электронный научный журнал

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

ISSN 2307-1303

9 772307 130308 80413>

выпуск 4, 2013

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

электронный научный журнал, выпуск 4 за 2013 год

Учредитель и издатель федеральное государственное образовательное бюджетное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича» (СПбГУТ)

Settler and publisher Federal State Educational Budget-Financed Institution of Higher Vocational Education «The Bonch-Bruevich Saint - Petersburg State University of Telecommunications»

Адрес учредителя, издателя и редакции: 193232, Россия , С.-Петербург, пр. Большевиков д.22, корп.1, e-mail: telecomsut@gmail.com

Address of the Settler and Publisher, Editorial Office: 193232, Russia, St-Petersburg, Prospekt Bolshevikov 22 - 1, e-mail: telecomsut@gmail.com

Электронное представительство журнала - Electronic representative of the Journal
www.itt.sut.ru

Журнал зарегистрирован в Российском индексе научного цитирования (РИНЦ)
The Journal is included in Russian Index of Scientidic Quotation (RINTS)

Журнал имеет институт рецензирования. The Journal has review institute

Журнал распространяется через электронное представительство без ограничений и по адресно-целевой подписке через редакцию
The Journal is distributed by subscription through the editorial and electronic representative
Электронное издание. Цена свободная - On-line magazin. Free price

Редакция

Главный редактор
С. В. Бачевский, д-р техн. наук, профессор

Заместитель главного редактора
С. М. Доценко, д-р техн. наук, профессор

Научный редактор
А. Г. Владыко, канд. техн. наук

Ответственный секретарь Л. М. Минаков

Редактирование, корректура, верстка
Е. А. Аникевич, канд. техн. наук,
Е. М. Аникевич

IT сопровождение журнала Л. М. Минаков

Editorial Office

Editor-In-chief
S. Bachevsky, Professor, Dr. Of Science, (Eng-ing)

Deputy Editor-In-chief
S. Dotsenko, Professor, Dr. Of Science, (Eng-ing)

CEO & Science Editor
A. Vladyko, Cand. Of Science, (Eng-ing)

COO & Formation of a portfolio of publications L. Minakov

Literary editing, proofreading, page proofs by Anikevich E., , Cand. Of Science, (Eng-ing),
Anikevich E.

IT support by L. Minakov

Минимальные системные требования для просмотра сайта www.itt.sut.ru
Тип компьютера, процессор, сопроцессор, частота: Pentium IV и выше / аналогичное; оперативная память (RAM): 256 Мб и выше; необходимо на винчестере: не менее 64 Мб; ОС MacOS, Windows (XP, Vista, 7) / аналогичное; видеосистема: встроенная; дополнительное ПО: Adobe Reader версия от 7.X или аналогичное. Защита от незаконного распространения: реализуется встроенными средствами Adobe Acrobat.

СОДЕРЖАНИЕ

СЕТИ СВЯЗИ

Журавлёв Д. А., Бурлаков С. О., Николаенко В. В.
Способ повышения помехоустойчивости радиолинии
спутниковой связи и его техническая реализация 4

Журавлёв Д. А., Сальников Д. В., Светлакова О. В.
Способ организации спутниковой связи
при использовании многолучевых антенн на борту ретранслятора связи 10

СИСТЕМНЫЙ АНАЛИЗ И МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

Гойхман В. Ю., Коваленко Е. А.
Анализ хронологического среза нормативных правовых актов
отраслевой системы сертификации связи в контексте охвата
и категоризации сетевых элементов и их характеристик 15

Dotsenko S., Popovich T., Vladyko A., Makshanov A.
Application of aggregated indices randomization method for prognosing
the consumer demand on features of mobile navigation applications 26

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Ahmammouch Faiza
The strategy of the security of information
and telecommunication systems in Morocco 34

Летенко И. Д., Герасимова Е. М.
Нечеткая модель управления доступом к ресурсам
программно-конфигурируемых сетей на основе оценки рисков 41

Штеренберг С. И., Красов А. В.
Варианты вложения информации в исполнимый файл формата .Intel HEX 52

