышение уровня пенсионного обеспечения граждан. Накопительная пенсионная система, аккумулиров.ав значительный объем финансовых средств, не гарантирует ни доходность, ни сохранность пенсионных накоплений.

пенсионная система, пенсионные накопления, инвестиционный доход.

Пенсионная система призвана выполнять социально значимую задачу государства – обеспечивать граждан пенсиями в старости. Начиная с 1990 года, практически постоянно происходит реформирование пенсионной системы. Работающему человеку все время приходится разбираться в быстро меняющихся схемах пенсионного обеспечения.

Советская распределительная пенсионная система в 2002 г сменилась переходом к распределительно-накопительной схеме. Размер пенсионных выплат стал зависеть не от стажа, а от объема средств, аккумулированных на индивидуальном лицевом счете. Пенсию разбили на три части: базовую, не зависящую от заработка, страховую, накапливающуюся на индивидуальном счете в Пенсионном фонде РФ (ПФР) и накопительную. Отчисления на базовую и страховую части шли на выплаты сегодняшним пенсионерам. Идея накопительной составляющей предполагала, что накопления обособляются на индивидуальном счете работника в ПФР и передаются в управление специально созданным институтам – негосударственным пенсионным фондам или управляющим компаниям (УК). Граждане получили возможность распорядиться накопительной частью трудовой пенсии, выбирая между государственной УК Внешэкономбанка (ВЭБ), либо частными негосударственными пенсионными фондами (НПФ). Изначально эта возможность была у мужчин моложе 1953 г. рождения и женщин моложе 1957 г. рождения, а с 1 января 2005 г. она касалась только лиц 1966 г. рождения.

Цель УК и НПФ – преумножить пенсионные накопления, формируя инвестиционный портфель из активов финансовых рынков. Доход от управления идет на пенсионные счета клиентов, на пополнение страхового резерва, на понесенные расходы и вознаграждение управляющих. С наступлением

пенсионных оснований выплата негосударственной пенсии происходит исходя из накопленной суммы, увеличивая основную пенсию от государства.

Понятная схема негосударственного пенсионного обеспечения позволила активно увеличивать пенсионные накопления, количество застрахованных лиц в НПФ, размер пенсионных резервов на одного участника. Большинство граждан по умолчанию доверили пенсионные накопления для обязательного инвестирования государственной УК ВЭБ. На долю НПФ пришлось лишь 16,4 % пенсионных накоплений, на частные управляющие компании – всего 2,3 % (по данным ФСФР на 2010 г.).

Теоретически рынок должен расти постоянно и гарантированно за счет роста количества участников, ежегодного перечисления новых средств на каждого застрахованного и инвестиционного дохода. Однако на финансовых рынках случаются кризисы. За 2008 г. пенсионные резервы НПФ сократились на 9991,1 млн руб. по сравнению с предыдущим годом, что отразилось на количестве участников НПФ (0,2 % прирост за 2009 г. и 0,3 % за 2010 г.) [1].

Чтобы оживить рынок пенсионных накоплений в 2008 г. была принята государственная программа софинансирования пенсий, по которой государство удваивало взнос в пенсионные накопления в объеме от 2 до 12 000 руб. в год в течение 10 лет. Эта программа заинтересовала на тот момент порядка 3 % экономически активного населения. На сегодня по данным ПФ РФ доля участников Программы софинансирования пенсионных накоплений, сделавших взносы в 2016 г. от количества индивидуальных лицевых счетов в системе обязательного пенсионного страхования столь же незначительна – менее 0,5 % в 2016–2017 гг. и 1,7 % в 2018 г. [2].

В 2013 г. наступил очередной этап реформирования пенсионной системы с новыми правилами учета пенсионных прав, зависящих от стажа, размера заработной платы, возраста выхода на пенсию. Граждан моложе 1967 г. рождения опять поставили перед выбором распоряжения страховыми взносами: либо направить их на формирование страховой части, либо продолжать накапливать. Пенсии стали рассчитывать с учетом годовых пенсионных коэффициентов, учитывающих годы трудовой деятельности гражданина через уплаченные работодателями страховые взносы, либо особые коэффициенты за периоды, когда человек не работал.

Положительным моментом можно считать принятую в декабре 2013 г. государственную программу обеспечения гарантий сохранности пенсионных накоплений физических лиц, формирующих и получающих накопительную пенсию, подобно страхованию банковских вкладов. Для этого НПФ – участники системы гарантирования прав застрахованных лиц, и ПФР обязаны платить гарантийные взносы в фонд гарантирования пенсионных накоплений. Агентство страхования вкладов (АСВ) выступает гарантом возмещения пенсионных накоплений, отраженных на индивидуальном

лицевом счете накопительной пенсии застрахованного лица. Но инвестиционный доход при этом не гарантируется.

В 2014 г. пенсионное законодательство вновь скорректировали. Для того чтобы уменьшить трансферты из федерального бюджета в ПФР, пенсионные отчисления граждан (6 % от заработной платы), которые должны были накапливаться, заморозили и направили в распределительную систему (на оплату пенсий сегодняшним пенсионерам). Будущих пенсионеров заверили, что пенсионный мораторий не уменьшит объем их пенсионных прав, так как суммы страховых взносов будут отражены на индивидуальных лицевых счетах застрахованных лиц и учтены при определении величины индивидуальных пенсионных коэффициентов. Мораторий на формирование накопительной части пенсии, заявленный как временная мера, продлевался ежегодно. В 2018 г. его продлили еще на 3 года, а 16 декабря 2019 г. очередным законом сохранили до 2022 г. включительно [3]. Пенсионная заморозка позволила ПФ с 2014 г. сэкономить около 2 трлн руб., и очередное ее продление в 2022 г. сократит размер трансферта из федерального бюджета в бюджет ПФ еще на 634,8 млрд руб. (по данным ПФР). Но одновременно эта мера означает, что на целых восемь лет работающие граждане лишены накопительной части пенсии и возможности ее роста на личных счетах.

Пенсионные накопления создавались для повышения уровня пенсионного обеспечения граждан. То есть накопления должны не просто сохранять средства будущих пенсионеров, а прирастать за счет инвестиционного дохода. Но этот прирост сильно зависит от как от состояния на глобальных финансовых рынках, макроэкономических и геополитических факторов, динамики долгового рынка, так и от профессионализма управляющей компании.

Следует отметить, что инвестиционная доходность сильно отличается у разных НПФ, и в самих НПФ по годам. Анализ доходности пенсионных накоплений НПФ за 2005–2019 годы показывает сильный разброс значений по годам. Лучшая доходность в отдельные годы никак не гарантирует в будущем ни столь же хорошие результаты, ни отсутствие отрицательной доходности. Не гарантирует высокую доходность ни размер, ни время работы на рынке пенсионных накоплений, ни известность самого НПФ. Так, два крупнейших по объему пенсионных накоплений фонда НПФ Сбербанка, Газфонд Пенсионные накопления показывают достаточно скромные по доходности результаты.

По данным ПФР за последние три года инвестиционная доходность пенсионных накоплений снизилась. В 2018 г. средняя инвестиционная доходность управления пенсионными накоплениями НПФ составила 5 % (упав с 10,8 % в 2017 г. и 14,2 % в 2016 г.). Это наихудший результат за 7 лет при разбросе доходности от максимальных 6,83 % у НПФ Аквилон

до минимальных –19,45 % у НПФ Образование [5]. Причем 12 НПФ показали доходность ниже инфляции, а 7 из 35 фондов ушли в минус. Такую ситуацию можно было бы объяснить наличием консервативных портфелей НПФ с большой долей облигаций (индекс гособлигаций РФ в 2018 г. потерял 5 %). Но результаты государственной УК ВЭБ при более жестких требованиях к структуре портфеля говорят скорее о низкой эффективности работы НПФ, некачественном управлении активами, в которые инвестируются средства пенсионных накоплений, либо высоких расходах на содержание самих себя. Инвестдоходность пенсионных накоплений по расширенному портфелю ВЭБ1 за тот же год составила 6,1 %, и 8,7 % по портфелю государственных ценных бумаг при инфляции в 4,3 %. Анализ ЦБ показал, что низкие показатели доходности были у фондов, где доля акций компаний с повышенным риском и сделок РЕПО в портфелях выше, чем у более успешных НПФ. А вот в 2019 г. средневзвешенная доходность инвестирования пенсионных накоплений НПФ (10,1%) оказалась выше, чем у государственной УК (8,3 %). Но это до вычета вознаграждения управляющим компаниям, спецдепозитарию и фондам.

Важно понимать, что доходность следует оценивать не просто по годам, а как накопленный результат на длинных промежутках времени с учетом инфляции. По реальной накопленной доходности в 23,16 % за 9 лет (с 2011 г.) портфель «ВЭБ государственные ценные бумаги» на сегодня обходит все НПФ. Для сравнения крупнейший НПФ Сбербанка с 573 млрд руб. показал накопленную реальную доходность за тот же период лишь 2,34 %, а НПФ Будущее и вовсе ушел в минус на 28,68 [4]. При этом 8 из 30 существующих на сегодня НПФ просто проели накопления будущих пенсионеров. Если бы все пенсионные накопления просто разместили на банковских депозитах, то реальная (с учетом инфляции) накопленная доходность за 9 лет составила бы 16,5 %, сократив при этом издержки на содержания самих НПФ. Кроме того, депозиты обладают большей ликвидностью: деньги, хоть и с потерей процентов, можно получить в любой момент, что невозможно в НПФ.

Средний размер получателей (1,2 млн чел.) накопительной пенсии в 2018 г. – 925 руб., а средний размер единовременной выплаты пенсионных накоплений – 3 935 руб. (2017 г.) [2]. Для сравнения средний размер выплачиваемой накопительной пенсии в 2010 г. был 800 руб. в месяц. О какой прибавке к пенсии может идти речь с такими показателями?

Оценить доходность НПФ за все время инвестирования средств пенсионных накоплений достаточно сложно ввиду того, что ПФ предоставляет статистические данные с 2016 г. Такую оценку также усложняет постоянно меняющийся состав и названия НПФов за счет слияния, отзыва лицензий, либо прекращения деятельности. Так, если в 2008 г. было зарегистрировано 240 НПФ, то в 2010 только 165 фондов. К 2019 г. осталось 49 фондов,

33 из которых входят в систему гарантирования прав застрахованных лиц, и 30 НПФ находятся в процессе ликвидации АСВ. Объяснить сокращение числа НПФ можно консолидацией самих фондов, и ужесточением регулирования со стороны Банка России. Поправки в законодательстве меняют вознаграждение участников процесса инвестирования пенсионных накоплений НПФ, создание системы управления рисками НПФ, дополнительные требования к инвестированию средств пенсионных накоплений [5]. Если 10 лет назад требования к минимальному размеру уставного капитала НПФ составляли 50 млн руб., то к 2019 г. уже 120 млн, а с 1 января 2020 г. уже не менее 150 млн руб. Такие требования продолжат вынужденный процесс присоединения фондов.

Очередной этап пенсионной реформы – повышение пенсионного возраста с 2019 г. – не решил проблем дефицита ПФР. Поэтому активно обсуждается создание новых пенсионных форм – индивидуального пенсионного капитала и гарантированного пенсионного плана. Смысл нововведений – замена накопительной части обязательного пенсионного страхования добровольной пенсионной накопительной программой. Вся история накоплений не позволяет гражданам поверить в новые пенсионные продукты и вряд ли стоит рассчитывать на дополнительные добровольные взносы к обязательным социальным выплатам.

Подводя итог состояния рынка пенсионных накоплений, отметим, что проводимые корректировки не дают никаких гарантий будущим пенсионерам. Длинные пенсионные деньги (на сегодня общий объем пенсионных накоплений 4,62 трлн руб.) ничем не защищены ни от глобальных финансовых кризисов, ни от неэффективного управления, ни от реорганизации, ликвидации и просто банкротства НПФ. Эти деньги служат инструментом поддержки капитализации российского фондового рынка и обеспечивают деятельность НПФ и УК. Пенсионные накопления означают сегодня вычет в пользу НПФ. Существует риск того, что вся система пенсионных накоплений к моменту, когда придется выплачивать пенсии, окажется значительно ниже ожидаемых сумм и вся полнота ответственности за выплату накопительной части пенсии вновь ляжет на федеральный бюджет.

Список используемых источников

1. Егорова М. А. Современное состояние и тенденции рынка НПФ в системе пенсионного обеспечения граждан // Сборник научных трудов преподавателей и аспирантов. СПб. : Линк, 2011. Вып. 1. С. 19–26.

2. Интернет портал «Пенсионный фонд Российской Федерации». URL: http://www.pfrf.ru/opendata/

3. Федеральный закон от 16 декабря 2019 г. N 435-ФЗ «О внесении изменений в статью 333 ФЗ «Об обязательном пенсионном страховании в РФ». URL: https://rg.ru/2019/12/19/pensii-dok.html

4. Кикевич С. Рейтинг доходности НПФ 2019. URL: https://rostsber.ru/publish/pension/npf_2019.html

5. Федеральный закон от 07.05.1998 N 75-ФЗ (ред. от 02.12.2019) «О негосударственных пенсионных фондах».

УДК 004.91; 681.51
ГРНТИ 82.01.85

ПРОБЛЕМЫ ВНЕДРЕНИЯ ПРОГРАММНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ НА ПРЕДПРИЯТИЯХ

А. В. Исаков, Е. В. Павлова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Несмотря на широкое применение цифровых информационных технологий во многие области современной экономики, государственного управления, да и во все сферы жизни общества, по-прежнему остается актуальным вопрос внедрения программных информационных систем на предприятиях. Во многом, это определяется ростом компаний, когда развитие бизнес процессов, рост объемов передаваемой информации, оперативности ее передачи, требует от бизнеса модернизации и автоматизации в части управления. Так же объективной причиной служит современное окружение – уровень цифровизации контрагентов, клиентов, государственных, в том числе налоговых, органов.

Но, независимо от причин, по которым предприятие приходит к необходимости внедрения программных информационных систем, практически все сталкиваются со сложностями, особенно на начальных этапах. Что характерно, каждый руководитель, во многом справедливо, считает, что его проблемы абсолютно уникальны. Но на практике, если анализировать этот вопрос со стороны профессионалов по внедрению, оказывается, что большинство проблем имеют типовую природу, вполне предсказуемы и решаемы, при условии грамотности разработчиков и открытости руководства предприятия к восприятию чужого опыта и знаний.

цифровизация, бизнес-процессы, управление, автоматизация, ERP-системы, CRM-системы, BI-системы, электронный документооборот.

Высокий уровень развития информационных технологий, их повсеместное внедрение, а также цифровизация практически всех сторон жизни современного человека подчас вынуждают собственника или руководителя российских предприятий задумываться о необходимости использования современных пакетных решений при управлении организацией.

На первоначальном этапе при отсутствии целостной картины и понимания целесообразности и необходимости достаточных финансовых вложений, а также на этапе роста предприятия практикуется внедрение отдельных программ, зачастую никак не взаимосвязанных между собой, и которые

в будущем также не могут быть объединены в рамках единой ERP-системы. Это могут быть программы, различаемые по функционалу: складские программы для учета поступления, движения и выбытия сырья, материалов, а также конечного продукта – готовой продукции предприятия, производственные программы для оперативно-производственного планирования, CRM-системы для учета и контроля за деятельностью отдела продаж, финансово-экономические программы для оценки результатов финансово-хозяйственной деятельности предприятия, бухгалтерские программы, программы электронного документооборота внутри предприятия, а также с внешними пользователями и т. д. Данные программы значительно не утяжеляют бюджет организации, что позволяет не проводить секвестирование бюджета за счет урезания расходов по другим статьям затрат [1].

Зачастую данные программы вводятся постепенно на предприятии. Их внедрение напрямую зависит от уровня компетенции руководителя того или иного функционального подразделения предприятия, а также их лоббирования интересов своего подразделения и умения доказать собственнику или руководителю предприятия их необходимость и целесообразность.

Этот вариант инициации приобретения и внедрения программной информационной системы «снизу» имеет свои плюсы и минусы. Плюсы в том, что руководитель подразделения, поднимая вопрос о внедрении информационных программ, заинтересован в развитии данного подразделения, оптимизации его структуры и исполнительной дисциплины, качественной оценки вклада каждого отдельного сотрудника в результаты работы всего подразделения, нацелен на прозрачность и эффективность работы данного функционального подразделения [4].

Но и упомянутый положительный фактор, доведенный до высшего руководства, частично теряет свой эффект, так как высшее руководство не может интересовать оптимизация только одного из подразделений. Во всех бизнес процессах, так или иначе, участвуют все подразделения компании и достигнуть положительного эффекта возможно лишь при комплексной автоматизации.

Тем не менее, существует еще один положительный эффект, проявляющийся при инициации «снизу». Во всех исследованиях, авторы сходятся во мнении, что одним из наиболее сложных тормозящих факторов при внедрении, является непонимание и нежелание перемен, со стороны рядовых работников и линейных руководителей. Именно при инициативе «снизу» есть реальная возможность минимизации подобного фактора.

Минусы состоят в том, что, не имея достаточного авторитета, или меньшего авторитета, чем у главного распределителя финансовых затрат, будь то финансовый директор, главный бухгалтер или начальник финансово-экономического отдела, он может быть не услышан или же не поддержан собственником или руководителем предприятия. На практике руководители

подразделений зачастую не имеют достаточной квалификации и знаний и не могут экономически обосновать целесообразность и необходимость принятия такого решения и внедрения информационных программ. В таком случае руководителю данного подразделения необходимо представить покупку и внедрение данного программного продукта как проект и обязать экономический блок предприятия провести технико-экономическое обоснование данного проекта.

Второй путь внедрения программных решений «сверху», то есть спускаемого в функциональные подразделения собственником или руководителем предприятия имеет также свои достоинства и недостатки. Плюсы заключаются в том, что сокращается время необходимое для продвижения идеи, на обоснование и проведение экономических расчетов внедрения данных программных продуктов.

Также, принимая решение об автоматизации бизнес процессов, высшее руководство, в подавляющем большинстве случаев, рассматривает подобные внедрения сразу в масштабе всего предприятия, что обычно положительно влияет на эффективность проекта для компании в долгосрочной перспективе [2].

В то же время минусом данного пути является то, что если руководитель функционального звена морально не готов к развитию функционала своего подразделению, консервативен по сути, привык работать старыми, так называемыми «проверенными» методами, не готов к нововведениям и новым методам работы, не гибок к принятию новых инструментов при решении своих повседневных задач, и, возможно, не заинтересован в повышении прозрачности вверенного ему функционального участка, то, какого бы уровня сложности и охвата не внедрялась система, она не даст результатов.

Здесь возникает второй и априори самый важный аспект при внедрении программных продуктов – человеческий фактор. Приведем простую аналогию: если дать обезьяне смартфон, она будет пользоваться им как камнем, т.е. раскалывать орехи, но не использовать по прямому назначению.

В этом и состоит главная угроза для собственников и руководителей предприятий при внедрении программных продуктов. Зачастую собственники предприятий считают, что, приобретя за достаточно значительные денежные средства, информационную систему, они получают панацею от всех проблем, которые стоят перед предприятием. Данное заблуждение как раз и формируется теми сотрудниками предприятия, которые годами списывают свои собственные ошибки и недоработки на отсутствие у них качественного программного продукта.

Под грузом данного ложного информирования у собственника редприятия возникают аллюзии, когда он представляет информационную систему как некую «красную кнопку», нажав на которую все проблемы предприятия обойдут его как «смертоносные айсберги корабль».

Но у собственника предприятия должно быть четкое понимание, что программный продукт сам по себе не решит задачи, стоящие перед организацией, а является лишь инструментом в руках его подчиненных. И чтобы они не уподоблялись той самой обезьяне, которая просто не понимает, что делать с вверенным ей приспособлением, а использует его знакомым ей способом, необходимо научить сотрудников предприятия правильно использовать данное программное обеспечение [5]. А также, что может оказаться и более важным фактором в этом вопросе, дать понимание, что информационная система – это, в первую очередь инструмент, который, при адекватном его принятии и использовании, призван облегчить и ускорить работу каждого сотрудника, а не придуман только для того, чтобы увеличить нагрузку на сотрудников и облегчить возможность слежки со стороны руководства.

Именно поэтому наиболее важным этапом при покупке программного продукта является не сам факт его приобретения, а длительный сложный процесс его внедрения и адаптации под особенности конкретного предприятия [3]. Недостаточно просто приобрести программный продукт – необходимо проводить его сопровождение разработчиками или специалистами, уполномоченными на внедрение данного программного продукта. В этом месте возможен сбой, так как собственник, считая, что он вложил достаточно средств в покупку данного программного продукта, не готов тратить на внедрение и сопровождение денежные средства, подчас превосходящие стоимость продукта в 2, 3, а иногда и 4 раза. А также время, как свое собственное, так и максимального количества сотрудников – что является необходимым условием успешного внедрения.

В данном случае неумелое использование программ, отсутствие адаптации под особенности предприятия, недостаточное заполнение данными производственной, хозяйственной и финансовой деятельности предприятия ведут к получению неполной искаженной информации на выходе при использовании программных продуктов. Противники среди персонала, «тайные» - не заинтересованные в прозрачности функционирования вверенной им зоны ответственности или «явные» – не обладающие достаточным уровнем знаний и подготовки, либо гибкостью, также активизируют свою информационную атаку по дискредитации данного нововведения, и как результат без жесткого приказа «сверху» о программе забывают [6]. Сторонники же приобретения информационной системы осуществляют безуспешные попытки использования данного программного продукта, но бессистемное внедрение и частичное использование не дает результативного эффекта.

Надо оговориться, что данная ситуация достаточно распространена с начала нулевых годов XXI века и продолжается до сих пор, причём ти-

пична не только для коммерческих организаций, функционирующих в условиях конкурентной среды, но и для бюджетных государственных учреждений.

Недобросовестные организации, занимающиеся созданием программных продуктов и декларирующие их как адаптивные под конкретные организации, пользуются отсутствием должной подготовки и понимания процессов внедрения программных системных продуктов у собственников и руководителей предприятий, и продают по сути разработки, не опробованные на практике. В итоге, собственник предприятия покупает воздушный шарик в красивой оболочке, при ближайшем рассмотрении оказывающийся по сути воздухом.

Если же команда разработчиков поставляет качественный продукт и собственник предприятия реально оценивает, что приобретает не панацею решения всех проблем предприятия, а инструмент, который требует кропотливого внедрения, тщательной подготовки, не только профессиональной квалификационной, но и, в том числе, психологической персонала, который будет заниматься вводом исходных данных на входе и получением результативных данных на выходе, и готов вложить значительные суммы денежных средств, а также затратить годы на внедрение и адаптацию данного программного продукта, то только в этом случае можно будет говорить об успешном применении программной системы.

Список используемых источников

1. Гринберг А. С., Горбачев Н. Н., Бондаренко А. С. Информационные технологии управления: учеб. пособие. М. : ЮНИТИ, 2004. 439 с.

2. Учебник для студентов вузов, обучающихся по специальностям «Финансы и кредит», «Бухгалтерский учет, анализ и аудит» и специальностям экономики и управления (060000) / Под ред. Г. А. Титоренко. 2-изд., перераб. и доп. М. : ЮНИТИ-ДАНА, 2008. 463 с.

3. Информационные технологии в бизнесе : [Энциклопедия] / Под ред. Милана Желены; [Пер. с англ. А. Железниченко и др.]. СПб. : Питер, 2002. 1117 с. ISBN 5-318-00125-4.

4. Лодон Дж., Лодон К. Управление информационными системами. СПб. : Питер, 2005. 915 с.

5. Васильев С. В. Организационные формы управления инновационными проектами на предприятии // Контроллинг. 2010. № 1. С. 82–87.

6. Васильев С. В. «Покой нам только снится…». Инновации – эпоха постоянных изменений // Российское предпринимательство. 2006. № 4. С. 40–45.

УДК 338.46
ГРНТИ 49.38.49

КОНЦЕПЦИЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ УЛУЧШЕНИЯ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ СФЕРЫ УСЛУГ

С. В. Ковалёв, В. В. Макаров, С. А. Синица, Д. О. Стародубов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Предлагается улучшить работу предприятия общественного питания посредством внедрения мобильного приложения, которое позволяет делать клиентам предварительный онлайн заказ с мобильного устройства абонента. Внедрение приложения на основе конструктора iBuildApp, не требуя существенных затрат, улучшает предоставление услуг и повышает конкурентоспособность предприятия.

мобильное приложение, инфокоммуникационные технологии, отдел IT, онлайн оплата.

В ходе анализа деятельности одного из предприятий общественного питания была выявлена проблема высокой загруженности кофейни в связи с большим количеством посетителей, преимущественно берущих кофе на вынос, перед работой или учебой. Вследствие чего часть людей, видя очередь, проходит мимо, не желая опаздывать на работу. При этом, и в течение дня заходит много людей, цель которых не провести время в кофейне, а взять кофе с собой и продолжить путь. Причинами очередей является нехватка персонала и оборудования для быстрого обслуживания большого количества людей.

Решение этой проблемы путем увеличения штата сотрудников является нецелесообразным в виду того, что после спада основного утреннего потока штат сотрудников становится избыточным. Дополнительным фактором является загруженность и ограниченность количества кофемашин, так как при большом потоке, бариста, физически не успевает быстро приготовить все напитки. Данный процесс представлен на рис. 1.

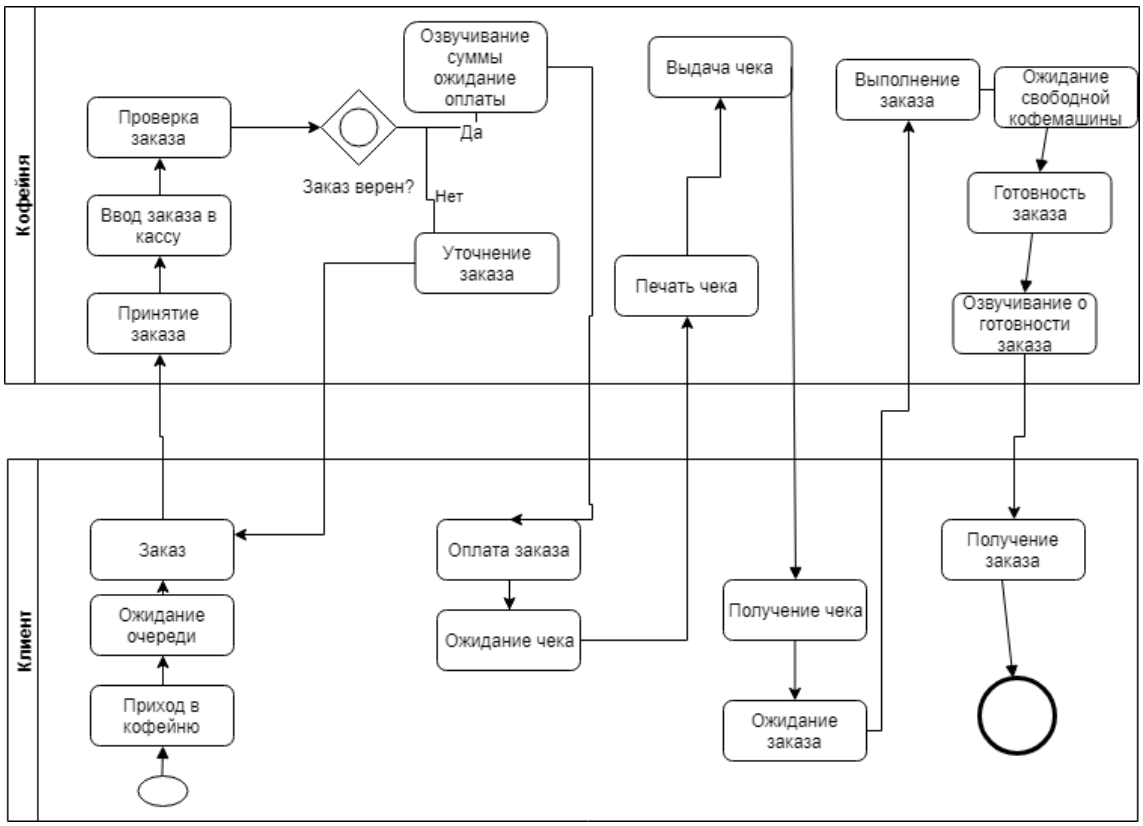


Рис. 1. Выполнение заказа классическим способом

Исходя из этого, возникает потребность в решении данной проблемы альтернативным способом, которым может стать использование бизнес-моделей цифровой экономики, основанных на инфокоммуникационных технологиях, позволяющих оптимизировать работу предприятия и повысить его конкурентоспособность [1, 2].