ИННОВАТИКА В ИНФОКОММУНИКАЦИЯХ

Макаров В. В., Блатова Т. А.
Инновации в информационно-коммуникационных технологиях
как атрибут экономики знаний 65

УДК 621.396.4

Д. А. Журавлёв, С. О. Бурлаков, В. В. Николаенко

Военная академия связи им. маршала Советского Союза С. М. Будённого

СПОСОБ ПОВЫШЕНИЯ ПОМЕХОУСТОЙЧИВОСТИ РАДИОЛИНИИ СПУТНИКОВОЙ СВЯЗИ И ЕГО ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ

радиолиния спутниковой связи, псевдослучайная перестройка рабочей частоты, отношение сигнал/шум.

Особенности организации спутниковой связи обуславливают наличие большого количества помех различного рода. Для повышения помехоустойчивости радиолинии применяют различные способы, одним из которых является псевдослучайная перестройка рабочей частоты (ППРЧ). Режим ППРЧ позволяет бороться с помехами сосредоточенными в узкой полосе частот. Однако в случае подавления радиолинии спутниковой связи (РЛСС) импульсными или ретрансляционными помехами, эффективность ППРЧ будет низкой.

Анализ известных способов передачи и приема информации по радиолинии с псевдослучайной перестройкой рабочей частоты (ППРЧ) позволил определить их достоинства и недостатки, а так же возможные пути их развития и совершенствования [1, 2]. Основываясь на принципах передачи и приема информации в радиолинии спутниковой связи с ППРЧ, предложен новый способ, который заключается в следующем. На передающем конце радиолинии формируют пакеты информации путем деления информационного сигнала на блоки заданной длины. После чего перестраивают несущую частоту передатчика на частоту, соответствующую коду псевдослучайной последовательности, с последующей ее модуляцией. Особенностью является то, что излучают радиосигнал с N-кратным повторением каждого информационного бита, на K частотных позициях в T временных интервалах (рис. 1).

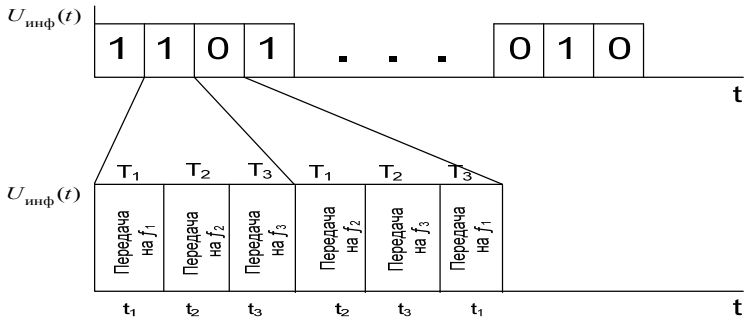


Рис. 1. Принцип организации передачи информации в РЛСС с ППРЧ

При равновероятном выборе частотных позиций сигнала с ППРЧ вероятность попадания на частоту, занятую помехой, будет определяться выражением $p_{п} = m/K$, где m – число частот, забитых помехой; K – общее число частот, выделенных для ППРЧ.

Генерируемый сигнал на основе кода модулируется частотой, синхронизируемой на основе несущей частоты передатчика. Излучение радиосигнала осуществляется сразу на нескольких частотах, которые образовывает генератор псевдослучайной последовательности (ПСП).

На приемной стороне радиолинии во 2-м приемопередающем устройстве переданный радиосигнал принимается N раз на K частотных позициях, соответствующих коду ПСП с последующей частотной фильтрацией в частотных фильтрах (ЧФ). Далее сигнал переносится на промежуточную частоту с последующим усилением и демодуляцией. Принятый сигнал поступает на коррелятор, где определяются корреляционные пики. Значение пика автокорреляционная функция (АКФ) на выходах корреляторов сравнивается с пороговым значением (рис. 2). Данное техническое решение позволяет отсеять помехи по временным окнам.

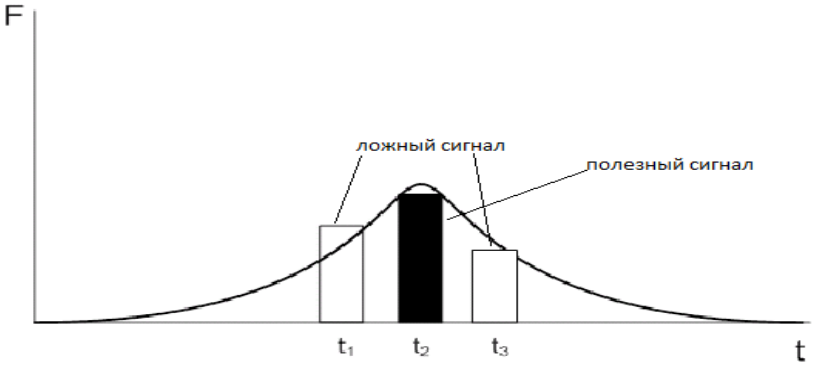


Рис. 2. Работа коррелятора по выделению информационного бита

После выделения информационного бита по мажоритарной схеме, вычисляют вероятность ошибки приема N повторенного одиночного бита $p^0_{\text{ош}}$. Далее ранжируют принятые значения одиночного бита в соответствии с величинами их вероятностей ошибок. Данная схема обеспечивает сравнивание между собой принятых сигналов, и выбор среди них сигнала с наименьшей вероятностью ошибки (рис. 3).

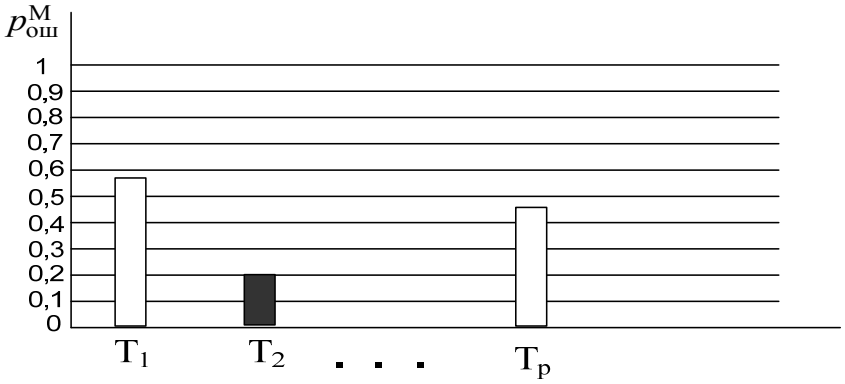


Рис. 3. Принятие решения по вероятности ошибки

Если вероятность ошибки приема бита на различных частотах в различные временные промежутки одинакова и равна $p_{\text{ош}1}$, то вероятность ошибочного приёма бита при мажоритарном декодировании равна

$$p_{\text{ош}}(M) = \sum_{i=\frac{M+1}{2}}^{M} C^i_M \cdot p^i_{\text{ош}1} \cdot (1 - p^0_{\text{ош}1})^{M-i},$$

где M – число повторений информационного бита; $p^0_{\text{ош}1}$ – вероятность ошибки бита при однократном приеме; $C^i_M = \dfrac{M!}{i!(M-i)!}$ – число сочетаний из M по i.

В реальных радиолиниях вероятность ошибки приема бита на разных частотах различна. В этом случае для вычисления вероятности ошибки при мажоритарном декодировании необходимо решить переборную задачу. Например, при $N = 3$ вероятность ошибочного приема бита определяется выражением:

$$p_{\text{ош}}(3) = p_{\text{ош}\,1} p_{\text{ош}\,2} p_{\text{ош}\,3} + (1 - p_{\text{ош}\,1}) p_{\text{ош}\,2} p_{\text{ош}\,3} +$$
$$+ p_{\text{ош}\,1}(1 - p_{\text{ош}\,2}) p_{\text{ош}\,3} + p_{\text{ош}\,1} p_{\text{ош}\,2}(1 - p_{\text{ош}\,3}).$$

Проведенные расчеты показывают, что в зависимости от вероятностей ошибок на отдельных частотах целесообразно исключать их из принятия решения о принятом бите. Использовать параллельно с деко-

дированием по всем N повторов бита, также по $N-2$ повторов взятых по лучшим вероятностям ошибок одиночного приёма бита, трёх лучших повторов. Определять вероятности ошибок $p_{ош}(M)$ для каждого декодирования. Решение о принятом бите принимается в результате сравнивания вероятностей ошибок по минимальной (рис. 4).