В виду неэффективности классических методов усовершенствования производства, оптимальным решением будет организация системы, позволяющей сделать онлайн заказ, помещаемый в специальную зону ожидания выдачи, где он слегка подогревается, не допуская остывания кофе. Прибыв в кофейню, клиент может получить его, без необходимости стоять в очереди, в специальной зоне выдачи.

На основании изложенного, принято решение о необходимости:

1. Создать мобильное приложение, в котором клиент сможет сделать заказ по пути в кофейню и получить уже готовый кофе по прибытии.

2. Внедрить систему онлайн оплаты кофе через приложение, с целью исключения очередей на кассе.

3. Сформировать рекламную компанию для информирования существующих клиентов и привлечения новых.

4. Выделить отдельную кофемашину и бариста, который будет заниматься исключительно приготовлением кофе на вынос.

5. Организовать специальную зону выдачи, в которой клиент через телефон будет сканировать qr-код, подтверждающий оплату, и забирать заказ.

Пример работы системы представлен на рис. 2.

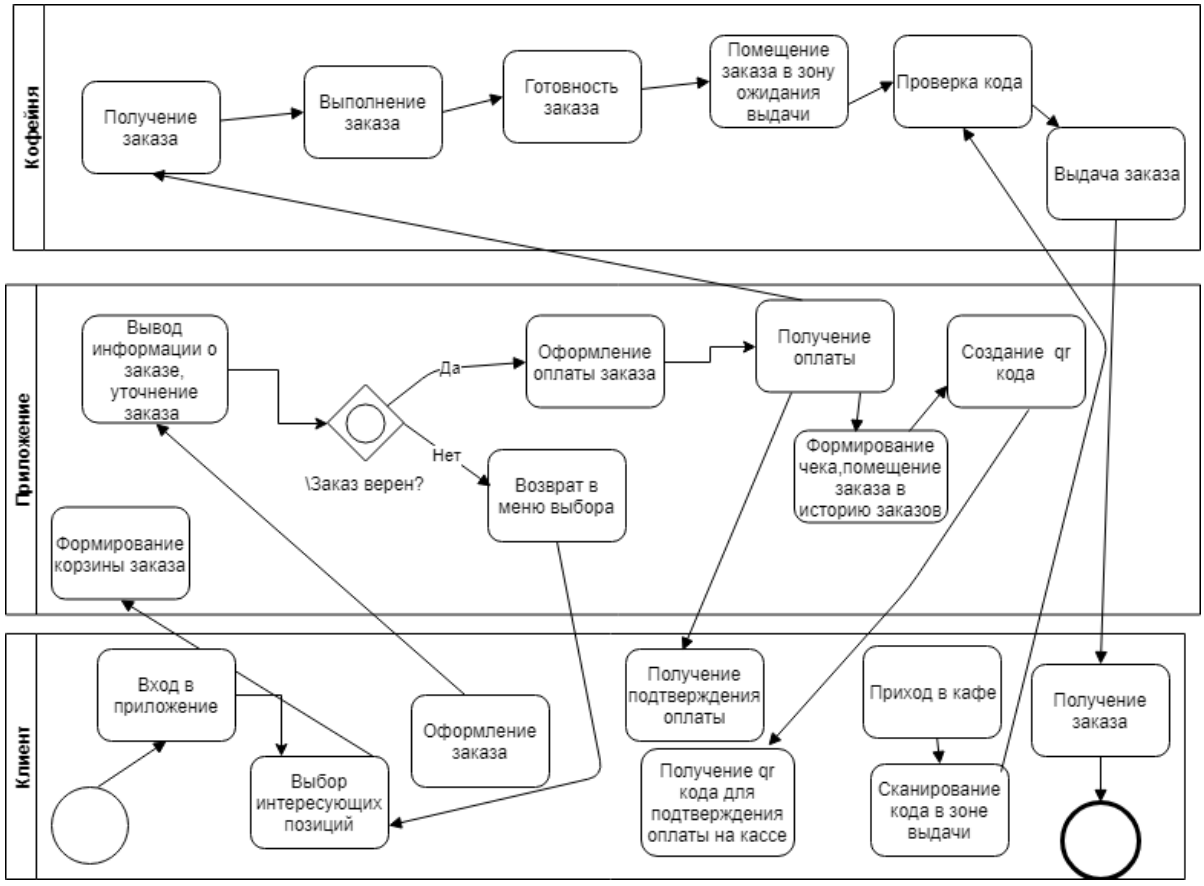


Рис. 2. Онлайн оплата заказа

В настоящее время существует несколько основных вариантов создания мобильного приложения для заведения общественного питания [3]. Можно воспользоваться готовыми шаблонами в конструкторе и платить абонентскую плату платформе, предоставляющей конструктор, либо же разработать собственное мобильное приложение.

В первом случае основным преимуществом являются относительно невысокие начальные инвестиции и быстрая разработка приложения. Сроки разработки при помощи конструктора составляют 1–2 месяца. Стоимость разработки может быть, как бесплатной, при самостоятельной разработке, так и составлять от 15 тыс. рублей и выше, при заказе у создателей конструктора шаблонов. Регистрация приложения в магазинах AppStore и Google Play может, как входить в стоимость, так и оплачиваться отдельно.

При создании собственного приложения можно выбрать разработчика приложений и заказать ему разработку. При этом будут затрачены большие средства на разработку, а также это займет много времени. Зато в итоге

можно будет получить полностью уникальное приложение со всем необходимым функционалом, с возможностью его модернизации и расширения в будущем. Сроки таких работ в среднем составляют 4–6 месяцев, а стоимость начинается от 400 тыс. рублей. Регистрация приложения в магазинах AppStore и Google Play, как правило, входит в стоимость.

Учитывая значительную стоимость разработки мобильного приложения, небольшой несетевой кофейне не имеет смысла вкладывать большие средства в разработку и поддержание собственного приложения. Гораздо более рациональным решением будет сделать приложение при помощи конструктора приложений и заказать у сервиса его разработку. Хотя в этом случае функционал приложения будет несколько ограничен возможностями конструктора.

Приложение будет разработано на основе конструктора iBuildApp. iBuildApp – это онлайн-сервис, который предоставляет простой и недорогой способ создания, тестирования, отслеживания и обновления мобильных приложений для iPhone/Android, HTML5 и iPad [4]. Сервис позволяет создавать в приложении тексты, изображения, аудио, видео. С его помощью можно бесплатно создать свое приложение и опубликовать его в магазинах приложений. При этом стоимость аккаунта разработчика для публикации приложения оплачивает сам клиент, также в бесплатной версии опубликованного приложения присутствует реклама от разработчика iBuildApp, которую можно убрать в платной версии конструктора.

Так как у кофейни нет своего отдела IT [5], в конструкторе будет создан макет приложения, а разработка полностью готового приложения будет заказана у компании «iBuildApp». Главными требованиями к приложению являются: простота и удобство интерфейса; быстродействие; безопасность.

Прежде всего, необходимо создать систему регистрации и авторизации в приложении. После регистрации клиенту будет необходимо установить четырехзначный пароль для защиты данных. При этом четырехзначный пароль не является достаточно безопасным методом для защиты данных клиента.

Для дополнительной защиты данных будет внедрена система идентификации по отпечаткам пальцев. Для настройки доступа по отпечатку пальцев необходимо сначала задать пароль. Датчик биометрической идентификации разработан для того, чтобы свести к минимуму использование пароля. Пароль при этом требуется для дополнительных проверок безопасности в следующих случаях:

– телефон был выключен или перезагружен;

– сделано подряд пять безуспешных попыток разблокирования с помощью отпечатка пальца;

– устройство ни разу не разблокировалось в течение двух суток;

– устройство не имеет биометрического датчика.

При этом для пользователей, чьи мобильные устройства не поддерживают биометрическую идентификацию, тоже возможно повысить безопасность. Пользователь может сменить 4-значный пароль на более сложный буквенно-цифровой. Для этого необходимо перейти в меню «настройки» и задать свой более сложный пароль.

После авторизации пользователь попадает в главное меню приложения. Оно содержит следующие элементы: выбор кофейни, настройки, новости и акции, сделать заказ, история заказов, помощь.

Пункт меню «выбор кофейни» предоставляет возможность выбрать заведение, в котором будет сделан заказ, и отображает его местоположение на карте.

В меню заказа перечислены позиции меню с ценами, изображениями и кратким описанием. Клиент может добавить в корзину позиции, которые собирается купить, и оплатить заказ. После оплаты клиент получает qr-код, который он сканирует на кассе для подтверждения заказа.

В пункте меню «история заказов» можно посмотреть список совершенных покупок и повторить заказ. Меню «настройки» позволяет сменить пароль и добавить данные о банковской карте.

В пункте меню «помощь» содержится форма для обратной связи, которая позволяет задать интересующие вопросы, внести предложения и пожелания, сообщить об ошибках в приложении.

При таком подходе, одному из сотрудников планируется добавить дополнительные задачи: реклама и поддержка приложения. Рекламную кампанию планируется проводить собственными силами предприятия.

В заключение следует ещё раз подчеркнуть, что ввиду отсутствия у компании собственного IT отдела, оптимальным решением будет заказать разработку и поддержку приложения у фирмы разработчика конструктора приложения, на основе которого и делался макет. Это будет значительно дешевле и быстрее разработки самостоятельного приложения.

Список используемых источников

1. Алексеев А. Л., Блатова Т. А., Макаров В. В., Шувал-Сергеева Н. С. Инновационные бизнес-модели в цифровой экономике и их конкурентные преимущества // Вопросы радиоэлектроники. 2018. № 9. С. 99–104.

2. Шувал-Сергеева Н. С., Блатова Т. А., Макаров В. В. Внедрение информационнокоммуникационных технологий в организации: от оптимизации структуры до повышения конкурентоспособности // Радиопромышленность. 2017. № 2. С. 101–106.

3. Официальный сайт журнала «Российский продовольственный рынок» [Электронный ресурс]. URL: http://www.foodmarket.spb.ru/current.php?article=1476 (дата обращения^ 07.02.2020).

4. Конструктор мобильных приложений «iBuildApp». [Электронный ресурс]. URL: http://russia.ibuildapp.com (дата обращения^ 07.02.2020).

5. Макаров В. В., Цатурова Р. Г., Мазурова М. М., Горбачев В. Л. Менеджмент в телекоммуникациях : учебное пособие / Под ред. В. В. Макарова, Р. Г. Цатуровой ;

Федеральное агентство связи, Федеральное гос. образовательное бюджетное учреждение высш. проф. образования «Санкт-Петербургский гос. ун-т телекоммуникаций им. М. А. Бонч-Бруевича». 2-е изд., перераб. и доп. Санкт-Петербург : СПбГУТ, 2011. 369 с. ISBN 978-5-89160-061-4.

УДК 338.2; 338.4; 338.5
ГРНТИ 06.52.35

СИСТЕМНЫЙ ПОДХОД К МАРКЕТИНГОВОЙ ФУНКЦИИ УПРАВЛЕНИЯ

В. И. Котов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Предложена иерархическая структура маркетинговых задач в системе управления фирмой. Представлен сравнительный анализ различных вариантов концепции маркетинг-микс широко используемой в научной литературе. Новый системный взгляд на маркетинг, как функцию управления бизнесом, может быть полезен как с практической точки зрения, так и с точки зрения методики преподавания этой дисциплины.

маркетинг, маркетинг-микс, ценовая политика, товарный ассортимент, сбыт, реклама, маркетинговые исследования, конкуренция.

Введение

Согласно определению Ф. Котлера, данном в его монографии «Основы маркетинга» в 1990 году «Маркетинг – вид человеческой деятельности, направленной на удовлетворение нужд и потребностей посредством обмена». В более поздней работе «Маркетинг. Менеджмент»

Ф. Котлер дает развернутое определение: «Маркетинг – это социальный и управленческий процесс удовлетворения нужд и потребностей, как индивидов, так и групп путем создания, продвижения и обмена товаров» [1]. Среди множества концепций маркетинга рассмотрим наиболее популярную концепцию «маркетинг-микс» предложенную Нэлом Борденом (*Neil Borden*) в 1964 году.

Вначале комплекс маркетинга состоял из четырех элементов (4P), а именно [2]:

1. *Product* – товар.
2. *Price* – цена.
3. *Place* – место (каналы сбыта).
4. *Promotion* – продвижение товара.

Ф. Котлер считал, что эта модель в большей степени отражает интересы продавца, а не покупателя. В след за концепцией 4P появилась концепция, в которой интересы покупателя в концентрированном виде были представлены концепцией 4C:

1. *Товар* – ценность для потребителя (*Customer value*).
2. *Цена* – расходы потребителя (*Customer Costs*).
3. *Место* – доступность товара для потребителя (*Customer Convenience*).
4. *Продвижение* – информированность потребителя (*Customer Communication*).

Ягдиш Шет предложил альтернативную схему, которую назвал 4A. Он считал, что покупке товара предшествуют:

1. *Осведомленность* (*Awareness*).
2. *Приемлемость* (*Acceptability*).
3. *Доступность* (*Affordability*).
4. *Легкость приобретения* (*Accessibility*).

Другие исследователи предлагают добавить новые компоненты *P* к уже имеющимся четырем:

1. Упаковку (*Packaging*).
2. Продажи через торговых представителей (*Personal selling*).
3. Энтузиазм (*Passion*).

Ф. Котлер не остался в стороне от «игр в буквы» и предложил включить в инструментарий еще два *P,* как инструменты глобального маркетинга:

1. *Политики* (*Politics*).
2. *Общественное мнение* (*Public opinion*).

В дальнейшем для сферы услуг были предложены еще три дополнительных *P*:

• *Персонал* (*Personnel*), работа с которым необходима, чтобы произвести благоприятное впечатление на клиента.

• *Процесс* (*Process*). Услуги могут оказываться самыми разными способами (например, в различных кафе еду можно заказывать по-разному: у официанта, у буфетной стойки, по телефону на дом).

• *Вещественное доказательство* (*Physical evidence*). Продавцы стремятся сделать свои предложения осязаемыми с помощью разного рода сертификатов, лицензий, логотипов и прочего.

На наш взгляд все вышеупомянутые «концепции» представляют собой разрозненные несистематизированные наборы важных сущностей, входящих в маркетинг как деятельность. Из этого перечня неясно, чем конкретно должны заниматься работники маркетинговой службы компании. Кроме того, указанный набор сущностей является неполным.

Системный подход к маркетинговой функции управления

Представим всю маркетинговую деятельности фирмы в виде иерархии последовательно решаемых задач, как показано на рис. (см. ниже).

Раскроем содержание макроблоков II–V, представленных на рис.

II. Влияние конкуренции на решение основных задач маркетинга

1. Сравнительный анализ товара фирмы с товарами конкурентов.
2. Конкуренты и рынки (сегменты) потребителей.
3. Доля рынка конкурентов.
4. Цены конкурентов.
5. Каналы сбыта и реклама конкурентов.

III. Маркетинговые исследования – для решения основных задач.

1. Маркетинговое исследование товара.
2. Маркетинговое исследование сегментов потребителей.
3. Оценка спроса и возможной доли рынка.
4. Анализ ценовой политики конкурентов.
5. Оценка эффективности рекламы и каналов сбыта.

IV. Управление маркетингом включает в себя:

1. Определение цели маркетинга.
2. Планирование маркетинга. Бюджет маркетинга.
3. Координация работ службы маркетинга.
4. Контроль и мониторинг результатов продаж.
5. Анализ результатов продаж.
6. Принятие решений о корректировки (обратная связь).

V. Организация деятельности маркетинговой службы:

1. Функциональная организация структура.
2. Территориальная организационная структура.
3. Товарная организационная структура.
4. Рыночная организационная структура.
5. Матричная организационная структура.
6. Материальное обеспечение службы маркетинга.
7. Подбор и обучение персонала службы маркетинга.

При выстраивании организационной структуры и деятельности маркетинговой службы важно подчеркнуть, что в приведенной системе все задачи I-го макроблока должны решаться в указанной логической последовательности с 1-й по 5-ю задачу. А далее выстраивается деятельность остальных макроблоков со II-го по V-й.

Сравнивая предложенную иерархию основных задач маркетинга с популярной концепцией маркетинг-микс 4P, можно видеть, что в последней отсутствуют две важнейшие задачи:

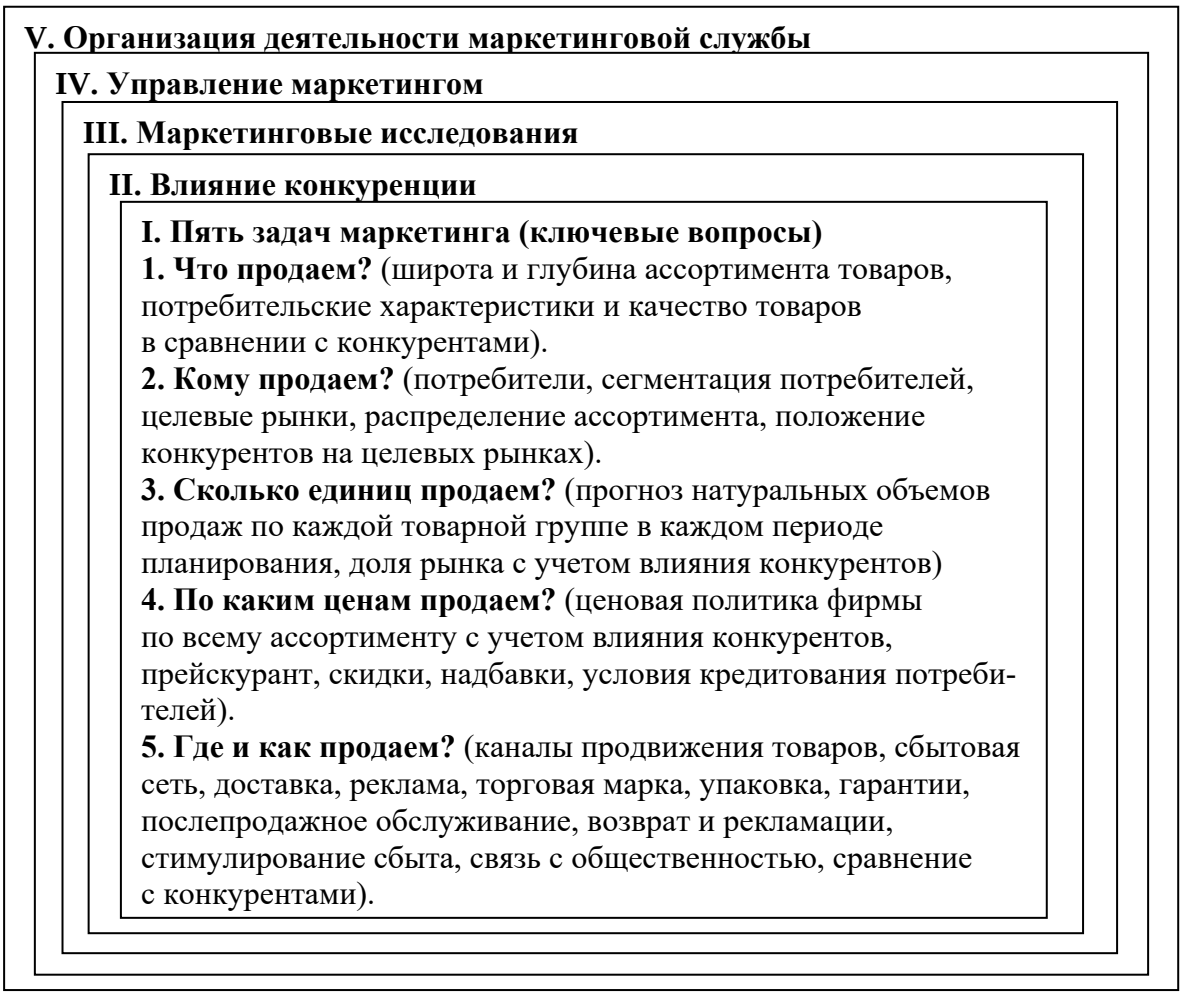


Рис. Иерархия задач маркетинга

2. Кому продаем? (потребители, сегментация потребителей, целевые рынки, распределение ассортимента, положение конкурентов на целевых рынках).

3. Сколько единиц продаем? (прогноз натуральных объемов продаж по каждой товарной группе в каждом периоде планирования, доля рынка с учетом влияния конкурентов)**.**

Эти задачи не входят и в другие концепции маркетинг-микс, о которых шла речь во введении.

Заключение

Завершая рассмотрение системного подхода к выстраиванию маркетинговой функции управления фирмой, отметим практическую ценность данного подхода, который был неоднократно использован в нашей консалтинговой деятельности. В 90-е годы, когда маркетинговые службы компаний только начинали формироваться, у нас появилась эта концепция как ответ на вопросы многих заказчиков: «Чем должны заниматься маркетологи

и служба маркетинга компании в целом? За что мы должны им платить заработную плату?».

Кроме того, как показала практика преподавания курса «Маркетинг», с методической точки зрения очень удобно выстраивать логику дисциплины, опираясь на предложенный системный подход [3].

Список используемых источников

1. Котлер, Ф. Маркетинг, Менеджмент. СПб. : ПИТЕР, 2018. 848 с.
2. Концепция маркетинг – микс (4P, 5P, 7P) // PowerBranding.ru. URL: http://power-branding.ru/osnovy-marketinga/4p-5p-7p-model/
3. Котов В. И. Риск-анализ инвестиционных проектов на основе функций чувствительности и теории нечетких множеств. СПб. : Астерион, 2019. 350 с.

УДК 338.47
ГРНТИ 49.34.06

ИТОГИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ НОШ «ЭКОНОМИКА И УПРАВЛЕНИЕ В ИНФОКОММУНИКАЦИЯХ»

В. В. Макаров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследуется результативность и достижения многолетней деятельности научно-образовательной школы СПбГУТ «Экономика и управление в инфокоммуникациях». Анализируется отраслевая направленность подготовки специалистов высшей квалификации; приводятся монографии, учебные пособия и научные статьи, выполненные в рамках НОШ. Прослеживается научная и учебная деятельность выпускников научной Школы, продолжающих сотрудничество с кафедрой экономики и менеджмента инфокоммуникаций. Рассматривается тематика научно-исследовательских работ и использование результатов исследований в производственной деятельности предприятий сферы ИКТ, а также в научной и учебной работе кафедры.

научно-образовательная школа, инфокоммуникации, инновационное развитие, научные исследования, цифровая экономика, учебная и научная деятельность.

Ведущие научные школы всегда определяли перспективы развития науки. Особую актуальность этот постулат приобретает в настоящее время, когда становится всё более очевидным, что решение научных проблем в любой отрасли знаний требует совместных усилий коллективов учёных. А значит, значительно возрастает важность и значение научных школ

как научно-образовательных коллективов. Причём, научные школы образуются как неадминистративные, неформальные производственные коллективы на кафедрах, факультетах, или в других структурных подразделениях.

Научную школу обычно определяют, как вид научного сообщества и одну из моделей эффективного образования, признавая при этом, особой формой кооперации научно-образовательной деятельности.

Научная школа – это инструмент для «воспитания исследовательского стиля мышления"(...) определенного способа подхода к проблемам» [1, с. 29]. Каждая научная школа вносит свой вклад в развитие инновационных идей в области науки.

Все вышеизложенные определения и характеристики в полной мере могут быть распространены и на понятие «научно-образовательная школа». На кафедре экономики и менеджмента инфокоммуникаций (ЭМИ) Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича под руководством заведующего кафедрой, доктора экономических наук, профессора, заслуженного деятеля науки РФ Макарова Владимира Васильевича функционирует научно-образовательная школа (НОШ) «Экономика и управление в инфокоммуникациях», в рамках которой разработаны теоретические основы эффективного функционирования предприятий связи в условиях рыночной экономики.

Профессор Макаров В. В. является основателем научно-образовательной школы. Школа функционирует уже много лет, хотя официально, как НОШ, она оформлена в 2010 г.

Под научным руководством профессора Макарова В. В. в рамках Школы подготовлено 3 доктора (в том числе один защитил диссертацию в 2019 г.) и 38 кандидатов наук. Все диссертационные работы выполняются в рамках НОШ, и посвящены проблемам работы отрасли связи и информационных технологий.

Так, в 2016 г. была защищена диссертация по специальности: 08.00.05 – Экономика и управление народным хозяйством (управление инновациями) Шувал-Сергеевой Н. С. на соискание ученой степени кандидата экономических наук на тему: «Совершенствование методов управления внедрением вторичных процессных инноваций» на примере программного обеспечения CATIA.

В 2019 г. – диссертация на соискание ученой степени доктора экономических наук по специальности: 08.00.05 – Экономика и управление народным хозяйством (связь и информатизация) Ноздриным В. В. на тему: «Развитие системы управления использованием радиочастотного спектра в условиях цифровой экономики».

Подавляющее большинство выпускников НОШ после успешной защиты диссертаций работает в сфере телекоммуникаций и информационных технологий, занимая руководящие должности различных уровней. Многие

из них продолжают сотрудничать с кафедрой ЭМИ: читают лекции, являются председателями ГАК, руководителями и рецензентами дипломных работ, совместно со штатными преподавателями выступают на научных конференциях, в том числе международных, публикуют учебники, монографии, научные статьи.

Фундаментальные исследования преподавателей, аспирантов и студентов Школы изложены в научных трудах. Только за последние 5 лет по направлениям НОШ преподавателями, докторантами и аспирантами кафедры опубликовано более 20 монографий, учебников и учебных пособий (монография профессора Макарова: «Управление внедрением инноваций на рынке программного продукта» – 2018 г.), учебные пособия: «Инновационный менеджмент и управление качеством в ИКТ» – 2019 г., «Экономика отрасли инфокоммуникаций» – 2019 г.), около 200 статей в научных изданиях (из них более 30 в 2019 г.).

Научные статьи последнего времени посвящены исследованиям в области цифровой экономики, например [2, 3]. Основополагающая монография профессора Макарова В. В. «Телекоммуникации России: состояние, тенденции и пути развития» [4] является базовой книгой учёных и специалистов, работающих в телекоммуникациях, а более поздняя монография [5] расширяет сферу профессиональных интересов и для специалистов IT.

В настоящее время четверо выпускников Школы являются штатными преподавателями кафедры ЭМИ – к. т. н., доц. Щербаков И. Б., старшие преподаватели Радюк М. А., Блатова Т. А., Старкова Т. Н., а доцент, к. э. н. Синица С. А. и доцент, к. э. н. Слуцкий М. Г. – преподавателями-совместителями, которые, будучи руководителями производства, делятся опытом практической деятельности предприятий отрасли ИКТ со студентами, активно работают над докторскими диссертациями.