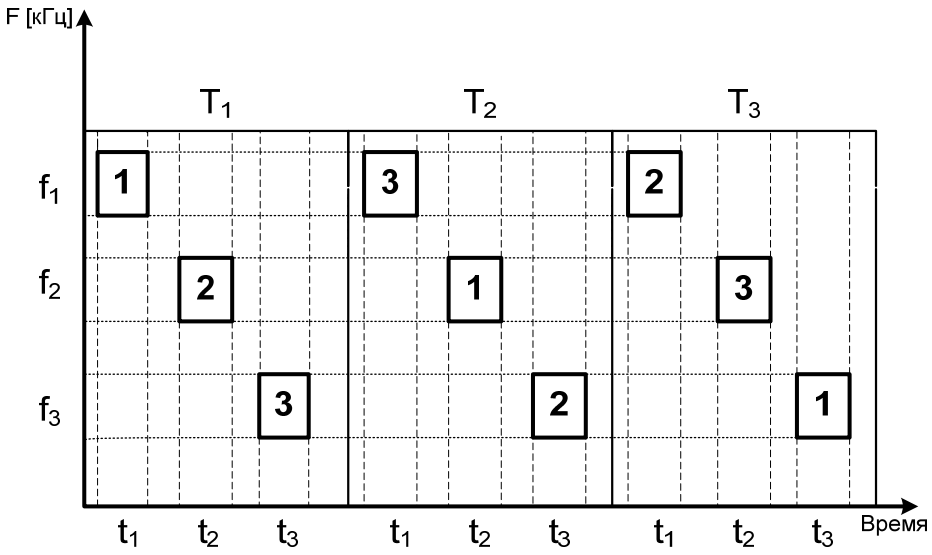


Рис. 4. Пример передачи трёх информационных битов

Сигнал с выхода коррелятора подается дальше в оконечное устройство. Одновременно информация о частотах, на которых отношение сигнал/шум наихудшие, поступает на генератор ПСП, который исключает их на временной период T из списка разрешенных для перестройки. Одновременно эта информация со списком пораженных частот передается на 1-е приемопередающее устройство. С приемника эта информация поступает в генератор ПСП, который аналогично исключает пораженными частотами из передачи.

Схема радиолинии с ППРЧ представлено на рисунке 5.

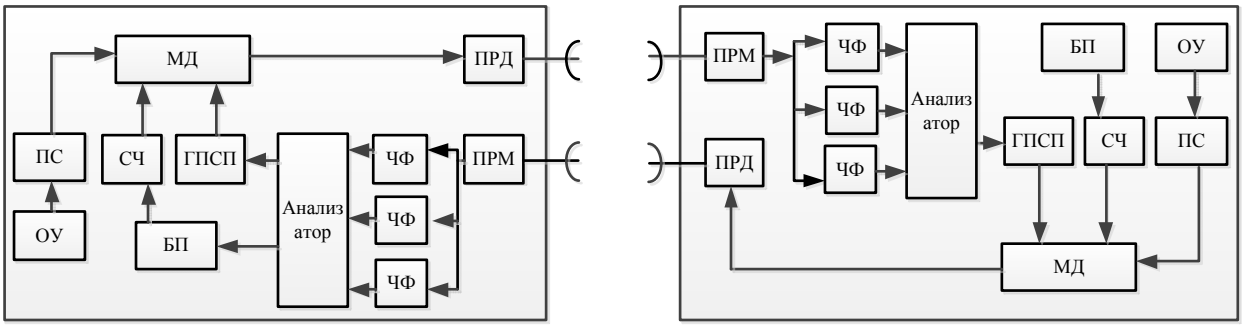


Рис. 5. Схема передачи и приема дискретной информации в радиолинии с ППРЧ

На передающем конце сигнал от оконечного устройства (ОУ) поступает в преобразователь сигнала (ПС), где происходит деление информационного сигнала на блоки заданной длинны. С выхода преобразователя информационные блоки подаются на первый вход модулятора (МД). Определенный в БП код ПСП с генератора ПСП (ГПСП) подается на информационный (второй) вход МД, где он модулируется частотой, синтезируемой частотным синтезатором (СЧ) на основе определенной в БП несущей частоты передатчика. Модулированная ПСП излучается в пространство с помощью антенны.