Основной миссией работы Школы является разработка перспективных направлений эффективного функционирования предприятий отрасли ИКТ в рыночной экономике. Результаты научных исследований представителей НОШ внедрены и успешно используются в практической деятельности на ведущих предприятиях связи России: ПАО «Ростелеком», ПАО «Мегафон», ПАО «Вымпелком», ОАО «Лентелефонстрой» и других. В рамках научной Школы осуществляется постоянно действующий проект – инициативная научно-исследовательская работа по проблемам инновационного развития и управления качеством в инфокоммуникациях.

Результаты этой работы неоднократно докладывались на различных международных конгрессах, форумах и конференциях (ЮАР, Франция – 2008 г.; Мексика – 2011 г.; Москва – 2011–2014 гг.; Санкт-Петербург – 2009–2019 гг.).

Частью этого проекта является выполнение хоздоговорных НИР, в частности:

1. «Разработка методических рекомендаций по формированию кооперационной стратегии научно-производственной компании ООО «Лазер-Граффити» при реализации системных проектов интеллектуального освещения, систем отображения информации и мониторинга» (заказчик – ООО «Лазер-Граффити», 2015–2016 гг.).

2. «Принципы коллективного использования радиочастотного спектра применительно систем подвижной связи общего пользования» (заказчик – ООО «Спектрум Менеджмент», 2018 г.).

3. «Разработка методических рекомендаций по организационной и маркетинговой политике компании «Гейзер-Телеком» (заказчик – ООО «Гейзер-Телеком», 2019 г.) и др.

Результаты проведённых НИР используются в производственной деятельности предприятий и организаций и при формировании планов инновационного развития.

Материалы научной деятельности НОШ используются в учебной работе в СПбГУТ: при чтении лекций, разработке учебно-методических пособий и постановке новых курсов, написании ВКР, а также служат основой для проведения диссертационных исследований. В рамках Школы к научным исследованиям привлекаются не только аспиранты, но и студенты. Только в 2019 г. участниками НОШ совместно со студентами было опубликовано более 10 статей в научных журналах и материалах международных научных конференций (например [2, 6]). Магистерская диссертация студента Устрикова Н. К. (н. р. проф. Макаров В. В.) на тему: «Конвергенция информационных технологий в условиях цифровой экономики» прошла отбор для участия в конкурсе на соискание премий Правительства Санкт-Петербурга за выполнение дипломных проектов по заданию исполнительных органов государственной власти Санкт-Петербурга в 2019/2020 учебном году (решение Комиссии от 06.11.2019).

Преподаватели Школы (руководитель коллектива, к. э. н., доцент кафедры ЭМИ Верединский С. Ю.) стали победителями Грантового конкурса Фонда Потанина 2019–2020 года для преподавателей магистратуры в номинации Новая магистерская программа.

Выигравшая конкурс, магистерская программа «Управление внедрением цифровых технологий в отрасли экономики» реализуется для решения задач, сформулированных в соответствии с задачами национальной программы «Цифровая экономика РФ», утвержденной протоколом заседания президиума Совета при Президенте РФ по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7.

В рамках НОШ профессор Макаров В. В. активно сотрудничает с другими вузами страны: СПбГЭУ, НИУ ИТМО, СПбПУ Петра Великого, МТУСИ, РЭУ имени Г. В. Плеханова. Регулярно оппонирует диссертации,

является председателем ГЭК по специальностям Бизнес-информатика, Менеджмент, Управление качеством и др., рецензирует учебники и монографии.

Список используемых источников

1. Ярошевский М. Г. Логика развития науки и научная школа // Школы в науке / Под ред. С. Р. Микулинского, М. Г. Ярошевского, Г. Кребера, Г. Штейнера. М., 1977. С. 7–96.

2. Макаров В. В., Старкова Т. Н., Устриков Н. К. Цифровая экономика: эволюция, со стояние и резервы развития // Журнал правовых и экономических исследований. 2019. № 4. С. 222–229.

3. Блатова Т. А., Макаров В. В., Шувал-Сергеева Н. С. Количественные и качественные аспекты измерения цифровой экономики // Радиопромышленность. 2019. № 4. С. 63–72.

4. Макаров В. В. Телекоммуникации России: состояние, тенденции и пути развития. М. : Информационное и рекламно-издательское агентство по связи и информатике, 2007. 296 с.

5. Макаров В. В., Шувал-Сергеева Н. С. Управление внедрением инноваций на рынке программного продукта; Санкт-Петербург. СПбГУТ, 2018. 160 с.

6. Стародубов Д. О., Макаров В. В., Александрова Н. А. Конкурентоспособные стратегии инновационного развития корпоративных структур // Евразийское Научное Объединение. 2019. № 5–4 (51). С. 291–293.

УДК 654.01
ГРНТИ 49.01.75

УПРАВЛЕНИЕ ЗНАНИЯМИ – ТЕНДЕНЦИЯ РАЗВИТИЯ МЕНЕДЖМЕНТА ОРГАНИЗАЦИИ

В. В. Макаров, Т. Н. Старкова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современных условиях данные, информация и знания с одной стороны накапливаются во все больших объёмах, с другой стороны остаются только частично востребованными. С точки зрения менеджмента знаний это обстоятельство вызвано трудностью добычи, превращения полученных знаний в цифровую форму, проверки их полноты и достоверности. Менеджмент знаний становится все более актуальным не только для отдельных отраслей, но и для развития цифровой экономики в целом. Таким образом, необходимо формировать у работников интеллектуального труда навыки по работе со знаниями в условиях цифровой экономики. Координаторы знаний, своевременно предоставляя знания и информацию всем сотрудникам, обеспечат возможность многократно использовать лучшие разработки, знания и извлечённые

из опыта уроки, что будет способствовать повышению эффективности менеджмента организации.

знание, менеджмент знаний, работник интеллектуального труда, координатор знаний.

В современной интерпретации с одной стороны знание представляет собой набор данных и информации (с точки зрения некоторой определённой информационной технологии), с другой представляет собой интеллектуальный капитал личности, который можно представить в следующем виде:

$$ИК = ИК_0 + \sum_{n=1}^{\infty} (b_n \cdot K_n^j),$$

где $ИК_0$ – стадия знаний, соответствующая уровню при приёме сотрудника на некоторую должность, выраженная в наборе его компетенций и уровне их освоения; b_n – индекс освоения определённого вида знания (компетенции) в процессе производственной деятельности и повышения квалификации; K_n^j – величина определённого n вида знания (значений величин, идей, методов решения проблем, информационных технологий, коммуникаций, нормативной документации и т. д.) для j – уровня развития отрасли и общества в целом.

Главная функция интеллектуального капитала – существенно ускорить прирост массы прибыли за счёт формирования и реализации, необходимых предприятию систем знаний, вещей и отношений, которые в свою очередь обеспечивают его эффективную хозяйственную деятельность [1]. Интегрированные системы современных предприятий включают и менеджмент знаний, который развивается по своим правилам, учитывая международные и национальные рекомендации и стандарты.

Знание является контекстным, то есть востребовано только тогда, когда это необходимо или же в ответ на соответствующий стимул или совокупность определённых условий, которые могут быть связаны с общей историей, окружающей средой или обстановкой. Рассмотрим исторические аспекты, связанные с понятием «знание» и управление знаниями.

Высказывание «знание – сила» особую популярность приобрело в XX веке, и было использовано как название, основанного в январе 1926 г. «Ежемесячного научно-популярного и приключенческого журнала для подростков». Журнал «Знание-Сила» ставил своей первостепенной задачей естественнонаучное и техническое просвещение школьников. За почти 100-летную историю журнал, как и вся экономика нашей страны, претерпевал значительные изменения, при этом основным направлением своего развития в настоящее время редакция считает: *«установление связей между*

разными областями науки и мысли и самое главное – выявление человеческого смысла всякого знания» [2]. На 8 лет позднее был основан ежемесячный научно-популярный иллюстрированный журнал широкого профиля «Наука и жизнь». Первый номер журнала «Химия и жизнь» вышел в марте 1965 г. Главным редактором журнала были заведены правила, которым следовали все те, кто работал в журнале «Химия и жизнь», – «информированность, уважение к фактам, преданность знанию, полная отдача делу, корректность в споре, дотошность в работе с мелочами, доброжелательность, бесстрашие».

Наряду с результатами научных исследований и дискуссий в журналах уделялось большое внимание применению изобретений и рационализаторских предложений на производстве и в быту. Так как избытка ресурсов не было, внедрение какого-либо знания происходило по принципу: семь раз отмерь и один раз отрежь. При этом существенное значение имело и то обстоятельство, что некоторые важные понятия такие как: «безлимитное» использование воды, воздуха, газа, землепользование и т. д. было предметом обсуждения в научных изданиях ещё 80 лет назад. Сопоставление ситуаций в регионах с различными климатическими условиями, социальной средой создавало у читателя более гуманное настроение по отношению ко всем ресурсам. При этом возникали разнообразные течения научной мысли, связанные с технологической революцией и имеющие широкое распространение среди различных слоёв населения. К таким явлениям можно отнести изучение: возможности межгалактических видов цивилизаций, использования различных источников энергии, создание новых видов растений и животных, и т. д. Занятие научными исследованиями могли выполняться только на работе, только дома или и первое, и второе одновременно. При этом проверка на истинность и закрепление знания осуществлялись многократным пересказом о сделанных наблюдениях, использованных методах и полученных результатах всем тем людям кто составлял сферу общения исследователя. Обмен знаниями на предприятии осуществлялся путём проведения научно-технических конференций, методических семинаров и производственных совещаний; а накопление в научно-технических библиотеках, отделах стандартизации, бюро рационализации и изобретательства. Однако такой способ управления знаниями, во-первых, не учитывал эффективность от реализации какого-либо изобретения или патента, не был встроен в бизнес-процессы, проходящие в организации, не имел единого ресурса и поэтому постепенно пробрёл чисто формальный характер. Современная инфокоммуникационная индустрия трансформировала основные понятия менеджмента знаний такие как: получение знаний и обучение, планирование, коммуникативность, взаимоотношения, переведя их в электронную форму. Развитая компьютерная индустрия обеспечивает мультисервисность, телекоммуникационная индустрия позволяет осуществлять

высокоскоростной и всеобъемлющий доступ к информационным ресурсам, медиа индустрия расширяет границы познания, а цифровая экономика использует многофункциональную коммуникативность доступную в равной степени предприятиям любой формы собственности и масштаба деятельности. Особенностью цифровой экономики часто называют прозрачность контроля над деятельностью предприятия, что естественно обуславливает необходимость каждого сотрудника быть ответственным за результат. При этом на бизнес-процессы, проходящие в организации, воздействует множество внутренних и внешних факторов, объективный учёт которых возможен только при наличии у всех сотрудников потребности вносить свой вклад в поток знаний и информации между организацией и внешним миром (рис.).

Учитывая размытые границы при обмене знаниями, возрастает роль координаторов знаний – людей, роль которых состоит в формировании компетенций, способствующих приобретению, систематизации, созданию, использованию и обмену знаниями [3]. На предприятии, в условиях неразвитых систем менеджмента знаний, роль координаторов могут выполнять, например, менеджеры: по связям с общественностью, по труду, по работе с клиентами.

Рис. Размытые границы и обмен знаниями

Менеджмент знаний можно представить в виде обобщённого сценария:

1. Запрос на решение проблемы, выполнение работ.
2. Изучение внутренних знаний.

3. Принятие решений об актуальности существующих решений или высказывание сомнений относительно об актуальности.

4. Обмен внешними знаниями.

5. Реализация обновлённого проекта.

6. Накопление знания в базе, с указанием значений сбалансированных показателей менеджмента организации.

При этом менеджмент знаний имеет свои собственные показатели, такие как:

– скорость установления связей, реакции на требования рынка и принятия решений;

– удовлетворённость клиентов актуальностью способов выполнения проектов;

– эффективные партнёрские отношения и союзы, обеспечиваемые (поддерживаемые) ИКТ и необходимые для внедрения новых способов работы в рамках всей цепочки поставок и логистики;

– мощность и производительность системы менеджмента знаний, позволяющей организовать поддержку мобильных трудовых коллективов в течение 24 часов семь дней в неделю в случае необходимости [3].

Следовательно, для того, чтобы быть востребованным на рынке труда каждый студент (выпускник вуза) должен осознать следующие аспекты в области менеджмента знаний:

– все сотрудники организации – это информационные работники;

– менеджмент знаний – это основная часть работы каждого сотрудника организации;

– успешная работа в области знаний требует определённого сочетания различных навыков, отношений и моделей поведения;

– информационная грамотность – это важный навык для информационного работника;

– модели поведения при обмене знаниями лежат в основе развития требуемых навыков и компетенций;

– неформальные сети и роли в них могут быть полезными при обмене знаниями.

Список используемых источников

1. Макаров В. В., Семенова М. В., Ястребов А. С. Интеллектуальный капитал. Материализация интеллектуальных ресурсов в глобальной экономике / Под ред. В. В. Макарова. СПб. : Политехника, 2012. 688 с. ISBN 978-5-7325-0965-6.

2. Журнал «Знание-Сила». URL: https://znanie-sila.su/istoriya-zhurnala (дата обращения: 30.01.2020).

3. ГОСТ Р 57134-2016. Менеджмент знаний. Мастерство приобретения знаний. Руководство по наилучшей практике.

УДК 338.47
ГРНТИ 49.38.99

КОНЦЕПЦИЯ СОЗДАНИЯ СИТУАЦИОННОГО ЦЕНТРА ГУБЕРНАТОРА ЛЕНИНГРАДСКОЙ ОБЛАСТИ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ИНСТРУМЕНТОВ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ

В. В. Макаров, Н. Ф. Урусова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается концепция создания Ситуационного центра Губернатора Ленинградской области, выступающего единой точкой сбора аналитической информации и являющегося одним из первых примеров практической реализации концепции управления регионом на основе интегрированного сбора данных. В информационно-аналитической системе Ситуационного центра применяются современные технологии обработки больших данных. Ситуационный центр может использоваться для принятия решений первыми лицами, как в экстренных ситуациях, так и в режиме регулярного управления регионом.

ситуационный центр, информационно-аналитическая система, интеграция информационных ресурсов, модульный принцип.

Разрозненные способы аналитического обеспечения информацией Правительства Ленинградской области стали основанием для создания Ситуационного центра Губернатора Ленинградской области. Для решения внутренних задач органов исполнительной власти области и органов местного самоуправления внедрены 82 информационные системы, но они используются только локально. Основаниями для инициирования проекта стали нормативно-правовые акты РФ [1, 2, 3].

Целью создания Ситуационного центра является обеспечение Губернатора, Правительства Ленинградской области и других пользователей Центра качественными цифровыми инструментами для принятия управленческих решений на основе комплексного мониторинга состояния наблюдаемых объектов, событий, процессов, анализа их причин и последствий, а также прогнозирования развития ситуации, как в экстренных случаях, так и в режиме оперативного и стратегического планирования.

Для этого необходимо ввести в действие первый технологический компонент цифровой системы управления регионом на основе концепции Data-driven region (управления, основанного на данных) – организационно-технический комплекс Ситуационного центра.

Ситуационный центр Губернатора Ленинградской области включает в себя:

– создание специализированных помещений для работы первых лиц области, оснащенных комплексом необходимого компьютерного, телекоммуникационного, мультимедийного оборудования и программного обеспечения;

– создание мобильного комплекса на базе планшетного компьютера для работы Губернатора Ленинградской области;

– создание и внедрение информационно-аналитической системы Ситуационного центра Губернатора Ленинградской области, включающей набор средств хранения, сбора, обработки, визуализации информации, моделирования и прогнозирования [4].

Информационно-аналитическая система решает следующие задачи:

– обеспечение унифицированного сбора и загрузки данных из различных информационных источников, в том числе интеграция с различными информационными ресурсами, с обеспечением мониторинга процесса сбора данных;

– прогнозирование и моделирование общественно-политической ситуации, социально-экономического развития и состояния региональной безопасности Ленинградской области;

– мониторинг закупочной деятельности Заказчиков; решение экспертно-аналитических задач социально-экономического и общественно-политического развития Ленинградской области;

– стратегическое планирование по направлениям пространственного развития, комплексной безопасности, развития отраслей промышленности, сельского хозяйства, торговли, науки и образования, бюджетного планирования, а также разработка государственных программ Ленинградской области;

– контроль исполнения планов и программ;

– формирование перечня показателей в соответствии с должностными полномочиями подразделений и сотрудников органов исполнительной власти;

– управление информационными потоками и визуализацией данных, поступающих из интегрированных информационных систем, других источников информации;

– прогнозирование динамики социально-экономических показателей состояния общества (региона);

– оценка влияния государственных программ и национальных проектов на значения социально-экономических показателей состояния общества;

– оценка рисков выполнения государственных программ и планирование их предотвращения;

– анализ состояния инженерной и социальной инфраструктуры и сопоставление с направлениями социально-экономического развития Ленинградской области;

– анализ и ранжирование угроз региональной безопасности;

– анализ и прогнозирование социальной напряженности.

Решение этих задач достигается путем реализации в информационной системе модульного принципа, которая включает в себя соответствующие модули («интерактивная карта», модуль мониторинга государственных закупок и деятельности заказчиков, модуль визуализации данных и т. д.) и подсистемы (подсистема экспертизы и сбора сведений, подсистема аналитической обработки информации, подсистема обеспечения информационной безопасности и т. д.).

Информационно-аналитическая система Ситуационного центра Губернатора Ленинградской области осуществляет интеграцию информационных ресурсов правительства области и федеральных ведомств.

Работа Ситуационного центра предусмотрена в трёх основных режимах:

1) В плановом режиме Ситуационный центр обеспечивает предоставление информационно-аналитических материалов Губернатору в виде набора интерактивных информационных панелей в соответствии с одним из базовых сценариев работы. Информационные панели могут включать как агрегированную информацию из различных информационных систем, так и результаты аналитической обработки данных с необходимой визуализацией. Внутри панелей имеются специализированные инструменты как для более глубокого анализа данных, так и для аналитической работы (инструменты корреляционного анализа, анализа данных в динамике с усреднением и без, и т. п.).

2) В случае возникновения экстренных и чрезвычайных ситуаций центр обеспечивает поддержку оперативного принятия решений как на основе типовых сценариев работы в ЧС, так и с помощью универсального набора инструментов для экстренных ситуаций (видео- и аудиосвязь с экстренными службами, изображения с видеокамер с мест событий, отображение на карте дислокации и движения транспортных средств и иных объектов, метеосводка, релевантная информация из соцсетей с мест событий).

3) При проведении крупномасштабных мероприятий в регионе на базе Ситуационного центра обеспечивается информационное обеспечение и взаимодействие различных ведомств и служб. В этом случае используется сочетание инструментов для оперативного реагирования на ситуацию и аналитического инструментария.

Эффективность работы Ситуационного центра обеспечивается интеграцией с ключевыми информационными системами и источниками дан-

ных (государственная автоматизированная система «Управление», региональная информационно-статистическая система Ленинградской области, геоинформационная система Ленинградской области «Фонд пространственных данных», Система-112 Ленинградской области, региональные системы управления финансами и закупочной деятельностью, информационные ресурсы ФСО России).

Система отображения видеоинформации представляет собой видеостену из 9 экранов и обеспечивает представление информации для коллективного просмотра во время докладов при обсуждении проблемных вопросов и других действий, осуществляемых при работе группы управления в ситуационном зале.

В базовом режиме на видеопанели доступны карта Ленинградской области с информацией о происшествиях и месторасположении камер видеонаблюдения, изображения с камер видеонаблюдения, лента происшествий, мониторинг рейтингов региона, мониторинг показателей социально-экономического развития, мониторинг СМИ и т. д.

Ключевым результатом проекта является создание и внедрение комплекса инструментов для управления регионом на основе данных как в экстренных (чрезвычайных) ситуациях, так и в режиме регулярного оперативного и стратегического управления. Программно-аппаратный комплекс Ситуационного центра, и, в частности, его Информационно-аналитическая система, позволяет увеличить эффективность принятия управленческих решений на основе визуализированных, систематизированных данных, одновременно предоставляемых из различных источников.

Информационно-аналитическая система «Ситуационный центр Губернатора Ленинградской области» призвана стать основным «конечным» инструментом поддержки принятия решений первыми лицами региона на основе «витрин данных», формируемых информационными системами, с которыми интегрируется данная информационная система.

В настоящее время уже осуществлена интеграция с пятью информационными системами и, более, чем с двадцатью, источниками данных. За счет использования типовых сценариев, интеграции с источниками данных, автоматизированной загрузки данных, использования специально разработанной аналитической подсистемы, трудозатраты на подготовку отчетов к плановым мероприятиям Губернатора значительно снижаются. При углублении интеграции с другими информационными системами, в том числе и с организациями, предоставляющими платные информационные услуги [5], и внедрении региональной системы управления данными, снижение трудозатрат станет ещё более существенным.

Тем не менее, основной эффект интеграции информационных систем, созданных на базе инновационных технологий – качественный: повышение скорости и качества принимаемых решений [6]. Новизна заключается

в успешной практической реализации комплексного подхода к созданию и функционированию регионального Ситуационного центра.

Сегодня во многих случаях Ситуационный центр – это специализированное помещение с видеостеной и средствами конференц-связи. В Ленинградской области Ситуационный центр – это прежде всего мощная информационно-аналитическая система для принятия решений первыми лицами как в экстренных ситуациях, так и в режиме регулярного управления регионов. До создания ИАС «Ситуационный центр Губернатора» существовали лишь разрозненные способы аналитического обеспечения Правительства Ленинградской области: в регионе внедрены и локально используются для решения внутренних задач ОИВ, ОМСУ 82 информационные системы.

Ситуационный центр Губернатора становится единой точкой сведения аналитической информации. Единая платформа предоставляет возможность проводить кроссотраслевой анализ. Статистика позволяет оперативно управлять ситуацией, а также детализировать информацию, при необходимости, – до первичной.

Система позволяет проводить не только аналитические работы с данными, но и обеспечивает их визуализацию и предоставление без привлечения программистов, и разработчиков. В информационной системе используются современные технологии обработки больших данных. Ситуационный центр Губернатора Ленинградской области – это один из первых примеров практической реализации концепции управления регионом на основе интегрированного сбора данных.

Список используемых источников

1. Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О стратегии национальной безопасности Российской Федерации до 2020 года».

2. Указ Президента Российской Федерации от 25.07.2013 г. № 648 «О формировании системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия».

3. Распоряжение Президента Российской Федерации от 3 октября 2013 года № Пр-2308 «О концепции создания системы распределенных ситуационных центров, работающих по единому регламенту».

4. Шувал-Сергеева Н. С., Блатова Т. А., Макаров В. В. Внедрение информационнокоммуникационных технологий в организации: от оптимизации структуры до повышения конкурентоспособности // Радиопромышленность. 2017. № 2. С. 101–106.

5. Макаров В. В., Синица С.А. Информация как товар на рынке инновационных продуктов и услуг // Журнал правовых и экономических исследований. 2014. № 3. С. 20–22.

6. Мальцева У. В., Макаров В. В. Информационные технологии в практике управления качеством // Инновации. 2011. № 12. С. 116–119.

УДК 336.744
ГРНТИ 06.73.45

КРИПТОВАЛЮТЫ КАК «ЧЕРНЫЕ ЛЕБЕДИ» СОВРЕМЕННОЙ МИРОВОЙ ВАЛЮТНОЙ СИСТЕМЫ

А. В. Мешков, А. А. Симонина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются основные проблемы современной Мировой валютной системы, основанной на долларе США, и варианты ее реформирования. Обосновывается точка зрения, согласно которой криптовалюта в перспективе может стать основной формой мировых денег.

криптовалюта, мировая валютная система, мировые деньги, событие типа «черный лебедь».

Сам термин «событие типа черный лебедь» ввел в научный оборот Нассим Николас Талеб, американский экономист и трейдер в своей книге «Черный лебедь: под знаком неопределенности» (2007 г.). С точки зрения Талеба «черный лебедь» обладает тремя признаками:

1) Событие, которое невозможно предсказать, так как оно никогда не происходило ранее или наблюдалось ранее крайне редко.

2) При его появлении последствия оказываются очень значительными.

3) После того, как событие уже произошло, эксперты дают ему рациональное объяснение так, как будто оно было ожидаемо [1].

Важно отметить, что «черные лебеди» могут нести как катастрофические последствия, так и неожиданную удачу. Примером первого могут быть такие события, как начало первой мировой войны, распад СССР, террористическая атака на Нью-Йорк 11 сентября 2001 г., банкротство глобального инвестиционного банка *Lehman Brothers* в сентябре 2008 г. К «черным лебедям» со знаком «+» можно отнести изобретение двигателя внутреннего сгорания, персонального компьютера, интернета. Безусловно, 2020 г. останется в истории как год, в который на мировую экономику опустилась целая стая катастрофических «черных лебедей».

Это и пандемия короновируса, и неожиданный для большинства экспертов, разрыв сделки ОПЕК+, приведший к обвалу мировых цен на нефть и резкому падению индексов мировых фондовых бирж. Все эти события спровоцировали начало нового мирового экономического кризиса, который, начался, казалось бы, на пустом месте, но через некоторое время эксперты, конечно, найдут всему этому рациональное объяснение.

Лекарства, которыми предложено лечить нынешнюю рецессию, уже известны. Президент США предлагает эмитировать 6,2 триллиона долларов для борьбы с кризисом, что составляет 20 % ВВП США сейчас и больше ВВП этой страны 1990 г. Такое резкое увеличение предложения американской валюты может оказать дестабилизирующее воздействие на всю мировую экономику. Ведь доллар – это не просто национальная валюта США, а по сути мировые деньги в которых осуществляется 70 % трансграничных сделок. Как и кризис 2008–2009 гг. современный кризис вновь показывает главный недостаток современной мировой валютной системы (МВС). В отличии от эпохи золотого стандарта, когда единственным видом мировых денег признавалось золото, ныне существующая Ямайская валютная система (1976 г. – по настоящее время) окончательно закрепила демонетизацию золота и функцию мировых денег за несколькими национальными фиатными валютами. Хотя в настоящее время к числу мировых резервных валют МВФ относит доллар США, евро, китайскую юань, японскую йену и британский фунт, фактически современная МВС основана на долларе. Доля доллара в золотовалютных резервах центральных банков составляет 61 %, в международных расчетах 80 %, в кредитах и депозитах – 57 % и 59 % соответственно.

Таким образом, главное противоречие современной МВС в том, что доллар одновременно является и мировыми деньгами, и национальной валютой США, подчиняется американской политике и правилам монетарного регулирования, служит национальным интересам США. Будучи эмитентом мировых денег, США имеют существенные экономические преимущества. Если другие страны, увеличивая или сокращая количество денег в обращении, могут влиять лишь на свою национальную экономику, то США воздействуют таким образом на мировую экономику в целом.

Во-первых, США обеспечивает высокий уровень потребления, превосходящий внутреннее производство за счет неэквивалентного обмена с другими странами, прежде всего с развивающимися. Внешнеторговый баланс США, начиная с 1980-х гг., постоянно сводился с дефицитом, который возрос от нескольких десятков миллиардов долларов в 1980-х – начале 1990-х до 891 миллиарда долларов в 2018 г. Это сверхпотребление ведет к постоянному росту государственного долга, который достиг в настоящее время 20 трл долларов. Собственная мировая валюта без труда позволяет этой стране покрывать дефициты путем наращивания эмиссии долларовой массы.

Во-вторых, роль США как эмитента мировых валют, обеспечивает доминирование банковской системы США в мире. Дело в том, что безналичные сделки с нбациональной валютой проводятся в банках-резидентах и проходят исключительно по их счетам. Все операции в долларах проходят

через корреспондентские счета, которые открываются банками- нерезидентами в американских финансовых институтах. Таким образом, выпущенные в оборот безналичные доллары, функционируют в пределах американской банковской системы. Не удивительно, что самые крупные банки в мире-американские, ведь они контролируют подавляющую часть мировой банковской ликвидности.

В-третьих, регулирование долларовой массы ФРС (Федеральная резервная система США, выполняющая роль Центрального банка) происходит исключительно в интересах самих США, которые могут противоречить интересам других стран. Снижение процентной ставки ФРС и связанная с этим кредитная экспансия доллара в мировой банковской сфере и на финансовых рынках провоцирует раздувание финансовых пузырей, приток в ту или иную страну «горячих» денег, повышение курсов национальных валют, то есть все то, что может противоречить проводимой в других странах монетарной политике и создать здесь предпосылки кризисной ситуации. Наоборот, сокращение долларовой массы ФРС может привести к оттоку капиталов и падению курсов национальных валют, стимулирует инфляцию, приводит к обрушению финансовых рынков.

Необходимость реформирования МВС, основанной на долларе, стала уже достаточно очевидна. Но большинство предложений сводится в основном к тому, чтобы увеличить роль и вес других резервных валют, прежде всего юаня и евро, и тем самым потеснить позиции доллара США. На взгляд авторов этой статьи, это тупиковый путь. Те преференции, которые сейчас извлекают США как эмитент мировой валюты частично достанутся Китаю и странам зоны евро. Все остальные страны мира едва ли от этого выиграют. Вернуться к золотому стандарту тоже не реально так как дефицит золота как мировых денег будет постоянно сдерживать рост мировой экономики. Отсюда часто делается вывод, что как бы несовершенна была современная МВС, ее нечем заменить.

И этот был бы верен, если бы внезапно не прилетели «черные лебеди» в виде криптовалют. Появление криптовалют не мог предсказать никто, не потому что это электронные деньги, а потому что это децентрализованная валюта, за которой не стоит никакой центральный банк никакого государства. Иными словами, это частные деньги. А существование частных денег всеми экспертами считалось абсолютно невозможным. Всеми, кроме одного лауреат Нобелевской премии в области экономики Фридриха фон Хайека (1899–1992). В работе «Частные деньги» (1976 г.) Хайек утверждает: «Немалая часть современной политики основана на допущении, что правительство имеет власть создавать и заставлять народ принимать любой дополнительный объем денег по своему желанию. Правительства по этой причине энергично защищают свои традиционные права. Но по этой же причине важно, чтобы эти права были у них отняты» [1] Мировые деньги,

во-первых, не должны быть национальной валютой какой-либо страны, так как эта страна всегда будет иметь искушение решать свои проблемы за счет остального мира, облагая его сеньоражем. Во-вторых, по природе своей они должны быть неинфляционны. «История есть, по большей части, история инфляции, – пишет Хайек, – причем инфляции, устроенной правительствами и ради выгоды правительства». В-третьих, обращение мировых денег не должно контролироваться банками страны – эмитента мировой валюты. Авторам представляется, что криптовалюта обладает всеми этими свойствами в полной мере. Выше уже было сказано, что эта валюта децентрализованная, эмиссией криптовалют занимаются не какой-то криптовалютный банк, а майнеры, разбросанные по всему миру. Причем майнером-эмитентом криптовалюты может стать любой человек, обладающий достаточными для майнинга криптомонет компьютерными мощностями. Никто из майнеров и держателей криптоденег не заинтересован в обесценивании. Выпуск криптовалюты строго ограничен. Так, выпуск первой и самой популярной на сегодняшний день криптовалюты биткойна ограничена 21 млн «монет». Скорость майнинга ограничена скоростью мировой добычи золота. Важно и то, что обращение криптовалют происходит без посредников в виде банков страны-эмитента. Технология блокчейн позволяет осуществлять перевод денег непосредственно от одного пользователя к другому почти мгновенно и без посредников и комиссии. Кроме того, заморозить счет или изъять криптовалюту невозможно, а значит ее нельзя использовать как орудие санкций одной страны против других. Все это говорит о том, что криптовалюты могут претендовать на роль мировых денег и существенно потеснить в этой роли доллар, евро, любые другие национальные валюты. Но есть и серьезные возражения против этого. Противники криптовалюты ссылаются на то, что она ничем не обеспечена. Но чем обеспечен доллар США? Утверждается, что экономической мощью этой страны. Действительно, в конце 1940-х годов, когда доллар стал главной мировой резервной валютой, доля ВВП США в мировом ВВП составляла 50 %. Но в настоящее время она упала до 23 %, а при пересчете по паритету покупательной способности – до 10 %. Однако, спрос на доллары не снижается. Значит курс доллара, как и других валют определяется спросом и предложением, а не экономической мощью страны. В противном случае юань должен был бы уже сильно потеснить доллар в качестве мировых денег, однако этого не происходит. Другое возражение сводится к тому, что криптовалюты в любой момент могут запретить ведущие государства. В 2010 г. курс биткойна к доллару составлял 0,06 доллара за биткойн. Тогда его действительно легко было запретить, но никто не обратил на него внимание. В конце 2017 г. курс составлял уже 1 биткойн – 20 000 долларов. Как полагают многие эксперты, к концу 2020 г. из-за безудержной эмиссии доллара, биткойн снова достиг-

нет этого курса (сейчас 630 долларов). Капитализация биткойна сейчас составляет 116,2 млрд долларов, суммарная капитализация всех криптовалют-177,4 млрд долларов.

Такого джина уже не удастся запихнуть обратно в бутылку.

Список используемых источников

1. Талеб Н. Черный лебедь. Под знаком неопределенности. М. : КоЛибри, 2017. 736 с.

2. Хайек Ф. Частные деньги. М. : Институт национальной модели экономики, 1996. 116 с.

УДК 338.517.2
ГРНТИ 06.75.47

ЭКОНОМИЧЕСКИ ОБОСНОВАННАЯ ИНФОРМАЦИЯ – УСЛОВИЕ ОПТИМАЛЬНОГО ВЫБОРА ЭНЕРГОРЕСУРСОВ

Г. Н. Сапожников

Уральский технический институт связи и информатики (филиал)
Сибирский государственный университет телекоммуникаций и информатики

Экономическая эффективность результатов производственной деятельности зависит от достоверности и полноты информации. В статье показано, как экономически не обоснованная информация о ценах на энергоресурсы приводит к ошибочным выводам по выбору источников энергии. Например, вместо электроэнергии, из-за ее не оправданно высокой цены, выбирается природный газ, то есть не восполняемый ресурс, а ряд исследователей по этой же причине, рекомендуют автономные генераторы электроэнергии на газе, считая полученную электроэнергию в два раза дешевле по сравнению с энергией из электросети. При экономически обоснованных ценах такие выводы были бы исключены. В настоящей статье предлагается разработать алгоритм выбора оптимального источника энергоснабжения для определенного потребителя на конкретной территории.

достоверная информация, энергоресурсы, себестоимость, обоснованная цена, природный газ, оптимизация выбора.

Основой экономических исследований является информация о факторах производства, одними из которых являются ресурсы. За счет оперативности и достоверности данных о производственных факторах информация

служит основой выявления не обоснованных затрат, способствуя этим повышению эффективности экономической деятельности. Теория оптимального распределения ресурсов, за создание которой советский математик и экономист Л. В. Канторович в 1975 г. получил Нобелевскую премию по экономике, была основой для разработки стратегических планов в масштабах государства. Информационные технологии, которые прошли с тех пор огромный путь развития, дают возможность углубить оптимизацию, распространяя ее и на исходные компоненты планирования, включая ресурсы. Чтобы «распределение ресурсов» было оптимальным, надо обоснованно выбрать самые экономичные из них. При этом в первую очередь следует оптимизировать те ресурсы, если это технологически возможно, которые оказывают наибольшее влияние на результирующие показатели.

Рассмотрим возможность повышения эффективности конечного результата за счет оптимизации выбора ресурсов, на примере выбора энергии. Энергия занимает важное место как непосредственно в обеспечении существования человека, так и в его производственной деятельности. В нашей стране, где отопительный сезон на большей части территории длится более полугода, довольно высоки затраты на отопление и освещение. Расходы на это значительны как для населения, так и для промышленности. Размер этих затрат в квитанциях коммунальных платежей для населения в зимнее время составляет не менее половины общей суммы. Доля затрат на тепловую и электрическую энергию в себестоимости промышленной продукции составляет в среднем около десяти процентов, достигая по некоторым видам продукции сорока и более процентов [1]. Причем, многие исследователи отмечают, что доля наших энергозатрат в производстве продукции на 10–20 % больше, чем в странах Европы. Повышенную энергозатратность в быту и в производственной деятельности в нашей стране только частично можно объяснить более суровым климатом, не маловажное значение оказывает физический и моральный износ оборудования. Ещё более увеличивают энергозатраты повышенные транспортные и иные инфраструктурные расходы, вызванные нашими огромными расстояниями. В результате, затраты энергии на производство любой продукции и услуг на наших территориях в 1,5–2 раза превышают соответствующие показатели западных стран [2].

Приведенные данные показывают, что снижение энергетических затрат имеет существенное значение для улучшения экономического положения как населения, так и производственных предприятий. Обеспечение энергией и теплом может осуществляться разными видами энергоносителей. В качестве возможных источников тепла и энергии рассматриваются как природные виды топлива: уголь, нефть, газ и другие, так и электроэнергия от сжигания топлива на тепловых электростанциях, на гидроэлектростанциях, на атомных электростанциях и на источниках, так называемой, зеленой

энергетики (солнце, ветер, приливы-отливы и другие источники). В настоящее время заявляет о себе такой источник, как когенерация. Сторонники такой автономной электрогенерации считают, что цена этой электроэнергии в два раза ниже цены сетей общего электроснабжения [3].

Однако обоснованно выбрать наиболее дешевый источник энергии у нас невозможно, так как нет объективно установленной цены энергии. Когда цену электроэнергии в конце девяностых – начале двух тысячных годов устанавливали с активным участием РАО ЕС, увеличив ее в десятки раз от существующей, руководствовались необходимостью обеспечить прибыль возникшим ниоткуда хозяевам электростанций и распределительных сетей. В результате, доля затрат на электрическую и тепловую энергию в себестоимости продукции предприятий машиностроительного комплекса выросла с 1–2 % в 1990 г. до 16–20 % в 1999 г., на предприятиях легкой промышленности доля затрат на электрическую и тепловую энергию в себестоимости продукции с 8–9 % в 1995 г. достигла 17–19 % в 1999 г. [3]. Велики энергетические затраты и в агрокомплексе, например, в тепличном комбинате «Майский» в Татарстане, они составляют около 40 % себестоимости [4]. В результате, неоправданный рост стоимости электроэнергии п**р**ивел к снижению конкурентоспособности в нашей стране промышленного и сельскохозяйственного производства, что негативно повлияло на эффективность всей экономики страны, ухудшило ее импортно-экспортные возможности.

При выборе источников энергоснабжения необходимо учитывать:

– стоимость разных видов энергии, возможной к применению для конкретного потребителя на данной территории [5];

– затраты на транспортировку (доставку) определенного вида энергии, которые являются функцией удаленности объекта от источников энергии и объемов потребления;

– безопасности использования данного вида энергии;

– обеспечения экологических требований.

Каждый из этих параметров нуждается в оценке объективности его величины. В настоящее время сложились не обоснованные представления сравнительной стоимости разных видов энергии. По фактическим ценам оказывается, что самый дешевый вид энергии, это природный газ. Но это мнение, очевидно, основано на искусственно завышенной цене электроэнергии, с того периода, когда приватизировали генерирующие и передающие электрические системы. В результате цена на природный газ выглядит не сопоставимо низкой, в сравнении с ценой электричества.

Чтобы убедиться, что это сравнение объективно не обоснованно, достаточно сравнить цены на газ у нас и в Европе, где они в 5–15 раз выше [6]. Поэтому за счет этих произвольных цен газовое отопление в нашей стране оказывается в семь раз выгоднее электрического [7].

Для получения объективного представления о ценах, необходимо обратиться к их основам. Себестоимость электроэнергии тепловых электростанций составляет около 0,69 руб. за квт-час, атомных электростанций немного меньше, а гидростанций – всего 0,1 руб. за квт-час [8]. То есть отпускные цены электроэнергии превосходят себестоимость в первом случае в семь – десять раз, а во втором – более чем в сорок раз. Даже если учесть увеличение цены в полтора – два раза за счет расходов на передачу электроэнергии и общепринятых торговых наценок, то сравнение все равно будет не в пользу газа.

Уменьшает преимущества использования газа также его высокая пожаро- и взрывоопасность, несравнимая с электричеством. Аварийные происшествия с газом, видимо, чтобы уменьшить негативное психологическое воздействие от опасности его применения, в последнее время стали называть не взрыв, а «хлопок» газа, хотя при этом есть и пострадавшие, и материальный ущерб. Таким образом, сложившееся представление о ценах искажает подлинную картину сравнения.

Приведенные рассуждения не затрагивали территориальный аспект. Критики, указывающие отставание в газификации восточных регионов России, например, Красноярского края, Иркутской, Амурской областей, исходят из существующих цен на газ и электроэнергию. Если исходить из себестоимости гидроэнергии, в избытке вырабатываемой в Восточной Сибири, то становятся оправданными низкие темпы газификации этих регионов из-за отсутствия экономической целесообразности этого. Но чтобы эта причина была понятна и правильно воспринята, надо, минимум на порядок снизить отпускную цену электроэнергии для потребителей. По крайней мере, для Восточных регионов с их ресурсом гидроэнергии, которая к тому же – восполняемый ресурс, в отличие от газа.

Изложенное показывает необходимость разработать алгоритм эффективного обеспечения энергией потребителей разного объема потребления энергоресурсов, с использованием обоснованных стоимостных параметров, с учетом их удаленности от магистральных энергетических сетей. В алгоритме эффективности следует учитывать кроме затрат на производство, добычу и транспортировку энергии, также стоимость ее подготовки, преобразования и расходы на обеспечение безопасности и возможные затраты на ликвидацию аварий. Также необходимо учесть экологические требования.

Таким образом, алгоритм будет представлять математическую модель выбора наиболее экономически выгодного источника энергообеспечения конкретного объекта в зависимости от его удаленности от магистралей энергии и от объема требуемых энергоресурсов. Оптимизация выбора ресурсов станет существенной частью практического развития теории оптимизации ресурсов Л. В. Канторовича на современной информационной базе.

Список используемых источников

1. Иванов В. А. Анализ энергозатрат в различных отраслях промышленности [Электронный ресурс] // Интернет-журнал «Науковедение». 2015. Том 7, № 1 (январь – февраль 2015). URL: publishing@naukovedenie.ru (дата обращения: 10.01.2020).

2. Экономика социализма: устройство и принципы. URL: https://cont.ws/@anddan01/878646 (дата обращения: 12.03.2018).

3. Когенерация – как возможность снижения затрат на энергообеспечение. URL: http://www.alfar.ru/smart/2/372/ (дата обращения: 10.01.2020).

4. Нуруллина Л. А. Анализ влияния факторов объема потребления и цены энергетических ресурсов на изменение себестоимости выпускаемой продукции на примере ООО «тепличный комбинат «Майский» // Вектор экономики. 2017. № 4. С. 54–55.

5. Цены разных видов топлива. URL: https://www.eurostroy.ru/articles/zatrati_na_otoplenie_razlichnih_vidov_topliva (дата обращения: 12.01.2020).

6. Сколько платят за газ европейцы. URL: https://zen.yandex.ru/media/crisis/skolko-platiat-prostye-evropeicy-za-gaz-kuplennyi-v-rossii-5bc14a6db7a6b100ac90627b. (дата обращения: 12.01.2020).

7. Газ или электричество? Какое отопление выгодно для загородного дома. URL: https://nedvio.com/gaz-ili-elektrichestvo-chto-vygodnee/ (дата обращения: 12.01.2020).

8. Себестоимость электроэнергии в России. URL: https://zen.yandex.ru/media/id/5a73fb68f4a0dd61bfdcb3c1/sebestoimost-elektroenergii-v-rossii-i-kuda-i-pochem-ee-prodaiut-plakat-hochetsia-5c639405b39fad00ad2c1f79. (дата обращения: 10.01.2020).

ANNOTATIONS

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Kryukova E., Parashchuk I., Mikhaylichenko N. Quality Analysis of Electronic Libraries as Elements of a Telecommunication Media. – PP. 5–9.
The questions of the analysis of the quality of electronic libraries as the basic elements of the modern educational information and telecommunication infrastructure (media) are considered. The advantages, functions and tasks of electronic libraries are analyzed. The study was conducted to identify and analyze their significant properties. The analysis of approaches to assessing the quality of electronic libraries is carried out, the potential possibilities of quality analysis using well-known principles of the theory of interval means are considered.
Key words: electronic library, quality, indicator, infrastructure, attribute, document, information resource.

Avramenko V., Bochkarev D., Malikov A. Analysis of Modern Approaches to Responding on Computer Incidents. – PP. 9–13.
In the article analyzes modern approaches to organizing a response to computer incidents. The main response stages, implemented organizational and technical measures are considered. The main shortcomings of existing approaches to incident management are highlighted. An approach to automating the function of analyzing incidents based on machine learning methods is proposed.
Key words: analysis, security breach, computer incident, response, machine learning.

Avramenko V., Malikov A. An Approach to Authentication of Users of Infocommunication Systems Using Machine Learning. – PP. 13–17.
In the article proposes an approach to authenticating users during their session using automation tools based on a combined artificial neural network. As a result of training an artificial neural network, a reference information handwriting is generated for each user. During the functioning of the infocommunication system, a determination is made of the degree to which the current values of the characteristics of user actions correspond to their reference information handwriting.
Key words: authentication, information handwriting, artificial neural networks, autoencoder, event log.

Aduevskij A., Verhova G., Kucherevskij K. A New Generation Distributed LMS model. – PP. 17–21.

At the present time, educational process management systems are becoming more widely used in higher and secondary education. Such systems provide comprehensive automation and Informatization of the educational process, significantly improving the quality of training. The concept of a digital University imposes new, more stringent requirements for this class of systems. The results of the analysis of the current state and prospects of LMS development are presented. The advantages and disadvantages of existing educational process management systems are analyzed. It is shown that to meet the requirements of the digital University concept, LMS must be built on the principle of distributed systems.

Key words: LMS, digital University, educational process management system, distributed system.

Akimov S., Gordeev M. Prototype of a Software Module for Managing Information Links Between Agents of the Cyberphysical Environment. – PP. 21–23.

A prototype of a software module that implements the management of information links between agents that form a cyberphysical environment is presented. Agents of the cyberphysical environment are individuals, groups of individuals, and man-made objects that are hardware and software. The software module allows you to establish information-loaded connections between agents of the following types: P2P, B2B, M2M, P2B, P2M, B2M. as a result of establishing these connections, a semantic network is formed that reflects the relations between agents. Based on the information contained in the semantic network, it can be implemented to manage information processes involving the above-mentioned agents, in particular, access rights management. A software module that implements information communication management can be used in the formation of a unified information environment of a post-industrial society.

Key words: cyberphysical environment, information communications, post-industrial society, agents, P2P, B2B, B2C, P2P, P2M, R2M.

Akimov S., Davletshina E. Models and Algorithms for Automatic Rating Calculation for Distributed Cyber Environment of Virtual Enterprises. – PP. 24–28.

The article presents the results of analysis of the problem of automatic calculation of ratings of subjects of virtual enterprises. A model for calculating individual multi-criteria ratings of individuals and groups of individuals, performed in real time, is proposed. Group ratings are calculated based on the ratings of individuals who make up these groups. Structural divisions and legal entities can act as groups. Groups can form hierarchical structures. Ratings of higher-level groups are calculated based on the groups that are part of them. The considered models and algorithms are designed to reduce routine procedures, increase the level of transparency and objectivity of the results of continuous monitoring.

Key words: cyber environment, electronic portfolio, automation, virtual enterprises.

Akimov S., Yuplov V. Application of Delta Coding for Automated Control Systems. – PP. 29–32.

The article presents the results of research in the field of using Delta coding methods and algorithms for automated control systems. Delta encoding is one of the preferred methods for generating electronic documents, since it is based on the principles of presenting data as a difference (Delta) between successive data sets, instead of the data itself. Delta encoding reduces data transfer traffic and reduces the required storage volume for document versions.

One of the promising ways to apply Delta encoding in distributed automated control systems is to use document formats that implement this principle. Possible ways of using Delta encoding in automation of electronic document management by creating appropriate microservices and standard client web technologies (HTML, CSS, JavaScript) are considered.
Key words: Delta encoding, VCDIFF, Quill Rich Text Editor.

Akchurina D., Belov M., Grishchenko I., Sholukho Yu. Analysis of the Use of Computer vision in the Industry. – PP. 32–35.
The article presents an analysis of modern computer vision systems used in industry. The types of technical vision systems and image processing methods are considered. Factors contributing to the growth of the use of computer vision technologies in the Russian Federation are identified.
Key words: computer vision, image processing, technical vision, industry.

Andreev D., Tarasov V. Automated Processing of Requests for Technical Maintenance of Legal Entities. – PP. 36–40.
The results of analysis of help desk systems, the issues of process automation customer service identified tasks that should be solved by the automation system on the basis of which requirements for the system, suggested its concept and overall structure.
Key words: outsourcing, business process automation, help desk.

Aronov V., Verzhakovskaya M. Traffic Analysis Information System Based on Yandex.Maps Service Data. – PP. 41–47.
The information system allows you quickly analyze the traffic situation and make decisions on the formation and change the movement route. The results of this work can be implemented in various organizations that are engaged in logistics activities, as well as used for home and personal purposes.
Key words: information system, analysis, optimization methods, traffic situation, Yandex.Maps.

Atanov V., Krasov A. Comparison of Security Mechanisms for Different Versions of the Android Operating System. – PP. 47–52.
Android is an open source operating system for mobile devices and a corresponding open source project is led by Google.
Key words: Linux kernel, applications, android framework, android runtime, Address Space Layout Randomization (ASLR), Application Programming Interface (API), Transport Layer Security (TLS), BlueBorne, Service Discovery Protocol (SDP), Bytecode Viewer, Manifest, Common Language Runtime (CLR).

Akhmetova Y., Dolgun V., Kazakov D., Packan M. Peculiarities of Implementing the System of the Integration Data Bus, Constant on the 1C Platform in SPbSUT. – PP. 52–57.
This article demonstrates the problems and features of the implementation of the ISD system (Integration data bus), implemented on the 1C platform. The implementation of the ISD system consists of several stages: conducting a survey in the entire area, preparing and setting up the infrastructure, installing the ISD, conducting acceptance tests, training and consulting

workers, and conducting pilot operation. The purpose of the implementation is to increase the efficiency of activities by automating the university's business processes.
Key words: integration data bus, digitalization, automation, 1C, university, business process, education.

Babaeva A., Litvinov V. Intelligent System of Decision Making Support in the Field of Financial Analysis loan Organizations. – PP. 57–61.
The financial stability of the banking sector and the country as a whole largely depends on effective banking regulation and supervision. When analyzing the financial condition of credit organizations, a huge amount of data is taken into account. When making decisions on the application of supervisory response measures, classification, and the selection of a further strategy for regulating the activities of credit organizations, the curators analyze many different indicators and standards. The introduction of new intelligent data analysis technologies will increase the efficiency of the supervisory unit of banking organizations.
Key words: banking supervision, analysis of the financial condition of credit organizations, intelligent decision support systems.

Bazhin M., Ivanov V., Karev V., Lebedev A. Structure of the Software and Hardware Complex of the Automated Control System of the Communication Node. – PP. 61–66.
This article presents the structure of the software and hardware complex of the automated control system for the communication center, designed to organize automated planning, operation of communication centers and implement trunk monitoring of the state of communication channels and means using web technologies.
Key words: hardware-software complex, control system, communication center, distributed application, management organization.

Balakirev D., Gunina E. Analysis of Geometric Models of Water Surface Simulation for Real Time Rendering. – PP. 67–71.
In three-dimensional graphics, the use of water is not uncommon. However, the methods of constructing its geometric model are markedly different from the construction of the static models, since it not only varies with time, but also transforms according to its own laws. Their investigation and analysis, including the search for shortcomings depending on the simulation goals, as well as the construction of conclusions, is what this work is dedicated to.
Key words: 3D-graphics, programming, visualization, simulation, geometric model.

Balandin I., Ziberov V., Kukunin D. Distributed Denial of Service Attacks (DDoS). – PP. 72–76.
Today, denial of service attacks has become very popular in the world of computer technology. Because of them, many services suffered, companies lost profits and their customers. This article provides theoretical information about denial of service attacks, their types, methods of action, and the motivation of the people who organize these attacks.
Key words: DDoS, denial of service, attacks, security.

Baranov I., Nevrov A. Normative Act Transformation into Interagency Exchange Format within "Digital Economic" National Project. – PP. 76–81.
We have to exchange by normative acts inter different agencies. A part of normative acts be transformed into new format, but this transformation cannot be done automatic mode. Document template based format transformation automation considered.
Key words: normative act, monotype text document format, format transformation.

Belikov I., Makeev S. Development of the Intellectual Processing Algorithm for Big Data Using the Apache Spark Module. – PP. 81–86.
In this paper, we consider a variant of the algorithm for the intellectual processing of large amounts of information based on open source software. A block diagram of the algorithm is presented, a description of the method used for the intellectual processing of information received from the Internet to classify content by emotional coloring.
Key words: Big data, Apache Spark module, classification task, processing of text information in a natural language.

Biryukov A., Lipatnikov V. Network Control Method Based on Analysis of Network Traffic in Information Systems in the Presence of Anomalies. – PP. 86–91.
The current problem of ensuring the level of cybernetic security of critical infrastructures of automated control and communication systems for special purposes is considered. The analysis of methods for monitoring network traffic, advantages and disadvantages of each method, as well as a detailed description of the new method, which specifies the principle of its operation, is presented.
Key words: network control, traffic, anomalies.

Bovykin E., Verhova G., Prisyazhnyuk S. Research of Methods and Algorithms for Optimization of Automatic Routing of Robotic Systems in Order to Minimize Power Consumption. – PP. 91–94.
The article presents the results of research on methods and algorithms for optimizing the construction of routes for robotic systems in order to minimize power consumption. The optimization problem can be reduced to finding the shortest path on a directed graph, where the weight coefficients of the edges are proportional to the energy consumption of an Autonomous underwater vehicle, taking into account the maneuver being performed, the path length and the environment parameters. The proposed method allows you to decompose the solution of the problem into three stages: 1) building a three-dimensional grid consisting of all possible graphs of the direction of movement; 2) determining the weight coefficients of the graph edges based on information about the environment in which the underwater vehicle is moving; 3) finding the optimal path on the graph.
Key words: route building, automatic systems, numerical optimization.

Bogolepov G., Pronin A., Skibinsky I. Selection and Justification of Development Tools for Special Software in High-Level Languages for National Hardware Software Platforms. – PP. 95–98.
The actual problem of the transition of the Russian Armed Forces to the national hardware and software platform (NHSP) is considered. The problem of transferring special software is solved by rewriting programs in cross-platform programming languages. The aim of the work is

to ensure the effectiveness of measures to modernize existing special software during the transition to NHSP. The article presents the classification of development tools for the domestic hardware and software platform.
Key words: state secret, automated control systems, national hardware and software platform, cross-platform programming languages, Astra Linux.