На приемном конце радиолинии входной сигнал, принятый антенной 2-го приемопередающего устройства, поступает на информационные входы ЧФ. Каждый из ЧФ настроен на частоту ($F_{\text{ППРЧ}}$), значение которой хранится в БП. С выходов ЧФ принятый сигнал поступает в анализатор, где вычисляется вероятность ошибок принятых сигналов. На выходе анализатора сигнал разветвляется. На первое направление поступает сигнал с лучшими показателями по отношению сигнал/шум. Он подаётся на преобразователь, который преобразует двоичную информационную последовательность в форму выходного сигнала. С выхода преобразователя сигнал передается в оконечное устройство. На второе направление поступает информация о частотах, на которых отношение сигнал/шум наихудшее. Эта информация формируется в виде информационного пакета, который поступает на генераторы ПСП 1-го и 2-го приемопередающих устройств.

Данный способ позволит значительно повысить уровень помехозащищённости радиолинии спутниковой связи, т. к. вероятность подавления сигнала на различных частотах и в разные временные интервалы мала, с одновременным исключением из передачи частот, на которых отношение сигнал/шум наихудшее.

Список используемых источников

1. **Челышев, В. Д.** Радиоинтерфейсы спутниковых систем персонального радиоинтерсервиса : учебное пособие / В. Д. Челышев, В. В. Якимовец. – СПб. : ВУС, 2003. – 364 с.

2. **Волков, Л. Н.** Системы цифровой радиосвязи: базовые методы и характеристики : учебное пособие / Л. Н. Волков, М. С. Немировский, Ю. С. Шинаков. – М. : Эко-Трендз, 2005. – С. 213–218.

Аннотация

В статье предлагается способ повышения помехоустойчивости радиолинии спутниковой связи, в котором используется передача сигнала на различных частотах и в разные временные интервалы с одновременным исключением из передачи частот, на которых отношение сигнал/шум наихудшее.

D. Zhuravlev, S. Burlakov, V. Nikolaenko

Military Academy of Communications

WAY TO INCREASE THE NOISE IMMUNITY OF RADIO LINK SATELLITE COMMUNICATION AND ITS TECHNICAL IMPLEMENTATION

Annotation

This article proposes a method of improvement of noise immunity of radio link satellite communications, which uses the transfer of the signal at different frequencies and in different time intervals, with the simultaneous exclusion of transmission frequency at which the signal/noise ratio for the worst.

Keywords: a radio link satellite communications, pseudorandom operating frequency agility, signal/noise ratio.

References

1. **Chelyshev, V. D.** Radiointerfejsy sputnikovyh sistem personal'nogo radiointerservisa : uchebnoe posobie / V. D. Chelyshev, V. V. Jakimovec. – SPb. : VUS, 2003. – 364 s.
2. **Volkov, L. N.** Sistemy cifrovoj radiosvjazi: bazovye metody i harakteristiki : uchebnoe posobie / L. N. Volkov, M. S. Nemirovskij, Ju. S. Shinakov. – M. : Jeko-Trendz, 2005. – S. 213–218.

Журавлёв Дмитрий Анатольевич – кандидат технических наук, преподаватель, Федеральное государственное казённое военное образовательное учреждение высшего профессионального образования «Военная академия связи им. маршала Советского Союза С. М. Будённого», ZhuravlevDmitriy84@yandex.ru

Бурлаков Сергей Олегович – доктор технических наук, профессор, Федеральное государственное казённое военное образовательное учреждение высшего профессионального образования «Военная академия связи им. маршала Советского Союза С. М. Будённого»

Николаенко Виталий Владимирович – курсант, Федеральное государственное казённое военное образовательное учреждение высшего профессионального образования «Военная академия связи им. маршала Советского Союза С. М. Будённого»

УДК 621.396.4

Д. А. Журавлёв, Д. В. Сальников, О. В. Светлакова

Военная академия связи им. маршала Советского Союза С. М. Будённого

СПОСОБ ОРГАНИЗАЦИИ СПУТНИКОВОЙ СВЯЗИ ПРИ ИСПОЛЬЗОВАНИИ МНОГОЛУЧЕВЫХ АНТЕНН НА БОРТУ РЕТРАНСЛЯТОРА СВЯЗИ

ретранслятор связи, многолучевая антенна, отношение сигнал/шум.