Bondarenko I., Komkov G., Shimanchuk S. Methods for Assessing Effectiveness of the Cost on Information Security Companies. – PP. 99–103.
In this article researched of methods for assessing effectiveness of the cost on information security enterprises. An example from a well-known Microsoft company is considered, conclusions are drawn about the advantages and disadvantages of Total Cost of Ownership. A methodology for evaluating the effectiveness of information security based on the theory of Total Cost of Ownership is proposed with amendments to improve this technique. A technique is proposed in which the Total Cost of Ownership methodology together with the method of calculating the return on investment complement each other, creating the optimal methodology for assessing the effectiveness of information security costs for Russian companies. The application of the developed methodology for assessing effectiveness contributes to increase the profits of the enterprise, by minimizing direct and indirect costs that are not included in the budget of the company.
Key words: information technologies, information security, methods for assessing effectiveness, cost estimate for information security, TCO, information risks.

Borodyansky Y., Dagaev A. Using Splines Based on Second-Order Delta Transformations at Different Stages and Stages of Data Mining. – PP. 104–108.
The article describes the possibilities of using splines based on second-order Delta transformations at the stages of data preparation for analyzing patterns in case of possible incompleteness of the available data in time in order to restore them, as well as at the stage of visualization of results. Splines based on second-order Delta transformations, unlike classical parametric functions, are characterized by high performance, which is critical when processing large and super-large data volumes.
Key words: intelligent data analysis, interpolation, data mining, spline, Delta-transformations of the second order.

Botyakov V., Reznickij A., Solovjov D., Toporkov N. Artificial Neural Networks in Questions of Parametric Optimization of Complex Technological Processes of Optical Production. – PP. 108–113.
The questions of mathematical modeling of a complex technological process of pulling an optical fiber from a blank in the virtual space of a computer are considered. The issue of parametric optimization of this technological process is being worked out using ANN technologies.
Key words: computer-aided design systems, artificial neural networks, software, optical fiber, multilayer perceptron

Botyakov V., Reznitsky A., Soloviev D., Toporkov N. Method for Detecting Low-Intensity Dos Attacks on an Information System Using Artificial Neural Network Algorithms. – PP. 113–117.

The problem of protecting information systems from denial-of-service attacks is becoming the most relevant among most other information system security issues. The protection of such systems is becoming a time-consuming and resource-intensive task, and the question of developing fundamentally new systems for detecting attacks based on artificial intelligence algorithms becomes acute.

Key words: *neural networks, denial of service, perceptron,self-organizing maps.*

Botyakov V., Reznitsky A., Soloviev D., Toporkov N. Methods for Carrying Out Distributed DoS Attacks to the Information System. – PP. 117–121.

The issues of ensuring the information systems security from attacks on denial of service are considered, and the classification of such attacks is given.

Key words: low-intensity DDoS attacks, botnet, RUDY, SlowLoris, HTTP-flood.

Bushuev S., Komashinsky V., Pantyukhin O., Parashchuk I., Saenko I. Creating a Perspective System for Information Access Control in Cloud Infrastructures of critical Information Objects. – PP. 122–127.

The architecture of a perspective system for information access control in cloud infrastructures of critical information objects based on the application of ABAC and RBAC access control models is presented. The main components of the system are described. The results of its implementation are discussed.

Key words: access control, cloud infrastructure, crucial object.

Bystrov I., Litvinov V. Intelligent System of Decision Making Support System When Working with Optional Strategies on Financial Markets. – PP. 127–131.

In modern society, trading in the financial market is becoming increasingly popular due to the possibility of obtaining additional profit due to the use of many instruments, such as stocks, futures and derivative options. However, the options market often discourages new and even experienced investors due to its specific terminology and variety of strategies. This leads to the fact that investors lose a huge set of opportunities that provide options for money management. Under these conditions, there is a need to create an Intelligent Decision Support System that analyzes the selected tools in conjunction with their standard parameters, which allows us to predict and visualize the behavior of the strategy developed by the investor.

Key words: financial market, option, pricing model, Intelligent Decision Support Systems.

Vaganov A., Vachugova V. Development and Research of Methods for Controlling the Concentration of Impurities in Liquid Dispersed Media. – PP. 131–135.

Issues related to the development of a method and system designed for continuous monitoring of the concentration of impurities in liquid media transported through a pipeline are considered. The relevance of this control is explained and a review of existing similar methods is performed. A model of a non-contact optical turbidimetric measuring transducer is provided, on the basis of which a block diagram is developed and the choice of a modern element base for the development of the measuring system as a whole is justified. Recommendations are given on the application of the mathematical apparatus and the study of sensor and system models,

as well as practical recommendations are formulated for the development of devices of this class.
Key words: dispersion, non-contact converter, turbidimetry, sensor.

Vaganov A., Ivanov A. The Primary Signal Processing Path, as an Element of the Data Acquisition System in ACS. – PP. 136–141.
The article discusses issues related to the design of the primary signal processing path from the measuring transducers (sensors) in various automated control systems. The need for preliminary normalization of the signal for its subsequent secondary processing is explained. The choice of a modern element base for the development of a path in the form of discrete-analog dynamically programmable electronic circuits is justified. Recommendations on the use of the mathematical apparatus and the study of models are formed. An example of the implementation of a fragment of the primary signal processing path in a specialized graphical programming environment with its subsequent modeling is given. Recommendations of a practical nature for the development of devices of this class are formulated. During development, a traditional mathematical apparatus is used.
Key words: ACS, discrete-analog circuits, signals, processing path.

Vaganov A., Ishkova A. Estimation of Efficiency of the Electronic Block Layout in ACS. – PP. 142–147.
The article discusses issues related to the development of a method designed to assess the effectiveness of the placement of electronic units in the devices of an enterprise management system, taking into account such important criteria as electromagnetic compatibility, distribution of thermal fields, strength characteristics, dust and moisture protection, etc. The relevance of this development is explained. a method based on a literature review and analysis of existing assessment methods. The idea of constructing an algorithm that allows us to evaluate the overall efficiency of the placement of individual components of the system based on the analysis of individual criteria is proposed. Recommendations on the use of the mathematical apparatus and the study of the resulting models are given. Practical recommendations are formulated for developing methods of this class.
Key words: ASC, layout, automated control systems, electromagnetic compatibility, thermal calculation, signal preprocessing path, efficiency assessment.

Verhova G., Grigor'eva A. Backup Methods and Models for Digital Management Environments. – PP. 148–151.
Ensuring continuous backup of information stored in modern management environments is one of the most important tasks. Backups should be performed frequently enough that if a failure occurs, it is possible to return to the latest current version, and it is necessary to ensure that the information being copied is presented rationally to avoid excessive backups. The report provides an analysis of backup methods and models for modern management environments. Scientific-based proposals for the selection and implementation of backup methods and models for digital management environments are presented.
Key words: backup system, backup methods, digital environments.

Verhova G., Kolesov D. Research of Algorithms for Automatic Get Away from Obstacles by an Autonomous Underwater Vehicle Based on Echolocation Data. – PP. 151–156.
One of the main and most complex problems of controlling an autonomous unmanned underwater vehicle is the underwater navigation to avoiding possible obstacles. Situation is aggravated in deep water by the complex relief of the bottom surface. The issues of returning the underwater vehicle to a given trajectory after an evasion maneuver are considered in the publication.
Key words: path planning, path finding, obstacle avoidance, algorithms, autonomous vehicle.

Verhova G., Prisyazhnyuk S., Fedorov N. Stabilization of the Location of an Autonomous Underwater Vehicle under the Influence of Current. – PP. 156–160.
Autonomous underwater remote-controlled vehicles are a promising type of underwater equipment that can solve a wide range of tasks in automatic and semi-automatic modes. The advantages of Autonomous underwater vehicles are their relative cheapness and lack of risk for operators. This type of equipment can be used for searching and examining underwater objects, as well as performing various manipulations. The operation of Autonomous underwater vehicles under the influence of underwater currents requires the use of measures to stabilize the position of the device. The task of stabilizing the position of the underwater vehicle is quite difficult and requires the use of complex mathematical algorithms and technical solutions. The article considers existing approaches to stabilization of underwater remote-controlled vehicles under constant external influence of the current, and also proposes a hierarchical architecture of the stabilization system, which provides invariance of modules implementing stabilization algorithms to sensors and actuators.
Key words: underwater uninhabited remote-controlled vehicles, stabilization, underwater currents, MEMS, PID controller, unified architecture for controlling an unmanned underwater vehicle.

Verhova G., Prisyazhnyuk S., Hvostov M. Research of Methods and Algorithms for constructing and Optimizing the Route of Underwater Vehicle Movement in the Conditions of Complex Bottom Surface Relief. – PP. 161–163.
One of the most important tasks of managing unmanned vehicles operating in autonomous mode with minimal operator involvement is to build an optimal route in conditions of difficult terrain of the bottom surface. The solution of this problem requires performing a grid approximation of the space in which the uninhabited underwater vehicle functions, converting the grid into a graph, and finding the optimal path on this graph. The article presents the results of analysis of graph construction methods for determining the optimal path of the underwater vehicle, taking into account several factors. We consider meshes with a uniform, random distribution of vertices, the distribution of vertices in triangulation, mapping of meshes to a graph, and algorithms for finding the optimal path on the obtained graphs.
Key words: route optimization, optimal path search, optimization algorithms, graphs, grid approximation.

Viharev A., Markin D. The secure Terminal Program System Based on Onion Virtualization of Executable Code. – PP. 164–169.
The article contains the description of the secure terminal program system based on onion virtualization of executable code. The object of protection is described. The protocol of secure

interaction and algorithms for functioning of system modules are developed. The system performance was confirmed experimentally.
Key words: virtual machine, obfuscation, interpreter, bytecode, protocol of secure interaction.

Voloshenenko D., Litvinov V., Trofimova L. Intellectualization of Functional and Cost Analysis Information Processes and Systems. – PP. 169–173.
The article considers the implementation of machine learning in the procedure for performing functional cost analysis (FCA). The stages of the FCA were identified, and the information characteristics of the stages and procedures were analyzed to determine the information model of the FCA process. A simulation of a machine learning algorithm to help with the object's FCA is performed. Summarizing the advantages and disadvantages of machine learning when performing functional cost analysis.
Key words: machine learning, intellectualization, functional and cost analysis, information model.

Voloshinov D., Ges A. Features of Modeling Personalized Sewing Goods. – PP. 173–178.
The article discusses the features of modeling personalized garment products. CAD software complexes presented on the foreign and domestic market are described. Methods of removal of individual measures are given. The method of designing and modeling of products with the help of free software is proposed.
Key words: individual sewing, 3d design of clothes, parameterization of anthropometry.

Voloshinov D., Kaznacheeva E., Khaibrakhmanova E. Using Telegram Bot for Support Technical Service. – PP. 178–181.
Currently innovations and technologies are being introduced in all spheres of our life. Active introduction of the latest systems. In order to keep up with the times for most office workers, using a messenger on the phone will facilitate communication with the technical support department to save time and accurately describe the problem.
Key words: telegram bot, messenger, technical support.

Voloshinov D., Soloveva A. Development of an Algorithmic Complex for Solving Problems of Constructive Geometry. – PP. 182–186.
The article is devoted to the issues of automated synthesis of constructive geometric models that allow programming geometrically determined tasks by visual-graphic means. The article formulates the requirements for systems of this kind and presents a simplex geometric modeling system developed by the authors of this article.
Key words: Structural geometric modeling, Simplex, visual design systems.

Volynkin P., Kononjuk O. Investigation of the LSB Steganographic Method Using Keys to Determine the Data Embedding Area in Image Containers. – PP. 186–190.
Digital steganography methods are used in order to ensure the confidentiality of transmitted data and protect copyrights to digital multimedia formats in the conditions of a developed network data exchange structure. The most popular of the steganographic methods is the method of replacing the least significant bit (NSB) due to its low computational complexity and high payload. This article discusses modifications of this method using steganographic keys

for clearly defining or adaptive selection of information embedding areas. Image files are defined as the media due to their redundancy and wide distribution.
Key words: information security, steganography, image files, NSB, secret key.

Vorobyov A., Voronetsky A. Algorithm for Restoring Omissions in Nominative Sociological Data using the Multiple Imputation Method. – PP. 191–194.
The article considers the results of the analysis of various types of omissions that occur in the course of conducting sociological surveys and actual methods used in practice to restore sociological data measured in nominative scales. The main result of the analysis of methods was the choice of the multiple imputation method. To improve the capabilities of this method, an approach was used to translate variables measured in nominal and ordinal scales into fictitious ones using dichotomization. To solve the problem of selecting independent variables that improve the quality of recovery (prediction accuracy), a series of experiments were conducted and rules were formulated based on them, which were later implemented in an algorithm for finding missing values in sociological data based on the multiple imputation method.
Key words: sociological survey, restoration of incomplete data, undecided respondents, multiple imputation method, statistical experiment, algorithm.

Vorontsov D., Mikhaylichenko N., Parashchuk I. Features and Quality Indicators of Identification Features Input Devices as modern Software and Hardware Means of Access Control to Information Infrastructure Objects. – PP. 194–199.
The results of the analysis of the features of input devices and reading identification features designed to control access to information infrastructure objects, to elements and resources of information systems are considered. A variant of the formulation of quality indicators of devices of this class, focused on the possibility of their quantitative assessment in the interests of supporting decision-making on the optimal choice of specific products for real-world access control tasks, is proposed.
Key words: identification features input device, access control, quality indicator, unauthorized access, information infrastructure object.

Vostrukh A. Terminology Basis for Evaluating User Interfaces: Overview of Standards. – PP. 200–207.
The article deals with the problem of measuring the quality user interfaces of software products using metrics and concepts used in standards. A comparative analysis of existing guidelines and normative and technical documentation, including international standards, with the recording of shortcomings and inaccuracies in defining concepts and criteria for evaluating user interfaces.
Key words: user interface, usability, standards, terms and definitions, user experience, interface evaluation parameters.

Galiev R., Saenko I. Application of Modern Systems of Electronic Document Circulation in Order to Increase the Effectiveness of Management of Scientific and Educational Activities of Universities of the Russian Federation. – PP. 208–210.
In modern conditions, the electronic document management system (EDMS) is increasingly acquired. Increase the effectiveness of their activities. As part of the work, modern existing

electronic document management systems will be provided within the framework of state institutions, large enterprises, as well as small organizations. In addition, to improve management efficiency in the scientific and educational sphere of the Russian Federation.
Key words: electronic document management; electronic document; university administration.

Germanova E., Fedorova A. Creating the Stages of Interface Development of a Mobile App with Using UX / UI Design Principles. – PP. 211–216.
The article is devoted to the current trend in the development of graphical interfaces. The stages of developing a mobile application interface are considered, which are presented in the form of a sequence of steps that form the life cycle of the development of the user interface. The stages of design development are based on the principles of UX / UI design, studying of user experience, the rules of graphic design and their joint application in preparation for the design phase of the application and design.
Key words: mobile application, step-by-step development, user interface, UX / UI design.

Glazkov G., Khoroshenko S. Analysis of the Existing Human Resources Software. – PP. 216–220.
Personnel management refers to a large number of different tools, methodologies and concepts. For a start-up or incompetent head of a small company, the existing staff management capacity may seem complex and incomprehensible. The areas of human resources management development have been considered, a comparative analysis has been carried out of available software solutions in the area of personnel management, and options have been proposed for the implementation of personnel management programmers for new managers.
Key words: information systems, personnel management, personnel management, software.

Glubin P., Shestakov A. Automation of Life Cycle Procedures for University Intellectual Activity Results. – PP. 221–225.
The article considers system-technical solutions for building a system of automated accounting and maintenance of intellectual activity results of an educational institution (University) based on the principles of building product lifecycle management systems. An interface environment for forms of reporting documents is proposed, information from which is the information basis for making decisions to ensure the commercialization of intangible assets (IA) of the University and to maintain intellectual property objects in an up-to-date state during their life cycle. The use of original software solutions makes it possible to ensure the completeness and reliability of information that has legal significance for maintaining the document flow of commercialized IA.
Key words: esults of intellectual activity, automated accounting of movement of intangible assets.

Gorban S., Krivtsov A., Nikonov E. Adaptation of Blockchain Technology Protection Methods for Information Systems. – PP. 225–229.
The article discusses the methods of protecting blockchain technology and their adaptation for a distributed messaging service. Examples of such an implementation for a prototype of a developed service using blockchain technology are given.
Key words: blockchain, information security, security, distributed service, key, message.

Gordievich G., Tarasov V. Application Concept for Automating Administrative Tasks in a Real Estate Agency. – PP. 229–233.
The concept of a cross-platform application in the form of a chatbot in Telegram, written in Google Script – a script language based on Java Script, for comfortable integration of applications with Google services. The main stages of creation are described, and the selected technological solutions are justified.
Key words: Google App Script, JavaScript, Telegram, chatbots.

Grigorieva E., Shestakov A. IT Solutions in Data Process Management for Remote Sensing in Network Infrastructure. – PP. 233–239.
The existing processes of organizing the collection and processing of Earth remote sensing data are analyzed based on standard system solutions and tools as applied to the business processes of communications enterprises and topological objects of communications infrastructure. Typical remote sensing data processing techniques are considered. The possibility of distributed updating of spatial data on topological objects of communication infrastructure under the current tasks of the business processes of communication enterprises in order to reduce material and time costs is being investigated.
Key words: linear communication objects, monitoring automation, spatial data, Earth remote sensing, data processing.

Gromov V., Serova M. Comparative analysis of virtual and augmented reality technologies. – PP. 239–242.
With the constant development of computer vision and an exponential increase in the computing power of computers Augmented Reality and Virtual Reality technologies are becoming more and more visible. Due to some coincidence in the applications and functions of augmented and virtual reality, sometimes these terms are confused or used incorrectly. This article will identify AR and VR and explain the main differences between them.
Key words: virtual reality, augmented reality, headsets, VR devices, AR devices.

Gromov V. Microcomputers and Prospects Their Development in the Modern Training Process. – PP. 242–245.
The report discusses the main directions of development of microcomputer systems in the educational process. Examples of creating information systems in the educational process based on Raspberry PI microcomputer systems are considered. The question of teaching the skills of administering complex information systems is examined using the example of the server platforms Raspberry PI and SUSE Linux Enterprise Server.
The possibility of applying modern academic programs on the use of modern operating systems with the possibility of building mock-ups simulating complex industrial systems in the educational process is being considered.
Key words: Microcomputers, information systems.

Gromov V. Key Problems of Standardization in Russia. – PP. 246–250.
The report discusses the challenges of introducing interstate and national standards in Russia, as well as possible options for amending existing and newly introduced standards. This article discusses examples of changes in interstate standards, and also analyzes the general state of the standardization system in Russia.

Key words: interstate standards, national standards.

Gubin A., Litvinov V., Filippov F. Information Efficiency Digital Smoothing Filters. – PP. 250–254.
The issues of evaluating the information efficiency of digital smoothing filters are considered. The studies are based on the analysis of changes in the entropy and dynamics of information processes of smoothing random signals, as well as on the concept of Kolmogorov complexity of the information object and entropy potential.
Key words: information, mining, filtering, Kolmogorov complexity.

Gubin A., Litvinov V., Filippov F. Control Lateral Inhibition Procedure Realization. – PP. 254–258.
The lateral inhibition procedure is used in models of neural networks designed for self-training. Based on the "winner takes all" rule, the competition function requires large computational costs. The lateral inhibition procedure realization is proposed, which greatly simplifies calculations and allows control of the self-learning process.
Key words: neural networks, competition function, lateral inhibition.

Gubin A., Litvinov V., Filippov F. Technologies for Developing Intelligent Decision Support Systems. – PP. 258–262.
The paper considers the essence, basic concepts, classification, and architecture of intelligent Decision Support Systems (DSS). A study of methods for developing and designing intelligent DSS was conducted. It is shown that the future of Intelligent DSS lies in the flexibility of solutions, since none of the known approaches (classical models, machine learning, game theory) is universal in terms of the effectiveness of solutions for all problems.
Key words: Intelligent Decision Support Systems, Data Mining, Data collection.

Gulyaeva K., Panihidnikov S., Sakova N. Aircraft Noise Monitoring in the Area of Pulkovo Airport. – PP. 263–268.
Intensive development of air transport increases the noise load in nearby cities. The work considers noise pollution of residential areas adjacent to Pulkovo Airport. Noise assessment was carried out at several points of the air town. Noise monitoring data are presented, a conclusion is made about unacceptable noise levels. The paper presents data on the imperfection of the regulatory framework in the field of noise pollution.
Key words: Equivalent noise level, maximum noise level, aircraft noise.

Gunina E., Moiseeva A. Study of the Methodology for Editing Audio Material in Broadcasting. – PP. 268–272.
Acquiring new knowledge through audio transmission is publicly available. Creating audio material to inform listeners requires the use of certain methods. However, there is the problem of attracting the attention of the audience and the perception of the information received. This article discusses the method of editing audio recordings for use in the field of broadcasting. As a result of the study, stages of work on the audio recording were proposed, which can serve to develop an algorithm of actions, which will not only improve the quality of work, but also accelerate the process of obtaining the result.

Key words: radio broadcasting, audio editing, sound engineering, sound track.

Gurbatov G., Panichev A., Ushakov I. Comparative Analysis of IaaS (openstack) and PaaS (openshift). – PP. 272–276.
Cloud services become more and more popular among application developers, network engineers, huge and small IT companies. Cloud computing helps to avoid expensive maintenance of own infrastructure cost during make development process with different complexity level These technologies provide flexibility of resources: faster application development with auto-healing and auto-scaling configurable policies provide users possibility to avoid interaction with OS layer and virtualization layers, pay-as-you go system.
Key words: PaaS, IaaS, Openstack, Openshift, Kubernetes, cloud computing, virtual infrastructure.

Dvornikov A., Kapchuk N., Savchenko S. Software «Terrier» Version 3.0 to Search and Secure Information Destruction on Disk. – PP. 277–282.
During the work, the principles of recording information on various types of media were considered, methods for guaranteed destruction of information from carriers were analyzed, experiments were conducted on the search for and guaranteed destruction of information using the Terrier 3.0 software.
The aim of this work is to analyze storage media using the search and guaranteed destruction program "Terrier 3.0".
Key words: information carriers, methods of information destruction, information security.

Dichenko S., Korsun N., Simorin B. Selecting the Best Data Representation in Storage Systems for the Possibility of Carrying out the Control of Their Integrity. – PP. 283–285.
The operation of modern data storage systems of information-analytical systems is based on the processing of large data arrays by means of various types and various architectures. One of the most urgent tasks in this case is the organization of data storage, ensuring the identity of the data from the operator that sent them to the storage and the decision maker when requesting their use.
Key words: data storage systems, information and analytical systems, integrity control, multidimensional representation of data.

Dulkov M., Fabiyanovsky I., Saenko I. Improving the Speed of Processing Unstructured Data in Distributed Information Systems Based on Blockchain Technology. – PP. 286–291.
The problem of operational processing of unstructured data in distributed information systems is considered. Increasing their operational processing through the use of blockchain technology is discussed. The problem statement for the development of a model and methodology based on it is formulated, and ways to solve it are proposed.
Key words: unstructured data, blockchain technology, information resource, distributed information system.

Dymchenko A., Ptitsyna L. Model Analytical Intelligence of Multi-Agent Early Warning Systems. – PP. 291–294.

The intellectualization of early warning systems has been updated. The advantages of combining agents for detecting sudden changes in the statistical properties of controlled invariants are described. The key principles of complexing agents are identified in order to increase the efficiency of detecting changes in the statistical properties of controlled invariants. Formal procedures for describing models of complexation of detection agents are proposed. The process of forming the model analytical intelligence of multi-agent early warning systems is disclosed.

Key words: early warning, intelligent agent, integration, invariant, detection speed, characteristics, model analytical intelligence.

Dubonos A., Evglevskaya N., Karasenko A., Lauta O. Simulation of an Information Network Node Behavior in DDoS Attack. – PP. 295–299.

This article discusses one of the most serious types of intentional impact to block/impede users' access to the provided resources, called DDoS attack. The purpose of this work is simulation of an information network node behavior in the DDoS attack. Developed model allows to demonstrate the state of the information network node during DDoS attack. Simulation results are planned to be used in training an artificial neural network to detect DDoS attacks in order to develop system to protect information networks.

Key words: simulation model, ddos attack, information network, load level.

Evglevskaya N. The Research of Computer Attacks Detection Possibility Based on Artificial Neural Networks. – PP. 300–304.

The article presents the research results devoted to the choice of architecture of the artificial neural network, analysis of input data and output data, choice of activation function, learning algorithm of artificial neural network to solve computer attacks detection tasks. To detect computer attacks, such as DoS attacks, the anomaly behavior detection technology was used. To determine the structure of the network, a series of machine experiments were conducted, theirs results are presented in this work.

Key words*:* attacks detection method, artificial neural network, computer attack, DoS-attack.

Elagin V., Rebrov D. Analysis of Characteristics of Additional Services on the Communication Network of a Mobile Operator. – PP. 304–309.

The report describes one of the most popular additional services on the mobile operator's network. Its main features, method of construction and main characteristics affecting the operation of the service as a whole are specified. All elements of the network that are involved in the implementation of the service and the goals that are pursued in the implementation of these elements are described.

An analysis of the main characteristics that affect the provision of the service has been carried out. Methods of changing and improving these characteristics to achieve the required quality of services are described.

Key words: VAS, operator's network, SIP, UDP.

Ershov A., Nosov M., Shurygin B. WAAS Availability Monitoring Algorithm Based on Local Augmentation System Data. – PP. 309–315.
The actual problem of monitoring the availability of the required GNSS navigation characteristics in real time, the solution of which is required for train control automation, is considered. The main approaches to the monitoring of the availability of GNSS users of the wide-area augmentation system, which is used as a prototype, are analyzed. It is shown, that the using WAAS can lead to an underestimated expected availability of navigation characteristics in comparison with the real situation. Instead of a network of WAAS reference stations, it is proposed to use local augmentation systems and direct measurements of locally dependent range measurement errors. In this case, a significant improvement in positioning accuracy can be achieved. Modernized algorithm for determining protection levels using data from LAS is proposed.
Key words: availability, required navigation characteristics, rangefinding errors, algorithm, control, system, modernization.

Ershov A., Nalimov K., Nosov M. Methods for Passing Parameters in a Procedure on the Elbrus Operating System. – PP. 315–318.
This article discusses methods for passing parameters in a procedure in low-level assembler language on the Elbrus operating system. This question can be used both to increase program optimization or to increase the level of security.
Key words: key parameters, transmission methods, assembler, low-level language, optimization, security.

Zharanova A., Kapitonenko V., Filippov F. Security of Web Applications on a Risk-Based Authentication Model. – PP. 318–323.
The relevance of using a risk-based authentication method is justified. The influence of the risk-based authentication approach on the security of web applications is described. The advantages of using a risk-based authentication model of web applications in comparison with common data protection methods are presented. A risk-based authentication model has been developed. Identified typical user parameters required for the implementation of secure authentication. Based on the selected parameters, a risk-based web application authentication mechanism is described. The prospects of developing a risk-based authentication are identified.
Key words: web application security, authentication, risk-based authentication model.