В настоящее время существует достаточное количество способов организации связи в системах спутниковых связи (СС) с многолучевыми антеннами (МЛА) на борту ретранслятора связи (РС) [1, 2]. Однако все эти способы не в полной мере реализуют возможность перераспределения энергетического потенциала радиолиний между зонами обслуживания в зависимости от активности абонентов и помеховой обстановкой.

Система СС включает в себя наземный и космический сегменты. Космический сегмент включает в себя один или несколько РС с МЛА на борту. Наземный сегмент включает в себя одну центральную земную станцию (ЦЗС) и несколько периферийных земных станций (ПЗС) произвольно расположенных на обслуживаемой территории, причем ПЗС могут быть как стационарными, так и подвижными, что соответственно приводит к колебанию трафика между зонами обслуживания. Время и продолжительность сеансов связи между ПЗС произвольное. На радиолинии СС могут воздействовать различного рода помехи, время и место появления которых заранее неизвестно.

В этих условиях необходимо разработать такой способ организации спутниковой связи, при котором обеспечивалось повышение скрытности ПЗС и требуемое качество связи между абонентами.

Суть способа. Центральная земная станция через РС организует помехозащищенный канал СС, который принимается всеми ПЗС (рис. 1). Перед выходом на сеанс связи, ПЗС посылают на ЦЗС заявку на установление соединения для информационного обмена и идентификационную метку с координатами места своего расположения. Координаты определяются с помощью спутниковой радионавигационной системы ГЛОНАСС или GPS. Вся зона обслуживания абонентов в зависимости от координат условно поделена между лучами МЛА. За каждым лучом МЛА определены несколько зон обслуживания имеющих различные приоритеты, которые определяются исходя из предельной дальности радиовидимости.