Zharanova A., Ptitsyna L. Analysis of How the Distribution Property Affects Performance of Complex Information Security Systems. – PP. 324–327.
The relevance of the development of complex information security systems is substantiated. The purpose of analysis of how the distribution property affects performance of complex information security systems is determined. A performance profile of complex information security systems has been selected. A task of expanding the complex information security systems range has been set. Methodology for defining profile indicators has been selected. A generic section of model extension is presented.
Key words: information security, complex information security systems, distributed systems, modeling.

Zhilin V., Lipatnikov V. User Interaction in a Single Data Warehouse. – PP. 328–333.
The interaction of users when working in a single data warehouse is considered. Modern operating systems and computing environments ensure that users work efficiently on all the data they need. However, tracking the integrity of information is problematic for the average user. A solution to the problem of organizing work in a closed environment where users work in a single information space is proposed. All actions can be tracked by the distribution device.
Key words: distribution device, users, rights, operations, data, read, write, change, hash sum.

Zhusov D., Kozlenko A. Approach to Monitoring Changes in Information Web-Resources. – PP. 334–336.
The urgency of information web-resources changing control task is established in the work. Decision variants for assigned task in the point of view by investigation of different functional web-portals mechanisms is listed. The periodicity control estimation method in conditions of known frequency computer attack exposure and information resources modification time estimation method in condition of successful computer attack realization are considered. Users requests and rejection for information resources analysis functional model is developed.
Key words: information web-resources, web-resources changing control, computer attacks.

Zakalkin P. Threats to the Security of Critical Infrastructure of the State. –PP. 337–342.
The article discusses the main techniques used in the framework of APT attacks carried out by hacker groups. In addition, the main features and stages of conducting APT attacks against critical infrastructure of the state are described.
Key words: APT attacks, critical infrastructure, cyberspace.

Zverev A., Markin D., Saklakov A. The Methods and Technologies of Obfuscation and Deobfuscation of JavaScript Web-Application Source Code. – PP. 342–347.
The article contains the description of the Entry point identification algorithm base on dynamic analysis method and Selenium web driver tool. The authors present the decision of informational optimal model development problem. The application based on dynamic analysis method and Selenium web driver tool are suggested and described. This application allows to analyze obfuscated JavaScript code to identify remote web application entry points.
Key words: fuzzing, obfuscation, JavaScript, web application, Selenium.

Zikratov I., Kazmin M. Optimization of Motion of Unmanned Vehicles. – PP. 347–351.
One of the main trends in the modern world is the gradual increase in an increasing number of unmanned vehicles due to the fact that it will simplify the many life aspects of both ordinary people and the production cycles of large companies and corporations. It is also understood that due to automation and optimization of control, unmanned vehicles should reduce the level of incidents and relieve traffic on the roads.
Key words: unmanned vehicles, automation, optimization, control, road.

Zolotov O., Ptitsyna L., Temnikova M. Organization of Intelligent Content Search for Distance Education Systems. – PP. 351–356.
The modern conditions for the development of a knowledge society are presented. The main directions of improving distance education systems in the interests of the digital economy are

highlighted. The determining factors for the development of expandable structures of competencies models of the digital economy are described. The key features of methods and means of intellectual content search for distance education systems are analyzed. Innovations in the architecture of intelligent content search systems are proposed. Innovations are aimed at expanding the situational flexibility of architecture. Conceptual models of intelligent content search systems for distance education systems have been built.
Key words: knowledge, education, search, content, intellectualization, service oriented architecture, service.

Ivanov A., Kleverov D., Kleverov M., Saenko I. Organization of a Data Warehouse in a Perspective Cloud Infrastructure Access Control System. – PP. 356–360.
The issues of creating the data warehouse in a perspective system of access control for cloud infrastructure information, in which an attribute-oriented model of access control is used, are discussed. The ability to share SQL, XML, and RDF data is justified and demonstrated.
Key words: data warehouse, access control, cloud infrastructure.

Izrailov K., Kuznetsov S. The use of Artificial Intelligence and Machnie Learning Methods to Search for Vulnerabilities in Source Code. – PP. 361–366.
The article considers the possibility of using artificial intelligence in the field of information security. A method for resolving a contradictory subject area is provided, which consists in the following: narrow focus of standard algorithms when detecting specific vulnerabilities according to a strictly specified pattern in comparison with changing versions of software leading to the use of "fluctuations" of its code. As a result, a hypothetical method is proposed for identifying software vulnerabilities by training artificial intelligence with malicious samples of source code. The results of such training can be used for probabilistic detection in the studied software of parts of the code that belong to different classes of vulnerabilities, but which are not identical to any of the available samples. A basic featured model of the source code is proposed that contains information about vulnerabilities and is suitable for machine learning methods.
Key words: artificial intelligence, neural networks, source code, vulnerabilities, information security.

Izrailov K., Tatarnikova I., Fedorova A., Shirev V. Comparative Analysis of Plagiarism Checkers. – PP. 366–371.
This article shows us the definition of concepts which are related to check text programs for borrowings and originality identifying – so called plagiarism checkers. The author provides the results of the verification experiment of scientific papers in three different systems. There is a comparative analysis of the most famous programs which is carried out according to various criteria. The paper proposes us the experiment conclusions which are related to further information systems and technologies promotion in the field of software development
Key words: plagiarism, borrowing, text originality, uniqueness, check criteria, plagiarism checkers, expert systems.

Kadyntsev A., Ptitsyna L. Information and Analytical Decision Support System for Stimulating the Educational Activities of Teachers. – PP. 372–375.

The development of information systems of educational institutions has been updated. The expediency of creating an information-analytical decision support system for stimulating the educational activities of teachers is shown. The conditions of stimulation are presented. The grounds for the selection of decision rules are considered. The key features of the taxonomy method are described. The mathematical support of the information-analytical decision support system for stimulating the educational activities of teachers is disclosed. The possibilities of a comprehensive assessment of the effectiveness of educational activities of teachers are demonstrated.

Key words: education, teacher, information and analytical system, decision support, stimulation, software.

Kadyntseva D., Ptitsyna L. Simulation of a Multi-Agent System for Monitoring the Equipment of Electric Networks, Gas Equipment and Water Supplies in the Sphere of Housing and Communal Services. – PP. 375–379.

The reasons for the development of intelligent monitoring systems in the field of housing and communal services are described. The relevance of creating a multi-agent system for monitoring the equipment of electric networks, gas equipment and water supply for housing and communal services has been substantiated. An extended object-oriented model of the proposed monitoring system is built. The indicators of the quality of functioning of the monitoring system and the method of analysis of the constructed model are selected. The model-analytical intelligence of the monitoring system in the field of housing and communal services is presented.

Key words: intelligent systems, monitoring, housing and utilities, multi agent system, model, quality, model analytical intelligence.

Kazarin M., Lipatnikov V. Risk-Oriented algorithm of Work of Multifactor Biometric Threshold System for Separating a Secret with a Key Generation. – PP. 380–385.

Known authentication methods for users of information systems using special protection measures in modern conditions are not effective enough, since any authentication factor can be compromised. The goal is to develop a method of authentication of users of information systems based on a threshold scheme, to increase the efficiency of authentication of users of the information system.

Key words: authentication, information networks, threshold schemes, algorithms, multifactor biometric system.

Kalegin M., Musaeva T. CPA Channel as a Method of Effective Attraction of Target Traffic. – PP. 385–388.

CPA-model is a model of payment for online advertising, in which only certain (targeted) user actions are paid on the advertiser's site. An action may be direct purchase of goods, registration, subscription to newsletters, viewing a promoted video, downloading files, replenishing the balance, installing the application, filling out the feedback form, and so on.

Key words: CPA, lead, affiliate network, advertising, webmaster.

Kireeva N., Pozdnyak I., Filippov N. Development of a Decision-Making Algorithm for an Expert Information Security Assessment System. – PP. 389–392.
In the modern world, expert systems are used to solve various problems. In particular, the issues of information security audit of an automated system can also be considered with the help of expert systems. The article offers one option of the decision-making algorithm of the expert information security assessment system to fight against modern information threats aimed at critical information objects of industrial systems and digital productions.
Key words: expert system, industry component, standards, risks, information security, decision-making.

Kozintsev D., Shiyan A. Containerization for Analysis of Big Data on the Example of Kubernetes and Docker. – PP. 393–396.
Every day, the volumes of processed information are growing exponentially. In this regard, an increase in resources is required. In this regard, it is necessary to increase the efficiency of the use of available resources. For these purposes, virtualization and clustering tools have been created.
Key words: virtualization, containerization, data lake, ETL, distributed systems, BigData.

Kozlova L., Kucherenko I. Adaptation of the Monitoring System of Distributed objects in Order to Increase the Level of Enterprise Security. – PP. 397–401.
With the advent of new intelligent technologies for processing and analyzing incoming information from monitoring objects, new opportunities are opening up in the field of ensuring the safety of distributed enterprises. The article describes the optimization of the typical architecture of a monitoring information system that provides comprehensive control and prompt response in case of emergency situations.
Key words: information system, monitoring, distributed objects, security, architecture.

Kozlova L., Laba R. Modern Approaches to the Development of Distributed Systems Electronic Document Management. – PP. 401–405.
Currently, electronic document management is one of the key elements of digitalization in any field of activity, which allows to accelerate the processes associated with the movement and coordination of documents and make them more transparent. The article discusses the main modern approaches to the development of electronic document management systems, which are based on new technological trends, such as ubiquitous mobile corporate, cloud models and much more.
Key words: distributed system, electronic document management, scaling, traceability, protection of information, application system.

Kozlova O. Blockchain – Possibility of Building Decentralized Data Processing System. – PP. 405–408.
Modern technologies are not standing still, and the concept proposed a few years ago of building a decentralized data processing system is gaining popularity, finding its application primarily in the economic sphere. The article sets out the principles of the construction of such systems, their peculiarities, advantages and disadvantages.
Key words: blockchain decentralized systems, cryptography.

Kolesnikov A., Ushakov A. The Identification of Software Implants in Applications by Means of Dynamic Binary Instrumentation. – PP. 408–411.
This article describes a method for implementing dynamic analysis using dynamic binary instrumentation technology. The main tool considered in the work is DynamoRIO. The instrumentation process used in this tool is described. The aim of this work is to increase the security of applications by identifying software implants in them.
Key words: dynamic analysis, dynamic binary instrumentation, fuzzing, base unit.

Kolesnikov A., Hilko A. The Automated Dynamic Analysis of Software with Dynamic Binary Instrumentation DynamoRio. – PP. 412–415.
This article describes a method for automating dynamic analysis with DynamoRio API functions. The main advantages and disadvantages of automation in this way are described. An example of software analysis automation is demonstrated. The aim of this work is to increase the security of application by identifying undocumented features.
Key words: dynamic analysis, dynamic binary instrumentation, automated analysis, processor instructions.

Koltsov P., Khaibrakhmanova E. Role in Designing Prototyping of Information Resources. – PP. 415–420.
This article describes the role of prototyping in the design of information systems, the creation of prototypes of information resource pages for a service aggregator. A comparative analysis of English-language information platforms. The article discusses the approach to prototyping information systems. The basic requirements for the prototyping of information systems are identified.
Key words: prototype, prototyping, usability, user interface, information systems.

Komlev G., Pesikov E. The Solution to the Problem of Optimizing the Selection of Assortment, Sales, Market Segments and Prices for Services of a Communications Company. – PP. 420–426.
The implementation of one of the possible approaches to the formation of a marketing strategy for a communications enterprise based on the application of operations research methods and allowing to optimize the selection of assortment, supply volumes, market segments and prices for communication services is considered. The results of solving the problem of nonlinear partially integer programming using the proposed heuristic method based on an iterative increase in prices for communication services and solving the problem of linear partial integer programming at each step of the price by the Land and Doig method are presented.
Key words: enterprise, marketing management, optimization model, communication service, target segment, sales volume, price, hierarchy analysis method.

Kosov P., Shiyan A. Optical Illusions Perception Specificity by Computer Vision. – PP. 426–429.
Computer vision is actively used in industries such as agriculture, medicine, automotive, etc. In addition, CV and artificial intelligence (AI) are able to help in the research of those areas of science that are still poorly understood. One such area is the study of optical illusions.
Key words: optical illusions, computer vision, perception systems.

Kosolapov V., Lipatnikov V., Shevchenko A. A Method for Managing Cybersecurity Based on Service Traffic Analysis. – PP. 430–434.
The possibility of increasing protection of an information network by introducing the method of control cybersecurity an information network based on the analysis of official traffic forecasting security events. A method for network monitoring of service traffic is proposed. Introduced procedures for recognizing an illegitimate user trying to access protected resources of the information and computing network. An algorithm for detecting the sequence of actions of the intruder, determining the vector and strategy of cyber intrusion has been developed. Situational parameters are taken into account in a mutually hostile environment with a reliable forecast of the attack vector.
Key words: information and computing networks, network control, information protection, cybersecurity.

Kotkina M., Ptitsyna L. Analysis of the Influence of Structural Composition on the Statistical Profile of Planners of Intelligent Information Agents. – PP. 435–439.
The advantages of introducing computational intelligence into information infrastructures are described. The architectural diversity of carriers of computational intelligence in the form of intelligent information agents is considered. Actual directions of expanding knowledge about the quality of functioning of intelligent information agents are determined. The alternatives in the structural composition of the planners of intelligent information agents are highlighted. The elements of the statistical profile of planners are described. Components of planner models are presented. A methodology for analyzing the influence of structural composition on the statistical profile of planners has been formed.
Key words: architecture, intelligent agent, structural composition, statistical profile, planner model.

Kryukova E., Parashchuk I., Chernyavsky A. Analysis of Tasks, Functions and Signs of Modern Electronic Libraries. – PP. 440–445.
The questions of the analysis of signs, properties and features of modern electronic (digital) libraries are considered. The stages of their development, advantages, functions and tasks are analyzed. The study was conducted in order to identify and analyze the essential properties of these IT-infrastructure objects in the interests of reliable and multi-criteria assessment of their quality and functioning efficiency.
Key words: electronic library, sign, document, classification, information resource, access.

Kuzkin A., Kutsakin M., Ryabokon V. Actual Software Vulnerabilities. – PP. 445–450.
This paper presents an example of actual software vulnerabilities and errors based on OWASP classification and metrics. It concerns many different ways for exploiting some vulnerabilities that may be different by difficulties in searching, exploiting and security risks. Actual most dangerous software defects are shown: from SQL injection to wrong security configuration. Also the most common approaches for increasing software security according actual vulnerabilities are presented.
Key words: information security, software, vulnerabilities.

Kukunin D., Maslova E., Shumilov S. Cloud Technologies. Advantages and Disadvantages of Cloud Technologies. – PP. 451–455.
The article discusses the introduction of a very entertaining and promising technology - cloud technologies or in common - the "cloud" in the IT infrastructure of business organizations. The article reveals the concept of cloud technology. The main three cloud service models are presented, their classification is analyzed. The article also presents the main advantages and disadvantages of cloud technology. The topic is quite important and relevant nowadays, since many services and business processes already work or use remote servers and cloud storage. **Key words:** cloud technologies, «clouds».

Kurnosov V., Shestakov A. Features of Alarm System Functioning in Telecommunication Systems. – PP. 455–460.
Methods of management of complexes of hardware and software of telecommunication system on the basis of resource-saving technologies and features of functioning of its control system are considered. A generalized model of information and logical paths of the signaling and control subsystems interacting in the system is proposed. The model of network service on ensuring interaction of subsystems is presented. Results of researches of the organization of construction of a network of data exchange of control system of telecommunication system and probabilistic-time characteristics of information exchange are resulted.
Key words: telecommunications, alarm systems, data exchange network, probabilistic-temporal characteristics.

Kutsakin M., Lapko A. The Technique for Verifying the SQL-Queries Correctness. – PP. 461–465.
The article is devoted to the development of the technique for verifying the SQL queries correctness. The verifying general idea is to compare the resulting data sets returned by the tested query and the sample query. Fixing the identity of the resulting data sets is performed using the testing SQL instructions. The testing SQL instructions composition for various SQL-queries is presented. The initial data and limitations of the technique are given. The technique for verifying the SQL-queries correctness is described in detail.
Key words: database, SQL-query, verifying the SQL-queries correctness, the sample query, the testing instruction.

Lebedev N., Ostrovsky Y., Fedoseev D. Development of a Method of Search of Relevant Images Based on Machine Learning. – PP. 466–471.
The development of search methods using patent images makes patent expertise more qualitative, international. Drawings omission may indicate an incomplete description of the invention and entail the rejection of patent applications and other problems. The classification of patent images is difficult. Since patent images, even if one considers images of the same type, class, etc., are unique, different from each other.
Key words: patent image, neural networks, formation dataset, training dataset quality, deep learning, search method.

Likar A. Analysis of Methods for Protecting Information from Malicious Software. – PP. 471–474.

The information processed on users ' personal computers at home, as well as at businesses, is very diverse. Its misuse can cause serious damage, both economic and reputational damage. Given that it is stored on computers and subjected to automated processing, the risk of loss increases. Information that contains various types of information, both private and private information from various organizations, is extremely valuable.

The purpose of analyzing methods for protecting information from malicious software is to analyze and develop affordable and effective measures to protect against unauthorized access to information and its safety. As a result of the proposed measures, the introduction of malicious software into the information system from the outside is reduced and minimized.

Key words: malicious software, analysis of information security methods.

Lipatnikov V., Matveev A., Fleysner V. History and Features of the Development of Artifical Intellect. – PP. 474–479.

The article discusses a brief history of the development of artificial intelligence, describes the direction of AI, considers the prerequisites for the development of AI, makes forecasts for development. The stages of development are determined and a multiple characteristic is given. The possibilities of using AI in the Armed Forces of the Russian Federation are considered.

Key words: artificial intelligence, development history, programming languages, typification, deep learning.

Lipatnikov V., Yarmush V. Analysis of the Efficiency of Menezes, Okamoto and Vanstone Reduction in Solving the Discrete Logarithm Problem in the Group of Points of an Elliptic Curve. – PP. 479–484.

An analysis of the effectiveness of MOV reduction to solve the discrete logarithm problem is presented. A mathematical description of the MOV reduction is presented. The main drawback of MOV reduction has been identified. An algorithm for the implementation of MOV reduction in the case of supersingular curves is proposed. The result of the algorithm with various safety factors is presented.

Key words: MOV-reduction, supersingular curves, solution of the discrete logarithm problem.

Litvinov V., Makarov A. Research of Creation Technologies Smart Home. – PP. 484–488.

In the modern world, automatic control systems are developing rapidly. Automation affected industry and production to a greater extent, but from the end of the last century the smart home system began to appear, which makes life more comfortable for its users. The smart home system implies the automation of ordinary everyday actions of people made with household appliances and life support systems. With the advent of the Internet of things, the smart home systems have become much more productive, it has become possible to remotely receive information about the state of your home or control equipment in it. A flexible solution of the smart home system based on the Arduino platform is considered in the work.

Key words: smart home, automation, control, Internet of things, Arduino.

Litvinov V., Mursalimova K., Trofimova L. Comparative Analysis of Neural Network Models in the Problems of Evaluating the Level of Knowledge of Applicants. – PP. 489–493.
The article provides a comparative analysis of neural network models as approaches to assessing the level of knowledge of applicants. Based on the results of the analysis and classification of neural network models, a system for evaluating the intensity of manifestation of criteria is introduced. An expert method of pairwise comparisons is used to evaluate the value of the importance coefficient of each indicator. The effectiveness of the use of neural network models for the analysis of various types of activities of the enterprise is also considered.
Key words: neural networks, pairwise comparisons, enterprise activity analysis.

Litvinov V., Filimonov L. Intellectualization of the Decision Support System of the Technical Support Department. – PP. 494–500.
The basic concepts and methods of development and design of intelligent decision support systems, including simulation methods, are considered. The paper offers a model of the process of technical support for users of the regional management information system in the AnyLogic environment.
Key words: intelligent decision support systems, expert systems, simulation, development methods, AnyLogic.

Litvinov V., Shalkov M. Research of Intellectual Methods of Monitoring Infocommunication Systems. – PP. 500–504.
For the successful operation of infocommunication systems, it is necessary to be able to quickly respond and eliminate all deviations that occur during operation of the system and prevent their escalation. For this reason, one of the key places in the work of information and communication systems is its comprehensive monitoring. The paper proposes and evaluates options for existing methods for monitoring information and communication systems. The essence and content of the basic concepts of monitoring are considered. A study of the prerequisites for the deployment of a monitoring system has been carried out. The methods of collecting, storing and processing information by monitoring systems, as well as examples of scenarios for using the received data are analyzed. The approaches to building monitoring systems, as well as its key components, are considered.
Key words: monitoring systems, Service Level Agreement, information and communication systems, service, server, network equipment.

Loborchuk A., Muthanna A. Using Kubernetes to Manage a MES System in 5G Networks. – PP. 505–509.
The article will analyze the use of Kubernetes open source software for automating the deployment, scaling of containerized applications based on Docker and managing them within a software-configurable network for building and managing a MEC system in the new 5G networks. Attention will also be paid to new principles, advantages and further prospects of building networks based on the MEC system and managing a deployed system as a software-configured network with containerized applications, both from the side of data transfer from the client to the server, and from the side of managing this network.
Key words: 5G, SDN, MEC, Kubernetes.

Malofeev V., Parashchuk I., Shestakov E. Selection and Justification of Effective Measures for Integrated Data Protection in Information Systems. – PP. 510–515.
The approach to the procedure for the selection and justification of effective measures of integrated data protection in information systems is considered. The approach allows us to generate the values of the probabilistic coefficient of the effectiveness of using the method (or a set of methods and means) of combating data security threats, based on a joint and combined analysis of the key types of threats, means and methods of dealing with them and the financial costs of implementing this fight.
Key words: information system, integrated data protection, efficiency, threat, resource.

Markin D., Minachev V. The Analysis of Code Execution Features in Trusted Execution Environment Based on ARM TrustZone Technology. – PP. 515–520.
The article contains the analysis and classification of trusted execution environment technologies in computers based on ARM processors. The authors describe code execution privilege modes and hardware units used for these aims. The works explain the scheme of data exchange processes between trustlet – Secure OS applications and Normal OS applications.
Key words: TrustZone, trusted execution environment, ARM, TEE, SMC, trustlet.

Markin D., Rykov D. The Methods and Technologies of Obfuscation and Deobfuscation of JavaScript Web-Application Source Code. – PP. 520–524.
The article contains the analysis methods and technologies of obfuscation and deobfuscation of JavaScript web-application source code. The work describes main metrics for obfuscation quality. Deobfuscation technologies are developed and classified. The authors offer the universal deobfuscator based on dynamic analysis methods.
Key words: JavaScript, obfuscation, deobfuscation, code emulator, web application.

Markin D., Ho Th. Ch. The Comparative Analysis of Trusted Operation Systems Based on TrustZone Technology. – PP. 525–530.
The article contains the analysis and classification of trusted execution environment technologies in computers based on ARM CPU. The comparative analysis of contemporary trusted operation systems was carried out. The authors identified their features, availability of source code, scope of application, developers. The conclusions devoted to development and application of trusted execution environment are formulated.
Key words: TrustZone, trusted execution environment, ARM, TEE, SMC, trustlet.

Medvedev V. Models of the binary sequence. Continued. – PP. 530–534.
The approach to binary sequence research as a model of its various implementations, in which a discrete can randomly accept one of two possible values identified as 0 and 1. Concepts are developed and definitions formulated in previous articles are refined. There has been a transition from the probability of counting the value of one position to the notion of the density of binary sequence values. The difference between the average and the mathematical expectation of zeros (units) for the final piece of binary sequence is shown.
Key words: binary sequence, model, probability, average.

Mikhajlichenko N., Popkov M., Strizhenko V., Sultanova Y. Optimizing Data Center Efficiency. – PP. 535–538.
Based on the analysis of the processes of functioning of existing data centers, the article considers the problems that arise in the process of fanctioning. Considers the methods of data center. Methods of managing data centers that can improve the efficiency of their operation are considered. Methods and ways of solving these problems are defined.
Key words: data center, IT-infrastructure, operational efficiency.

Mikhalev O., Petrenko V., Tipakov V., Tkachev D., Yakovlev T. Research of Applications of Artificial Intelligence for Intellectual Communication and Control Systems. – PP. 538–542.
The questions of the use of elements of artificial intelligence are considered as an element of the development of related systems. Introduction and application of advanced technologies in communication and control systems. It is indicated that the construction and use of intelligent blocks based on neural networks allows you to use existing classical algorithms and find new ways to solve existing problems.
Key words: artificial intelligence, communication systems, control systems, neural networks, cognitive control units.

Musaeva T. Research of Image Processing Methods. – PP. 542–547.
The article considers the issue of determining the percentage of decay of the image. To achieve the goal, we propose a study of existing image processing methods in the LabView program to select the optimal one.
Key words: image, decay, quality**.**

Ptitsyna L., Sulyakayev T. Research Methods and Means of Distributed Registrations in Information Structures. – PP. 547–550.
The objective necessity of developing methodological support for distributed systems is shown. The tasks are set of expanding the methodological support of the life cycle of distributed data recording systems in information structures. The methods of optimizing the distribution of registrations among the nodes of a computer network are highlighted. The main components of the methodology for determining the functional specification of a typical system of distributed registrations in information structures are presented. The basic means of distributed data recordings in information structures are described.
Key words: distributed system, methodological support, extension, optimization, components, information structure, resources.

Ptitsyna L., El Zabayar Shevchenko N. Model-Analytical Intelligence Based Formalization of the Action Planning Task in Intellectual Service-Oriented Systems on PDDL Language with Assessment of Their Quality. – PP. 551–556.
The task of action planning for the dynamic composition of business processes from the point of view of ontology is actualized. A technique for translating the ontological description of OWL-S services into the PDDL language is disclosed. A model of a dynamic business process has been built, combining different standard patterns of integration of service-oriented tools. Performance indicators of dynamic business processes of intelligent service-oriented systems were selected. The mathematical apparatus for assessing the quality of the time profile of dynamic business processes for intelligent service-oriented systems is formalized.

Key words: service-oriented systems, dynamic business process, adaptive quality management, time profile, ontology.

Rozhkova T. A Survey of Resource Management Models in a Distributed Computer System. – PP. 556–560.
A distributed computing system is an object of study of this paper. A survey of existing resource management models in a distributed computing system is carried out. We have pointed out its main features and disadvantages. The prototype of the object under study is presented, and we have substantiated the need for its modification.
Key words: distributed computing systems, mobile cloud computing, auction.

Salomatin A., Senchuk D. Designing Control System for Remotely Piloted Air Systems. – PP. 561–565.
This article analyzes the existing approaches to design and construction of the control system for remotely piloted aircraft systems (RPAS). We propose a study scenario for the optimal actions algorithm of the unmanned aircraft vehicle (UAV).
Key words: remotely piloted aircraft systems, operation restrictions, interconnection algorithm.

Slesarchik K. Artificial Neural Network in the Task of Detecting a Multi-Vector DDOS Attack. – PP. 565–570.
The article considers a method for detecting multi-vector distributed denial-of-service attacks aimed at the network and application level of the infocommunication network. The features of using artificial neural networks in the task of detecting multi-vector DDoS attacks at the application and network level are considered. The results of experimental studies of the characteristics of the probability of errors in identifying the state of an attack by an artificial neural network and errors of "false" triggering are presented.
Key words: multi-vector DDoS attack, artificial neural network, network application layer, infocommunication network, destructive information cybernetic impact.

Suzdaltseva O., Tarasov V. Automated Parking Space Monitoring System. – PP. 570–575.
A brief description of the relevance of the existing problem of lack of Parking spaces is given, taking into account the growing number of cars. The automated Parking space monitoring system is designed to find and provide Parking spaces for cars. The system has a software interface for interaction with other information systems and is a source of information for the preparation of Analytics in order to develop a policy for the development of Parking space. A review of methods for searching for a Parking space is conducted. The issue of car recognition features was raised.
Key words: parking space, recognition, neural network.

Tarasov V., Furasiev E. Creating Single-Page Applications in a Reactive Style using the Library «Vue.js». – PP. 576–580.
Features of software development based on the Vue library are considered.js is a progressive JavaScript framework for creating a user interface and ultra-fast, powerful, fully adaptive sin-

gle-Page Web applications (Single Page Application). Thanks to a step-by-step system of components, the library is easily integrated with other projects and libraries. Aspects of implementing the software architecture are described.
Key words: SPA, Javascript, Vue, reactive programming, framework.

Tarasov V., Shapovalov P. Automation of Interaction with a Customer of Interior Design Studio. – PP. 580–585.
The rationale for the need to develop an automated business process management system is given. The advantages of using automation tools for interaction with customers through the use of a corporate Web resource are considered. The requirements for the composition of the system's software structure and its functionality are presented. The paper presents the current concepts of Web design in relation to the solution of applied problems.
Key words: automation, business process, Frontend, Backend.

Trubitsyn V., Cheusov V. Algorithm of Speech definition Using Neural Network Technology and its Application of Informational-Analytics Activity. – PP. 586–591.
The authors of the article reveal aspects of neural network technology, and also describe in detail the application of this technology in solving modern applied problems in information and analytical activities. As an example, the introduction of an automated system for entering and further processing primary results of sociological surveys is given. The authors present the results of functional modeling in the IDEF0 notation of the studied process without the introduction of an automated system and with its implementation, emphasizing how the process will improve if an automated system is implemented. An algorithm for processing speech information and converting it into text is described. The author also draws attention to the requirements for the values of indicators of efficiency of the automated system – efficiency and error-free. This article is of interest and practical value for specialists in the field of analytical activities and artificial intelligence systems.
Key words: neural network, automated system, speech recognition, sociological survey, efficiency, accuracy.

Khodanovich A., Shibakov E. Research of Information Systems and Scientific Knowledge Support Technologies. – PP. 591–595.
The relevance of the development of systems and technologies for supporting scientific knowledge is substantiated. The purpose of researching information systems and technologies for supporting scientific knowledge is determined. A profile of the quality of functioning of the systems was selected in order to accompany scientific knowledge. The task of expanding versions of technology to support scientific knowledge. A typical fragment of the expansion of versions of technologies for supporting scientific knowledge is described. The optimal structure of the interaction "man – computer" in scientific activity is selected. The results of a study of information systems and technologies for supporting scientific knowledge are presented.
Key words: information system, information technology, scientific knowledge.

Chernomyrdin V., Shiyan A. Analysis of Methodologies for the Development of it Projects and the Development of Agile-Concept for the Beginning Team of the Software Developers. – PP. 595–600.

IT project management involves a large number of different methodologies and concepts. For a novice team, existing methodologies may seem complicated and incomprehensible. The most popular "flexible" methodologies for developing IT projects are considered, a comparative analysis with other methodologies is carried out, options for integrating elements of several approaches into one methodology, relevant for a small, novice software development team, are proposed.

Key words: development, project management, agile, novice developers, methodologies.

DIGITAL ECONOMY, GOVERNANCE AND BUSINESS INFORMATICS

Arzoumanian Y., Volfson M., Zakharov A., Sotnikov A. The use of Quantitative Methods of Analysis of the Educational Program. – PP. 601–605.

The method of quantitative assessment of the relationship of courses of the educational program based on the characteristics of key concepts is described. An algorithm for the formation of quantitative characteristics of key concepts is considered, taking into account the cognitive mentality of the teacher. The principles of constructing an educational trajectory according to key concepts for the required specialty are formulated. Scenarios of using the obtained results to harmonize both individual disciplines and the educational program as a whole are presented.

Key words: an educational program, a key concept, a quantitative description of a key concept, a measure of the relationship of disciplines, an educational trajectory.

Arzoumanian Y., Zakharov A., Sokolova J. The Comparative Analysis of Information Characteristics of Academic Disciplines. – PP. 606–609.

Academic disciplines are represented by information sources in which key concepts of didactic units act as messages. The model used allows one to obtain estimates of various characteristics of the classical theory of information. In particular, according to the amount of mutual information, the method makes it possible to assess the proximity of lectures to the materials of the selected textbook. An example of comparing a lecture with the corresponding material of the textbook discipline "Enterprise Architecture".

Key words: key concept, informational characteristic of a didactic unit, mutual information.

Atayan A. Comparative Analysis of Global Index of Innovation and Global Connectivity Index for evaluating the prospects for the development of digital economy. – PP. 610–615.

Various indices have been developed by international organizations to measure the level of digitalization in countries. Of particular interest for ranking analysis is the Global Connectivity Index (GCI), used to analyze indicators of ICT infrastructure and digital transformation, and the Global Innovation Index (GII). Despite the fact that Russia is not included in the group

of leaders in the digital economy, a comparative analysis of the indices of these indices with those of the ranking leaders will highlight strategically important areas of development.
Key words: digitalization; rating, international development indices; the *Global Innovation Index, the Global Connectivity Index.*

Blatova T., Makarov V. Digital Transformation Trends in Education. – PP. 615–619.
The rapid development of digital technology has a significant impact on industries and serves to provide new opportunities, reduce costs and maximize efficiency. As the education sector is becoming increasingly competitive, digital transformation is currently a necessary means of survival for the university, as the new digital world requires teachers to adapt, adopt digital technologies, methodologies and attitudes. Digital transformation in higher education exerts its influence on two main areas of education informatization. Firstly, it is the transformation of services, which is aimed at creating new educational products and converting existing products into digital ones. In addition, this includes the provision of digital communications between students and teachers. Secondly, it is the digitalization of all common operations that take place in educational institutions, such as educational planning, student admission, scheduling, the development of working training programs and ensuring their quality.
Key words: education, digital transformation, technology, teachers, training.

Vasileva N., Stepanenko A. Accounting when Using BitCoin as a Single World Cryptocurrency. – PP. 619–624.
The use of crypto BitCoin as a single international digital money can provide a significant economic effect to national economies and the world economy as a whole. There will be objective problems of unified accounting and accordingly in tax matters. In selected developed market economies, with a view to legalizing BitCoin and addressing the issue of national accounting and taxation, the issue is now gradually being addressed.
However, accounting and taxation issues in the context of the use of BitCoin as the world 's digital money and related difficulties are not currently being addressed.
The article contains proposals to overcome objective difficulties in achieving the goal, which makes such work relevant and timely, including for the implementation of the Digital Economy of the Russian Federation program.
The ways of organizing accounting and taxation in the new conditions are considered and a list of issues requiring a solution in the future is given.
Key words: accounting, taxes, financial system, BitCoin cryptocurrency, transaction, infocommunications, digital economy.

Veredinskiy S., Makarov V., Starodubov D. Promising Options for Organizing Interaction Between Participants of Digital Technology Implementation Projects. – PP. 625–629.
The introduction of digital technologies in the economy is aimed at creating fundamentally new conditions for their functioning, in which it becomes possible to achieve "breakthrough" technological, organizational and economic results of the functioning of both individual enterprises and entire industries. Modern conditions for managing enterprises in the real sector of the economy force the initiators of projects to implement digital technologies to improve existing ways of organizing interaction between project participants, and to develop new ones that were not previously used. An example is the development of the theory and practice of applying the so-called "energy service contracts", the legal and organizational and economic

content of which is quite suitable for developing the organizational and economic basis for innovative projects in the field of digital technology implementation. Interaction mechanisms based on leasing schemes can also be used. Such organizational and economic mechanisms are particularly effective in conditions of insufficient current solvency of recipients of innovative solutions in the form of digital technologies.
Key words: innovations, digital technologies, innovative project.

Gunina E., Ivanova S. Illusions in the Design of Outdoor Advertising. – PP. 630–634.
The article provides an analysis of examples of optical illusions of movement in advertising. The relevance and practical aspect of the chosen topic is determined by a number of key problems related to the relevance and effectiveness of using the new approach in the advertising field to increase attention and interest in advertising, as well as increase sales of advertised products. The possibility of applying new techniques of visual solutions in the process of creating advertising banners is considered. On the example of well-known advertising campaigns, techniques for creating the movement of optical illusions are presented.
Key words: color, illusion of color, advertising, printing, design, optical illusions, images, illusion of movement.

Dubolazova Y., Konnikov E., Makarov V. Development of a Development Strategy for Import Substitution of High-Tech Products in the Russian Federation. – PP. 635–639.
The effective functioning of the enterprise is an integral part of the economic model of industrial policy aimed at protecting the domestic producer – that is, the import substitution policy. At the same time, the substitution of the imported industrial products by domestic production is an innovative development program for domestic enterprises, as replacement products for manufacturing enterprises are new. The author suggests considering the criterion of economic efficiency of the innovation process at the enterprise as the elasticity of the cost of the product production relative to the saving of capital investments – the coefficient of elasticity of the cost of production relative to capital investments is less than one.
Key words: import substitution, endogenous variables, exogenous variables, high-tech goods, export, import.

Dubolazova Y., Makarov V., Okateva A. Application of Information Technologies to Optimize the Training Process for ERP System Analysts. – PP. 639–644.
Effective enterprise management requires information support for management processes for timely management decision-making. In the configuration "1C:ERP Enterprise Management 2" (hereinafter – 1C:ERP) there are tools that allow to display information in visual representation in the form of visible graphs and diagrams, which allows to quickly analyze current indicators and factors affecting the business activity of the enterprise, to make timely and fast management decisions. But there are also problems: high cost of training with a professional, fragmented data structure for self-study, too much information aimed at the average level of training of a specialist.
Key words: ERP system, enterprise information system, automated enterprise management system, software, information technology, analytics, ERP analyst, training system, optimization, systematization, efficiency improvement.

Egorova M. Specificity of Regulation of the Russian Finansial Market. – PP. 645–650.
Pension changes have been taking place continuously since 2002. The low profitability of the funded part of the pension calls into question the achievement of the main goal of the pension system – to increase the level of pension provision for citizens. The accumulative pension system, having accumulated a significant amount of financial resources, does not guarantee either the profitability or the safety of pension savings.
Key words: pension system, pension savings, investment income.

Isakov A., Pavlova E. Information Systems Implementation Problems at Enterprises. – PP. 650–654.
Despite the widespread use of digital information technologies in many areas of modern economy, public administration, and in all spheres of society, the issue of implementing software information systems in enterprises is still relevant. In many ways, this is determined by the growth of companies, when the business development of processes, the growth of the volume of transmitted information, the speed of its transmission, requires business modernization and automation in terms of management. Also, the objective reason is the modern environment - the level of digitalization of contractors, clients, government, including tax authorities.
But, regardless of the reasons why the company comes to the need to implement software information systems, almost everyone faces difficulties, especially at the initial stages. Tellingly, each Manager, in many ways rightly, believes that their problems are absolutely unique. But in practice, if you analyze this issue from the side of implementation professionals, it turns out that most of the problems are of a typical nature, quite predictable and solvable, provided that developers are competent and the company's management is open to the perception of other people's experience and knowledge.
Key words: digitalization, business processes, management, automation, ERP-systems, CRM-systems, BI-systems, document exchange automation.

Kovalev S., Makarov V., Sinitsa S., Starodubov D. Mobile App Concept for Improving the Performance of a Service Company. – PP. 655–660.
It is proposed to improve the operation of the catering company through the introduction of a mobile application that allows customers to make a preliminary online order from the subscriber's mobile device. Implementation of an application based on the iBuildApp constructor, without requiring significant costs, improves the provision of services and increases the competitiveness of the enterprise.
Key words: mobile app, infocommunication technologies, IT Department, online payment.

Kotov V. System Approach to the Marketing Management Function. – PP. 660–664.
A hierarchical structure of marketing tasks in the company management system is proposed. A comparative analysis of various options for the marketing mix concept is widely used in the scientific literature. A new systematic view of marketing, as a function of business management, can be useful both from a practical point of view and from the point of view of the teaching methodology of this discipline.
Keywords: marketing, marketing mix, pricing, product mix, sales, advertising, marketing research, competition.

Makarov V. Results and Prospects of the Scientific and Educational School Development "Economics and Management in Infocommunications". – PP. 664–668.
The results and achievements of the long-term activities of the scientific and educational school "Economics and management in Infocommunications"are studied. The article analyzes the branch orientation of training of specialists of higher qualification; it provides monographs, textbooks and scientific articles made within the framework of School. The research and educational activities of graduates of the scientific School, who continue to cooperate with the Department of Economics and management of information communications, are traced. The subject of research works and the use of research results in the production activities of enterprises in the field of IT, as well as in the scientific and educational work of the Department.
Key words: scientific and educational school, Infocommunications, innovative development, research, digital economy, educational and scientific activities.

Makarov V., Starkova T. Knowledge Management – a Tendency of Development of Organization Management. – PP. 668–672.
In modern conditions, data, information and knowledge on the one hand are accumulating in increasing volumes, on the other hand, they remain only partially in demand. From the point of view of knowledge management, this circumstance is caused by the difficulty of extraction, digitalization of acquired knowledge, verification of their completeness and reliability. Knowledge management is becoming increasingly relevant not only for individual industries, but also for the development of the digital economy as a whole. Thus, it is necessary to develop knowledge-based skills among knowledge workers in the digital economy. Knowledge coordinators, providing knowledge and information to all employees in a timely manner, will provide an opportunity to reuse the best developments, knowledge and lessons learned from experience, which will help to increase the effectiveness of the organization's management.
Key words: Knowledge, knowledge management, intellectual worker, knowledge coordinator.

Makarov V., Urusova N. The Concept of Creating a Situation Center for the Governor of the Leningrad Region using Digital Tools of the Information and Analytical System. – PP. 673–677.
The concept of creating a Situation center For the Governor of the Leningrad region, which acts as a single point for collecting analytical information and is one of the first examples of practical implementation of the concept of regional management based on integrated data collection, is considered. The information and analytical system of the Situation center uses modern big data processing technologies. The situation center can be used for decision- making by top officials, both in emergency situations and in regular regional management.
Key words: situation center, information and analytical system, integration of information resources, modular principle.

Meshkov A., Simonina A. Cryptocurrencies as “Black Swans” of the Modern World Currency System. – PP. 678–682.
The article discusses the main problems of the modern world monetary system based on the US dollar, and options for its reform. The point of view is substantiated, according to which cryptocurrency in the future can become the main form of world money.
Key words: cryptocurrency, world monetary system, world money, an event like “black swan".

Sapozhnikov G. Economically Justified Information as Optimum Power Source Selection Condition. – PP. 682–686.

The economic efficiency of production depends on the reliability and completeness of the information. The article considers wrong conclusions about the choice of power sources drawn on the economically unfounded information concerning energy prices. The selection of natural gas, a non-renewable resource, instead of power grid electricity due to its unjustifiably high price turned out to be quite costly, meanwhile a number of researchers advise Autonomous natural gas power generators to be more efficient for the same reason.

The article proposes to develop an algorithm for selecting the optimum power source supply for the specific consumer in the specific territory.

Key words: reliable information, power sources, cost, reasonable price, natural gas, optimization of choice.

АВТОРЫ СТАТЕЙ

АВРАМЕНКО Владимир Семенович — кандидат технических наук, доцент, профессор кафедры автоматизированных систем специального назначения Военная академия связи, vsavr@yandex.ru

АДУЕВСКИЙ Александр Михайлович — магистрант группы ИСТ-951м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zero.2012@yandex.ru

АКИМОВ Сергей Викторович — кандидат технических наук, доцент кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akimov-sv@yandex.ru

АКЧУРИНА Диана Ришадовна — студентка группы ИСТ-811м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, diashulik@gmail.com

АНДРЕЕВ Дмитрий Алексеевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vat-reg@yandex.ru

АРЗУМАНЯН Юрий Вазгенович — кандидат технических наук, доцент кафедры бизнес-информатики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, arz@fem.sut.ru

АРОНОВ Виталий Юрьевич — кандидат технических наук, доцент кафедры программного обеспечения и управления в технических системах Поволжского государственного университета телекоммуникаций и информатики, avy@psuti.ru

АТАНОВ Владимир Дмитриевич — студент группы ИКТБ-88м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, danskoy76@mail.ru

АТАЯН Ануш Михайловна — кандидат педагогических наук, доцент кафедры бизнес-информатики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anush-atayan@inbox.ru

АХМЕТОВА Юлия Славовна — магистр кафедры инфокоммуникационных сетей и систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Ahmetova.us@spbgut.ru

БАБАЕВА Алла Васильевна — студент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, beljaeva-a@list.ru

БАЖИН Михаил Иванович — слушатель Венной Академии Связи им. Маршала Советского Союза С. М. Буденного, mbazhyn@gmail.com

БАЛАКИРЕВ Дмитрий Денисович — студент группы ИСТ-831м Санкт-Петербургского государственного университета телекоммуникаций им. Бонч-Бруевича, dimurator1@yandex.ru

БАЛАНДИН Иван Андреевич — студент группы ИКТИ-85м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, balandinniv@gmail.com

БАРАНОВ Игорь Юрьевич — кандидат технических наук, доцент, сотрудник Академии ФСО России, i_baranov@rambler.ru

БЕЛИКОВ Илья Владимирович — сотрудник Академии ФСО России, ivanrivanov@yandex.ru

БЕЛОВ Михаил Петрович — доктор технических наук, доцент, профессор кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, milesa58@mail.ru

БИРЮКОВ Артем Сергеевич — оператор научной роты Военной академии связи, biryukov-artem@list.ru

БЛАТОВА Татьяна Александровна — старший преподаватель кафедры экономики и менеджмента инфокоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nsnlon@gmail.com

БОВЫКИН Евгений Александрович — магистрант группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rebovykin@gmail.com

БОГОЛЕПОВ Григорий Сергеевич — заместитель начальника отдела научно-исследовательского центра Военной академии связи, bogolepov@inbox.ru

БОНДАРЕНКО Игорь Борисович — кандидат технических наук, доцент, доцент кафедры факультета безопасности информационных технологий Национального исследовательского университета ИТМО, igorlitmo@rambler.ru

БОРОДЯНСКИЙ Юрий Михайлович — кандидат технических наук, доцент, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, borodyanskyum@gmail.com

БОЧКАРЕВ Дмитрий Александрович — слушатель Военная академия связи, d.a.bochkarev@yandex.ru

БОЯТКОВ Вячеслав Витальевич — студент группы ИСТ-841м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, wiseboy@yandex.ru

БУШУЕВ Сергей Николаевич — доктор технических наук, профессор, заместитель директора акционерного общества «Научно-производственное предприятие ТЕЛДА» (АО «НПП «ТЕЛДА»), bsn@telda.ru

БЫСТРОВ Игорь Владимирович — студент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ibystrov93@mail.ru

ВАГАНОВ Александр Валерьевич — старший преподаватель кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sut-ispiu@mail.ru

ВАСИЛЬЕВА Надежда Николаевна — старший преподаватель кафедры экономики и менеджмента телекоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vnn2008@gmail.com

ВАЧУГОВА Виктория Алексеевна — студент группы ИСТ-841м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tarakanovfers@gmail.com

ВЕРЕДИНСКИЙ Сергей Юрьевич — доцент кафедры экономики и менеджмента инфокоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, veredinskiy@yandex.ru

ВЕРЖАКОВСКАЯ Марина Александровна — кандидат физико-математических наук, доцент кафедры программного обеспечения и управления в технических системах Поволжского государственного университета телекоммуникаций и информатики, vma@psuti.ru

ВЕРХОВА Галина Викторовна — доктор технических наук, профессор, заведующая кафедрой автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, galina500@inbox.ru

ВИХАРЕВ Антон Николаевич — сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

ВОЛОШЕНЕНКО Дарья Владимировна — студент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dasha.voloshenenko@gmail.com

ВОЛОШИНОВ Денис Вячеславович — доктор технических наук, доцент, заведующий кафедрой информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, denis.voloshinov@yandex.ru

ВОЛЫНКИН Павел Александрович — кандидат технических наук, доцент кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pavelas@mail.ru

ВОЛЬФСОН Михаил Борисович — кандидат экономических наук, заведующий кафедрой бизнес-информатики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, volfson_mb@mail.ru

ВОРОБЬЕВ Андрей Анатольевич — кандидат технических наук, доцент, сотрудник Академии ФСО России, AWA@mail.ru

ВОРОНЕЦКИЙ Александр Александрович — сотрудник Академии ФСО России, Alexcs57@mail.ru

ВОРОНЦОВ Дмитрий Михайлович — курсант Военной академии связи, mr.vorrond@gmail.com

ВОСТРЫХ Алексей Владимирович — аспирант Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.vostrykh@list.ru

ГАЛИЕВ Ренат Венерович — оператор научной роты Военной академии связи, galieff.renat@yandex.ru

ГЕРМАНОВА Елена Владимировна — студентка группы ИСТ-831М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elengermnova@gmail.com

ГЕСЬ Анастасий Сергеевич — магистрант кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, polyges3d@gmail.com

ГЛАЗКОВ Глеб Сергеевич — студент группы ИСТ-621 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glazkov@bonch.dev

ГЛЫБИН Петр Алексеевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, port.gun2012@yandex.com

ГОРБАНЬ Сергей Андреевич — студент группы ИКБ-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sergo.t.t@mail.ru

ГОРДЕЕВ Михаил Алексеевич — студент группы ИСТ-942 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, michael.xfox@outlook.com

ГОРДИЕВИЧ Григорий Александрович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vat-reg@yandex.ru

ГРИГОРЬЕВА Анастасия Алексеевна — магистрант группы ИСТ-841м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nastya-grig@mail.ru

ГРИГОРЬЕВА Екатерина Владимировна — студент группы ИСТ-651 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, katya_grigoreva_98@mail.ru

ГРИЩЕНКО Ирина Витальевна — студентка группы ИСТ-812м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, irinagrishchenko@bk.ru

ГРОМОВ Владислав Витальевич — кандидат технических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gromov_vladislav@hotmail.com

ГУБИН Александр Николаевич — кандидат технических наук, доцент, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gan50_60@mail.ru

ГУЛЯЕВА Ксения Валерьевна — студент группы ЭП-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gulksu@mail.ru

ГУНИНА Елена Викторовна — кандидат педагогических наук, доцент, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, e.v.gunina@yandex.ru

ГУРБАТОВ Глеб Олегович — студент группы ИКТЗ-63 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 12345678987654321geb@mail.com

ДАВЛЕТШИНА Элеонора Ринатовна — магистрант группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, eleonora.davletshina@mail.ru

ДАГАЕВ Александр Владимирович — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, adagaev@list.ru

ДВОРНИКОВ Александр Сергеевич — кандидат технических наук, начальник научно-исследовательского отдела НИЦ Военной академии связи

ДИЧЕНКО Сергей Александрович — кандидат технических наук, старший преподаватель 31 кафедры 3 факультета Краснодарского высшего военного училища, dichenko.sa@yandex.ru

ДОЛГУН Владислав Олегович — аспирант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Dolgun@spbgut.ru

ДУБОЛАЗОВА Юлия Андреевна — кандидат экономических наук, доцент кафедры экономики и менеджмента инфокоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, julia005@mail.ru

ДУБОНОС Александр Сергеевич — курсант Военной академии связи, dubonos99@inbox.ru

ДУЛЬКОВ Михаил Владимирович — слушатель Военной академии связи, mikhaildulkov2@gmail.com

ДЫМЧЕНКО Александр Сергеевна — студент группы ИСТ-812м кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alex.dym96@yandex.ru

ЕВГЛЕВСКАЯ Наталья Валерьевна — кандидат технических наук, преподаватель кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи, n.evglevskaya@gmail.com

ЕГОРОВА Марина Александровна — кандидат экономических наук, доцент кафедры управления и моделирования в социально-экономических системах Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egorova-mak@yandex.ru

ЕЛАГИН Василий Сергеевич — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elagin.vas@gmail.com

ЕРШОВ Александр Владимирович — подполковник, начальник научно-исследовательского отдела НИЦ Военной академии связи, aershov@mail.ru

ЖАРАНОВА Анастасия Олеговна — студент группы ИСТ-911м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zharanovaan@gmail.com

ЖИЛИН Виктор Владимирович — старший оператор научной роты Военной академии связи, zhilin95@inbox.ru

ЖУСОВ Дмитрий Леонидович — кандидат технических наук, сотрудник Академии ФСО России, d.zhusov@mail.ru

ЗАКАЛКИН Павел Владимирович — кандидат технических наук, докторант Военной академии связи, ansmed82@mail.ru

ЗАХАРОВ Ариан Арианович — кандидат технических наук, доцент кафедры бизнес-информатики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, za54ar@gmail.com

ЗВЕРЕВ Артем Александрович — сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

ЗИБЕРОВ Владимир Олегович — студент группы ИКТГ-84м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ziberov.vladimir@yandex.ru

ЗИКРАТОВ Игорь Алексеевич — доктор технических наук, профессор, декан факультета информационных системы и технологий Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, igzikratov@yandex.ru

ЗОЛОТОВ Олег Иванович — кандидат технических наук, профессор, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, oleg_1938@mail.ru

ИВАНОВ Василий Геннадьевич — кандидат военных наук, доцент Военной академии связи, wasj2006@yandex.ru

ИВАНОВ Алексей Сергеевич — магистрант группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aleks_1503@mail.ru

ИВАНОВ Александр Юрьевич — доктор технических наук, профессор, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, alexandr.y@mail.ru

ИВАНОВА Светлана Владимировна — студентка группы ИСТ-931м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivanova2530@bk.ru

ИЗРАИЛОВ Константин Евгеньевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, konstantin.izrailov@mail.ru

ИСАКОВ Александр Вячеславович — кандидат экономических наук, доцент кафедра экономики и менеджмента инфокоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexander.isakov@mail.ru

ИШКОВА Анна Александровна — студентка группы ИСТ-851м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, IshkovaAnn@ya.ru

КАДЫНЦЕВ Антон Николаевич — студент группы ИСМ-71з кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, morzes8@gmail.com

КАДЫНЦЕВА Дарья Вячеславовна — студентка группы ИСМ-71з кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, morzes8@gmail.com

КАЗАКОВ Дмитрий Борисович — аспирант кафедры защищенных сетей связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dkazakov@spbgut.ru

КАЗАРИН Михаил Андреевич — оператор научной роты Военной академии связи, kazarinmisha@mail.ru

КАЗНАЧЕЕВА Екатерина Сергеевна — аспирант кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ekaterina2694@mail.ru

КАЗЬМИН Михаил Александрович — студент группы ИСМ-91з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Kazmin.MA@gmail.com

КАЛЕГИН Михаил Андреевич — студент группы ИСТ-831м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, m_kalegin@mail.ru

КАПИТОНЕНКО Виктория Викторовна — студент группы ИСТ-911м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vika@kaptn.ru

КАПЧУК Никита Викторович — старший оператор научной роты Военной академии связи, nikitapv@mail.ru

КАРАСЕНКО Анатолий Олегович — старший оператор научной роты Военной академии связи, mclot1234@gmail.com

КАРЕВ Валерий Александрович — оператор научной роты Военной академии связи, karev.valera2013@yandex.ru

КИРЕЕВА Наталья Валерьевна — кандидат технических наук, доцент кафедры информационной безопасности, декан факультета телекоммуникаций и радиотехники Поволжского государственного университета телекоммуникаций и информатики, zeppelinSN@yandex.ru

КЛЕВЕРОВ Денис Анатольевич — младший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, denklewer@gmail.com

КЛЕВЕРОВ Максим Анатольевич — младший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, klevermx@gmail.com

КОВАЛЁВ Сергей Валерьевич — студент группы БИМ-81з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ekon_up@sut.ru

КОЗИНЦЕВ Дмитрий Алексеевич — магистрант кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cozinczev@yandex.ru

КОЗЛЕНКО Андрей Владимирович — кандидат технических наук, сотрудник Академии ФСО России, et-ak@yandex.ru

КОЗЛОВА Людмила Петровна — кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tigrenok59@mail.ru

КОЗЛОВА Ольга Александровна — старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, k_olga_a@mail.ru

КОЛЕСНИКОВ Александр Александрович — сотрудник Академии ФСО России, alexlion@inbox.ru

КОЛЕСОВ Даниил Сергеевич — магистрант группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, KolesovD98@gmail.com

КОЛЬЦОВ Павел Олегович — студент группы ИСТ-631 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zemtirstudio@gmail.com

КОМАШИНСКИЙ Владимир Ильич — доктор технических наук, доцент, заместитель директора по научной работе Института проблем транспорта им. Н. С. Соломенко Российской академии наук, kama54@rambler.ru

КОМКОВ Глеб Валентинович — аспирант кафедры факультета безопасности информационных технологий Национального исследовательского университета ИТМО, kgv.94@mail.ru

КОМЛЕВ Григорий Олегович — студент группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, G.O.Komlev@yandex.ru

КОННИКОВ Евгений Александрович — старший преподаватель кафедры экономики и менеджмента инфокоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, konnikov.evgeniy@gmail.com

КОНОНЮК Ольга Алексеевна — магистрант группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hola.aloha@outlook.com

КОРСУН Николай Алексеевич — старший оператор научной роты Краснодарского высшего военного училища

КОСОВ Павел Валерьевич — магистрант кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kosov_pavel@bk.ru

КОСОЛАПОВ Владислав Сергеевич — адъюнкт Военной академии связи, kvs_mil@mail.ru

КОТКИНА Мария Сергеевна — студентка группы ИСТ-812м кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maria.kotkina@yandex.ru

КОТОВ Виктор Иванович — кандидат технических наук, доцент кафедры управления и моделирования в социально-экономических системах Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kotov-vi@yandex.ru

КРАСОВ Андрей Владимирович — кандидат технических наук, доцент, почетный работник высшего профессионального образования, заведующий кафедрой защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krasov@inbox.ru

КРИВЦОВ Александр Николаевич — кандидат физико-математических наук, доцент, доцент кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a_kriv@mail.ru

КРЮКОВА Елена Сергеевна — адъюнкт кафедры автоматизированных систем специального назначения Военной академии связи, e.kkrukovaa69@yandex.ru

КУЗНЕЦОВ Станислав Александрович — студент группы ИКБ-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, staskonkurs12@mail.ru

КУЗЬКИН Александр Александрович — кандидат технических наук, сотрудник Академии ФСО России, kuzmich313@mail.ru

КУКУНИН Дмитрий Сергеевич — кандидат технических наук, доцент кафедры сети связи и передача данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kukuninds@spbgut.ru

КУРНОСОВ Валерий Игоревич — доктор технических наук, профессор, профессор кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vi-Kurnosov@mail.ru

КУЦАКИН Максим Алексеевич — кандидат технических наук, сотрудник Академии ФСО России, max_kooks@mail.ru

КУЧЕРЕВСКИЙ Кирилл Владимирович — магистрант группы ИСТ-951м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zero.2012@yandex.ru

КУЧЕРЕНКО Ирина Сергеевна — студент группы ИСМ-81з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, irinakikucherenko@gmail.com

ЛАБА Роман Зиновьевич — студент группы ИСМ-81з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman.laba@mail.ru

ЛАПКО Александр Николаевич — кандидат технических наук, сотрудник Академии ФСО России, lan46@mail.ru

ЛАУТА Олег Сергеевич — кандидат технических наук, старший преподаватель кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи, laos-82@yandex.ru

ЛЕБЕДЕВ Александр Сергеевич — оператор научной роты Военной академии связи, artabsolve@gmail.com

ЛЕБЕДЕВ Никита Сергеевич — оператор научной роты Военной академии связи, asdnicki@rambler.ru

ЛИКАРЬ Александр Иванович — старший преподаватель кафедры безопасности информационных систем Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, likar_a@mail.ru

ЛИПАТНИКОВ Валерий Алексеевич — доктор технических наук, профессор, старший научный сотрудник Военной академии связи, lipatnikovanl@mail.ru

ЛИТВИНОВ Владислав Леонидович — кандидат технических наук, доцент, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vlad.litvinov61@gmail.com

ЛОБОРЧУК Александр Александрович — студент группы ИКТГ-84м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, loborchuk@gmail.com

МАКАРОВ Владимир Васильевич — доктор экономических наук, профессор, заведующий кафедрой экономики и менеджмента инфокоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akad.makarov@mail.ru

МАКАРОВ Алексей Александрович — студент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aleksmakarov5@yandex.ru

МАКЕЕВ Сергей Михайлович — кандидат технических наук, сотрудник Академии ФСО России, maksm57@yandex.ru

МАЛИКОВ Альберт Валерьянович — адъюнкт Военная академия связи, mkv.vas@yandex.ru

МАЛОФЕЕВ Валерий Александрович — курсант Военной академии связи, valeron12.1366@gmail.com

МАРКИН Дмитрий Олегович — кандидат технических наук, сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

МАСЛОВА Екатерина Александровна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, acidcathouse@gmail.com

МАТВЕЕВ Алексей Александрович — старший оператор научной роты Военной академии связи, a.matveev1995@mail.ru

МЕДВЕДЕВ Валерий Александрович — кандидат технических наук, доцент кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, medvedev.spb@list.ru

МЕШКОВ Александр Владимирович — кандидат экономических наук, заведующий кафедрой управления и моделирования в социально-экономических системах Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aleksander-v-meshkov@yandex.ru

МИНАЧЕВ Владислав Маратович — сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

МИХАЙЛИЧЕНКО Николай Валерьевич — кандидат технических наук, преподаватель кафедры автоматизированных систем специального назначения Военной академии связи, 23esn2008@rambler.ru

МИХАЛЕВ Олег Александрович — кандидат технических наук, начальник 3-го отдела НИЦ Военной академии связи, oleg.mikhalev.74@mail.ru

МОИСЕЕВА Анна Яковлевна — студент группы ИСТ-831М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dafna97@yandex.ru

МУРСАЛИМОВА Камила Болатовна — студент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lidia.comarowa@yandex.ru

МУСАЕВА Татьяна Вагиф кызы — кандидат технических наук, доцент, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, neli_6868@mail.ru

МУТХАННА Аммар Салех Али — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ammarexpress@gmail.com

НАЛИМОВ Кирилл Игоревич — оператор научной роты Военной академии связи, kiria95@mail.ru

НЕВРОВ Алексей Александрович — кандидат технических наук, сотрудник Академии ФСО России, newrow@mail.ru

НИКОНОВ Евгений Русланович — студент группы ИКБ-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nikkstudio3023@gmail.com

НОСОВ Михаил Иванович — полковник запаса, доктор технических наук, доцент, старший научный сотрудник научно-исследовательского отдела НИЦ Военной академии связи, mikhail.nosov.64@mail.ru

ОКАТЬЕВА Анастасия Дмитриевна — студентка группы 3733801/60103 Санкт-Петербургского политехнического университета Петра Великого, oka.nastya@gmail.com

ОСТРОВСКИЙ Юрий Николаевич — старший преподаватель Военной академии связи, nr7vas@mail.ru

ПАВЛОВА Елена Васильевна — кандидат экономических наук, доцент кафедра экономики и менеджмента инфокоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, epavlova.pnd-9@yandex.ru

ПАНИХИДНИКОВ Сергей Александрович — кандидат военных наук, доцент, заведующий кафедрой экологической безопасности телекоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, panihidnikov@mail.ru

ПАНИЧЕВ Артем Дмитриевич — студент группы ИКТЗ-63 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, robogiar2@inbox.ru

ПАНТЮХИН Олег Игоревич — кандидат технических наук, доцент, доцент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, p_oleg99@mail.ru

ПАРАЩУК Игорь Борисович — доктор технических наук, профессор, Заслуженный изобретатель РФ, профессор кафедры автоматизированных систем специального назначения Военной академии связи; ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, shchuk@rambler.ru, parashchuk@comsec.spb.ru

ПАЦКАН Максим Юрьевич — начальник отдела эксплуатации инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pmy@spbgut.ru

ПЕСИКОВ Эдуард Борисович — доктор технических наук, профессор, профессор кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ed_pesikov@mail.ru

ПЕТРЕНКО Михаил Игоревич — младший научный сотрудник Военной академии связи, Petrenko_88@yandex.ru

ПОЗДНЯК Ирина Сергеевна — кандидат технических наук, доцент кафедры информационной безопасности Поволжского государственного университета телекоммуникаций и информатики, vis_517@mail.ru

ПОПКОВ Максим Александрович — курсант Военной академии связи, 23esn2008@rambler.ru

ПРИСЯЖНЮК Сергей Прокофьевич — доктор технических наук, профессор, профессор кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, office@itain.ru

ПРОНИН Антон Александрович — оператор научной роты Военной академии связи, pronin.topki@mail.ru

ПТИЦЫНА Лариса Константиновна — доктор технических наук, профессор, почетный работник высшего профессионального образования Российской Федерации, заведующая кафедрой информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ptitsina_lk@inbox.ru

РЕБРОВ Дмитрий Алексеевич — студент группы ИКМ-81з, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, drebroff2012@yandex.ru

РЕЗНИЦКИЙ Александр Денисович — студент группы ИСТ-851м Санкт-Петербургского государственного университета телекоммуникаций имени профессора Бонч-Бруевича, laosen@mail.com

РОЖКОВА Татьяна Сергеевна — аспирант кафедры ИВТ Академии ФСО России, 9192058128@mail.ru

РЫКОВ Даниил Алексеевич — сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

РЯБОКОНЬ Владимир Владимирович — кандидат технических наук, сотрудник Академии ФСО России, mimicria@mail.ru

САВЧЕНКО Станислав Олегович — магистрант Омского государственного технического университета, stassavchenko@mail.ru

САЕНКО Игорь Борисович — доктор технических наук, профессор, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук; профессор Военной академии связи, ibsaen@comsec.spb.ru, saenko.igor@mail.ru

САКЛАКОВ Алексей Иванович — сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

САКОВА Наталья Владимировна — кандидат технических наук, доцент, доцент кафедры экологической безопасности телекоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nat.sakova@mail.ru

САЛОМАТИН Александр Александрович — инженер лаборатории киберфизических систем Института проблем управления им. В. А. Трапезникова РАН, магистрант МФТИ, aleksandr.salomatin@phystech.edu

САПОЖНИКОВ Герман Никифорович — кандидат технических наук, доцент кафедры экономики связи Уральского технического института связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики», sgn1941@rambler.ru

СЕНЧУК Дмитрий Владимирович — аспирант лаборатории киберфизических систем Института проблем управления им. В. А. Трапезникова РАН, tyxer2006@gmail.com

СЕРОВА Маргарита Владимировна — студентка группы ИСТ-831М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, margo7997@yandex.tu

СИМОНИНА Анна Александровна — старший преподаватель кафедры управления и моделирования в социально-экономических системах Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ann-simonina@yandex.ru

СИМОРИН Борис Игоревич — оператор научной роты Краснодарского высшего военного училища

СИНИЦА Сергей Александрович — кандидат экономических наук, доцент кафедры экономики и менеджмента инфокоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sinica@sulus.ru

СКИБИНСКИЙ Илья Юрьевич — оператор научной роты Военной академии связи, ilyaskibinsky@yandex.ru

СЛЕСАРЧИК Константин Федорович — сотрудник Академии ФСО России, interline57@mail.ru

СОКОЛОВА Яна Владимировна — кандидат технических наук, доцент кафедры бизнес-информатики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ya.v.sokolova@inbox.ru

СОЛОВЬЕВ Денис Викторович — кандидат технических наук, доцент кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 9218964588@mail.ru

СОЛОВЬЕВА Александра Владимировна — старший преподаватель кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexis.soloveva@gmail.com

СОТНИКОВ Александр Дмитриевич — доктор технических наук, декан факультета цифровой экономики, управления и бизнес-информатики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, adsotnikov@mail.ru

СТАРКОВА Татьяна Николаевна — старший преподаватель кафедры экономики и менеджмента инфокоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tania_starkova@bk.ru

СТАРОДУБОВ Денис Олегович — аспирант кафедры экономики и менеджмента инфокоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, starden@mail.ru

СТЕПАНЕНКО Александр Александрович — кандидат технических наук, доцент кафедры экономики и менеджмента телекоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vip.saa2005@mail.ru

СТРИЖЕНКО Вадим Николаевич — курсант Военной академии связи, 23esn2008@rambler.ru

СУЗДАЛЬЦЕВА Ольга Константиновна — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vat-reg@yandex.ru

СУЛТАНОВА Ясмина Маратовна — курсант Военной академии связи, 23esn2008@rambler.ru

СУЛЯКАЕВ Тимур Рашидович — студент группы ИСМ-71з кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tsulikaev@gmail.com

ТАРАСОВ Владимир Анатольевич — старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vat-liquidator@bk.ru

ТАТАРНИКОВА Ирина Михайловна — аспирант кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича, itatarnikova@list.ru

ТЕМНИКОВА Марина Вячеславовна — студентка группы ИСМ-71з кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mtemnikova@ya.ru

ТИПАКОВ Василий Сергеевич — оператор научной роты Военной академии связи, outn9h6rzn@gmail.com

ТКАЧЕВ Дмитрий Федорович — кандидат технических наук, заместитель начальника 3-го отдела НИЦ Военной академии связи, dimas.portnoy@inbox.ru

ТОПОРКОВ Николай Юрьевич — студент группы ИСТ-851м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, toporkov.kolya96@gmail.com

ТРОФИМОВА Лидия Дмитриевна — студент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lidia.comarowa@yandex.ru

ТРУБИЦЫН Владимир Геннадьевич — кандидат технических наук, сотрудник Академии ФСО России, twg64@rambler.ru

УРУСОВА Наиля Фяридьевна — магистрант группы БИМ-81з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ekon_up@sut.ru

УШАКОВ Игорь Александрович — старший преподаватель кафедры Защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakovia@gmail.com

УШАКОВ Андрей Валерьевич — сотрудник Академии ФСО России, ushakov.andrey257686@gmail.com

ФАБИЯНОВСКИЙ Игорь Николаевич — адъюнкт Военной академии связи, fabik-spb@yandex.ru

ФЁДОРОВ Никита Сергеевич — магистрант группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fyodorov.ns@gmail.com

ФЕДОРОВА Алина Владимировна — кандидат экономических наук, начальник отдела аспирантуры и докторантуры, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций М. А. Бонч-Бруевича, fav111@yandex.ru

ФЕДОСЕЕВ Денис Олегович — кандидат технических наук, доцент Военной академии связи, nr7vas@mail.ru

ФИЛИМОНОВ Леонид Сергеевич — студент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, filimonov.leonid.sergeevich@yandex.ru

ФИЛИППОВ Феликс Васильевич — кандидат технических наук, старший научный сотрудник, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 9000096@mail.ru

ФИЛИППОВ Николай Витальевич — студент группы ИБТС-71 Поволжского государственного университета телекоммуникаций и информатики, kfilipppov@mail.ru

ФЛЕЙСНЕР Владислав Всеволодович — старший оператор научной роты Военной академии связи, fleisner.omsk@gmail.com

ФУРАСЬЕВ Евгений Андреевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vat-reg@yandex.ru

ХАЙБРАХМАНОВА Екатерина Сергеевна — аспирант кафедры информатики и компьютерного дизайна, руководитель группы поддержки мультимедийных аудиторий Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, katusha.1994.10@mail.ru

ХВОСТОВ Максим Алексеевич — магистрант группы ИСТ-941м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, makshvostov@mail.ru

ХИЛЬКО Алексей Сергеевич — сотрудник Академии ФСО России, alexey111154@gmail.com

ХО Тхай Чунг — сотрудник Академии ФСО России, mdo@academ.msk.rsnet.ru

ХОДАНОВИЧ Александр Иванович — доктор педагогических наук, профессор кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akhodanovich@yandex.ru

ХОРОШЕНКО Сергей Викторович — кандидат технических наук, доцент, заведующий кафедрой безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, khoroshenko@mail.ru

ЧЕРНОМЫРДИН Владимир Викторович — студент группы ИСТ-931м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vov.cher@mail.ru

ЧЕРНЯВСКИЙ Андрей Владимирович — слушатель (магистрант) Военной академии связи, zxcdewqa@mail.ru

ЧЕУСОВ Валентин Андреевич — сотрудник Академии ФСО России, LV.STENmark2@yandex.ru

ШАЛЬКОВ Максим Валерьевич — студент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, max.shalkov@gmail.com

ШАПОВАЛОВ Павел Михайлович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vat-reg@yandex.ru

ШЕВЧЕНКО Александр Александрович — научный сотрудник Военной академии связи, alex_pavel1991@mail.ru

ШЕСТАКОВ Александр Викторович — доктор технических наук, старший научный сотрудник, профессор кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexandr.shestakov01@yandex.ru

ШЕСТАКОВ Евгений Олегович — курсант Военной академии связи, shestakov220919977@yandex.ru

ШИБАКОВ Евгений Дмитриевич — магистрант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, edsh_@mail.ru

ШИМАНЧУК Сергей Николаевич — аспирант кафедры факультета безопасности информационных технологий Национального исследовательского университета ИТМО, shimanchuk.s@gmail.com

ШИРЕВ Владислав Юрьевич — аспирант кафедры Безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича, vladshv1990@gmail.com

ШИЯН Андрей Анатольевич — кандидат педагогических наук, доцент, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 1001digit@gmail.com

ШОЛУХО Юлия Александровна — студентка группы ИСТ-811м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yulia.sholukho@gmail.com

ШУМИЛОВ Семен Сергеевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, semka.shumilov@gmail.com

ШУРЫГИН Борис Викторович — оператор научной роты Военной академии связи, shurigin66@mail.ru

ЭЛЬ САБАЯР ШЕВЧЕНКО Нидал — аспирант кафедра информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nzs.vus@gmail.com

ЮПЛОВ Вячеслав Юрьевич — магистрант группы ИСТ-841м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, s.uplov1@gmail.com

ЯКОВЛЕВ Тимур Александрович — старший оператор научной роты Военной академии связи, mx-m16@mail.ru

ЯРМУШ Василий Сергеевич — оператор 7-й научной роты Военной академии связи, vasiliy.yarmush@mail.ru

АВТОРСКИЙ УКАЗАТЕЛЬ

Авраменко В. С. **9, 13**
Адуевский А. М. **17**
Акимов С. В. **21, 24, 29**
Акчурина Д. Р. **32**
Андреев Д. А. **36**
Арзуманян Ю. В. **601, 606**
Аронов В. Ю. **41**
Атанов В. Д. **47**
Атаян А. М. **610**
Ахметова Ю. С. **52**
Бабаева А. В. **57**
Бажин М. И. **61**
Балакирев Д. Д. **67**
Баландин И. А. **72**
Баранов И. Ю. **76**
Беликов И. В. **81**
Белов М. П. **32**
Бирюков А. С. **86**
Блатова Т. А. **615**
Бовыкин Е. А. **91**
Боголепов Г. С. **95**
Бондаренко И. Б. **99**
Бородянский Ю. М. **104**
Бочкарев Д. А. **9**
Ботяков В. В. **108, 113, 117**
Бушуев С. Н. **122**
Быстров И. В. **127**
Ваганов А. В. **131, 136, 142**
Васильева Н. Н. **619**
Вачугова В. А. **131**
Верединский С. Ю. **625**
Вержаковская М. А. **41**
Верхова Г. В. **17, 91, 148, 151, 156, 161**
Вихарев А. Н. **164**
Волошененко Д. В. **169**
Волошинов Д. В. **173, 178, 182**
Волынкин П. А. **186**
Вольфсон М. Б. **601**
Воробьев А. А. **191**
Воронецкий А. А. **191**
Воронцов Д. М. **194**
Вострых А. В. **200**
Галиев Р. В. **208**
Германова Е. В. **211**
Гесь А. С. **173**
Глазков Г. С. **216**
Глыбин П. А. **221**
Горбань С. А. **225**
Гордеев М. А. **21**
Гордиевич Г. А. **229**
Григорьева А. А. **148**
Григорьева Е. В. **233**
Грищенко И. В. **32**
Громов В. В. **239, 242, 246**
Губин А. Н. **250, 254, 258**
Гуляева К. В. **263**
Гунина Е. В. **67, 268, 630**
Гурбатов Г. О. **272**
Давлетшина Э. Р. **24**
Дагаев А. В. **104**
Дворников А. С. **277**
Диченко С. А. **283**
Долгун В. О. **52**
Дуболазова Ю. А. **635, 639**
Дубонос А. С. **295**
Дульков М. В. **286**
Дымченко А. С. **291**
Евглевская Н. В. **295, 300**
Егорова М. А. **645**
Елагин В. С. **304**
Ершов А. В. **309, 315**
Жаранова А. О. **318, 324**
Жилин В. В. **328**
Жусов Д. Л. **334**
Закалкин П. В. **337**
Захаров А. А. **601, 606**
Зверев А. А. **342**
Зиберов В. О. **72**
Зикратов И. А. **347**
Золотов О. И. **351**
Иванов В. Г. **61**
Иванов А. С. **136**
Иванов А. Ю. **356**
Иванова С. В. **630**
Израилов К. Е. **361, 366**
Исаков А. В. **650**
Ишкова А. А. **142**

Кадынцев А. Н. **372**
Кадынцева Д. В. **375**
Казаков Д. Б. **52**
Казарин М. А. **380**
Казначеева Е. С. **178**
Казьмин М. А. **347**
Калегин М. А. **385**
Капитоненко В. В. **318**
Капчук Н. В. **277**
Карасенко А. О. **295**
Карев В. А. **61**
Киреева Н. В. **389**
Клеверов Д. А. **356**
Клеверов М. А. **356**
Ковалёв С. В. **655**
Козинцев Д. А. **393**
Козленко А. В. **334**
Козлова Л. П. **397, 401**
Козлова О. А. **405**
Колесников А. А. **408, 412**
Колесов Д. С. **151**
Кольцов П. О. **415**
Комашинский В. И. **122**
Комков Г. В. **99**
Комлев Г. О. **420**
Конников Е. А. **635**
Кононюк О. А. **186**
Корсун Н. А. **283**
Косов П. В. **426**
Косолапов В. С. **430**
Коткина М. С. **435**
Котов В. И. **660**
Красов А. В. **47**
Кривцов А. Н. **225**
Крюкова Е. С. **5, 440**
Кузнецов С. А. **361**
Кузькин А. А. **445**
Кукунин Д. С. **72, 451**
Курносов В. И. **455**
Куцакин М. А. **445, 461**
Кучеревский К. В. **17**
Кучеренко И. С. **397**
Лаба Р. З. **401**
Лапко А. Н. **461**
Лаута О. С. **295**
Лебедев А. С. **61**
Лебедев Н. С. **466**
Ликарь А. И. **471**
Липатников В. А. **86, 328, 380, 430, 474, 479**
Литвинов В. Л. **57, 127, 169, 250, 254, 258, 484, 489, 494, 500**
Лоборчук А. А. **505**
Макаров А. А. **484**
Макаров В. В. **615, 625, 635, 639, 655, 664, 668, 673**
Макеев С. М. **81**
Маликов А. В. **9, 13**
Малофеев В. А. **510**
Маркин Д. О. **164, 342, 515, 520, 525**
Маслова Е. А. **451**
Матвеев А. А. **474**
Медведев В. А. **530**
Мешков А. В. **678**
Миначев В. М. **515**
Михайличенко Н. В. **5, 194, 535**
Михалев О. А. **538**
Моисеева А. Я. **268**
Мурсалимова К. Б. **489**
Мусаева Т. В. кызы **385, 542**
Мутханна А. С. А. **505**
Налимов К. И. **315**
Невров А. А. **76**
Никонов Е. Р. **225**
Носов М. И. **309, 315**
Окатьева А. Д. **639**
Островский Ю. Н. **466**
Павлова Е. В. **650**
Панихидников С. А. **263**
Паничев А. Д. **272**
Пантюхин О. И. **122**
Паращук И. Б. **5, 122, 194, 440, 510**
Пацкан М. Ю. **52**
Песиков Э. Б. **420**
Петренко М. И. **538**
Поздняк И. С. **389**
Попков М. А. **535**
Присяжнюк С. П. **91, 156, 161**
Пронин А. А. **95**
Птицына Л. К. **291, 324, 351, 372, 375, 435, 547, 551**
Ребров Д. А. **304**
Резницкий А. Д. **108, 113, 117**
Рожкова Т. С. **556**
Рыков Д. А. **520**
Рябоконь В. В. **445**
Савченко С. О. **277**
Саенко И. Б. **122, 208, 286, 356**
Саклаков А. И. **342**
Сакова Н. В. **263**

Саломатин А. А. **561**
Сапожников Г. Н. **682**
Сенчук Д. В. **561**
Серова М. В. **239**
Симонина А. А. **678**
Симорин Б. И. **283**
Синица С. А. **655**
Скибинский И. Ю. **95**
Слесарчик К. Ф. **565**
Соколова Я. В. **606**
Соловьев Д. В. **108, 113, 117**
Соловьева А. В. **182**
Сотников А. Д. **601**
Старкова Т. Н. **668**
Стародубов Д. О. **625, 655**
Степаненко А. А. **619**
Стриженко В. Н. **535**
Суздальцева О. К. **570**
Султанова Я. М. **535**
Сулякаев Т. Р. **547**
Тарасов В. А. **36, 229, 570, 576, 580**
Татарникова И. М. **366**
Темникова М. В. **351**
Типаков В. С. **538**
Ткачев Д. Ф. **538**
Топорков Н. Ю. **108, 113, 117**
Трофимова Л. Д. **169, 489**
Трубицын В. Г. **586**
Урусова Н. Ф. **673**
Ушаков И. А. **272**
Ушаков А. В. **408**
Фабияновский И. Н. **286**
Фёдоров Н. С. **156**
Федорова А. В. **211, 366**
Федосеев Д. О. **466**
Филимонов Л. С. **494**
Филиппов Ф. В. **250, 254, 258, 318**
Филиппов Н. В. **389**
Флейснер В. В. **474**
Фурасьев Е. А. **576**
Хайбрахманова Е. С. **178, 415**
Хвостов М. А. **161**
Хилько А. С. **412**
Хо Т. Ч. **525**
Ходанович А. И. **591**
Хорошенко С. В. **216**
Черномырдин В. В. **595**
Чернявский А. В. **440**
Чеусов В. А. **586**
Шальков М. В. **500**
Шаповалов П. М. **580**
Шевченко А. А. **430**
Шестаков А. В. **221, 233, 455**
Шестаков Е. О. **510**
Шибаков Е. Д. **591**
Шиманчук С. Н. **99**
Ширев В. Ю. **366**
Шиян А. А. **393, 426, 595**
Шолухо Ю. А. **32**
Шумилов С. С. **451**
Шурыгин Б. В. **309**
Эль Сабаяр Шевченко Н. **551**
Юплов В. Ю. **29**
Яковлев Т. А. **538**
Ярмуш В. С. **479**