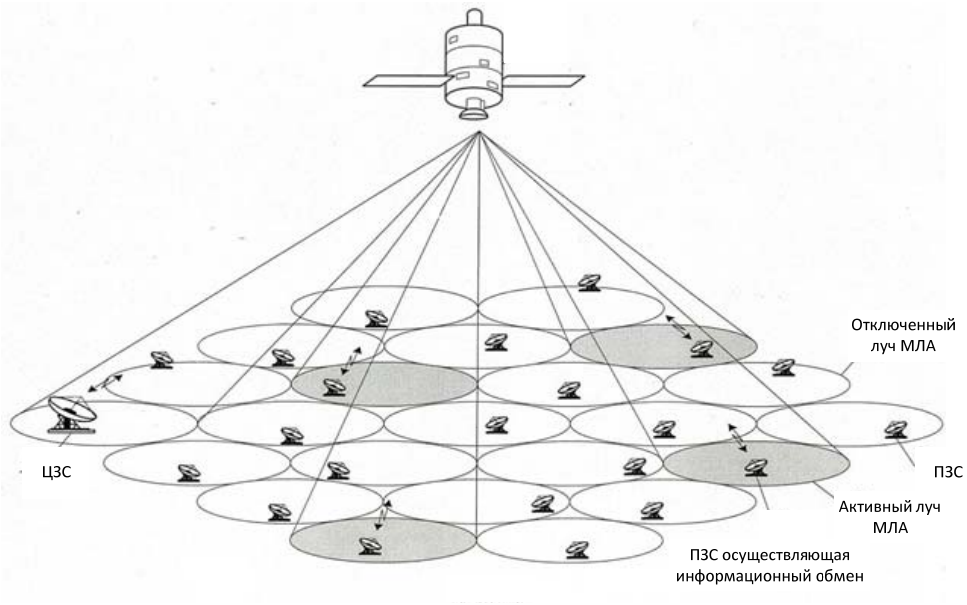


Рис. 1. Система спутниковой связи с использованием МЛА на РС

Например, к зоне обслуживания первого приоритета относится территория с углом радиовидимости от $\beta = 90^0$ до $\beta = 60^0$, ко второму от $\beta = 60^0$ до $\beta = 30^0$ и к третьему от $\beta = 30^0$ до $\beta = 0^0$. Сбор заявок от ПЗС осуществляется ЦЗС в режиме реального времени. После чего обобщенные данные передаются на РС с МЛА в виде целеуказаний для перестройки номеров лучей МЛА по зонам обслуживания, в которых расположены ПЗС, от которых поступили заявки, а остальные, не задействованные лучи отключаются.

После окончания информационного обмена, ПЗС посылает сигнал «Отбой» на ЦЗС. Если в данный момент времени в данном районе других ПЗС, ведущих информационный обмен нет, то ЦЗС отключает луч на МЛА обслуживающий эту зону обслуживания. Кроме того ЦЗС осуществляет мониторинг качества информационного обмена и абонентскую нагрузку в каждом луче МЛА. При несоответствии качества связи, ЦЗС может либо перераспределить мощность передачи между лучами МЛА за счет неактивных лучей, тем самым обеспечив требуемое отношение сигнал/шум либо изменить диаграмму направленного действия этого луча или на время полностью отключить данный луч. Кроме того мониторинг, проводимый ЦЗС, позволяет оценить нагрузку по трафику в зонах обслуживания каждого луча и рассчитать требуемое количество каналов для его обслуживания.

Предложенные для «Способа организации спутниковой связи при использовании многолучевых антенн на борту ретранслятора связи» организационно-технические решения позволяют перераспределять энергетику между активными и неактивными лучами МЛА и тем самым

обеспечивать требуемое качество связи в зонах обслуживания при воздействии различного рода помех.

Пример расчета показателей сигнал/шум на один луч МЛА РС для предложенного способа.

Исходные данные. Тип орбиты – геостационарная (высота орбиты H_0 = 35 786 км), радиус Земли $R_З$ = 6 371 км. Многоканальная антенна гексагональной конструкции с числом колец $n_k = 9$ формирует $n = 250$ лучей. Для этого используется $m = 128$ усилителей мощности по $P_у$=17 Вт каждый. На один луч приходится мощность $P_л$ = 9,4 дБВт. Усиление многолучевой антенны на один луч $G_л = 34{,}8$ дБ, а ЭИИМ $E_л = 44{,}2$ дБВт. Энергетическая полоса сигналов в луче $\Delta F_л = 7 \cdot 10^5$ Гц. Частота работы $f = 1{,}55$ ГГц. Добротность тракта приема $Q_{РС} = 6{,}3$ дБ/К.

Абонентский терминал имеет мощность на передачу $P_{АТ} = 2$ Вт = 3 дБВт, добротность тракта приема $Q_{АТ} = -24$ дБ/К, усиление антенны $G_{АТ}$= 3 дБ и ЭИИМ $E_{АТ}$ = 4 Вт = 6 дБВт, энергетическую полосу передаваемого АТ сигнала $\Delta F_{АТ} = \Delta f_i$ = 27,7 кГц = $2{,}77 \cdot 10^4$ Гц. Частота работы $f = 1{,}65$ ГГц.

Радиолиния спутниковой связи РС-АТ. Для зоны обслуживания 3-го приоритета отношение сигнал/шум, согласно расчетов, изменяется в пределах γ= 1,52 до γ= 1,75. Для зоны обслуживания 2-го приоритета отношение сигнал/шум изменяется в пределах γ = 1,75 до γ = 2. Для зоны обслуживания 1-го приоритета отношение сигнал/шум изменяется в пределах γ= 2,0 до γ= 2,05.

Расчёт энергетики радиоинтерфейсов линейных трактов передачи на радиолинии РС-АТ с учетом предложенного способа, т. е. на МЛА активны только лучи тех зон, в которых АТ осуществляют информационный обмен. Допустим из 250 лучей активны только 10. Тогда на один луч будет приходиться мощность $P_л = P_у m / n$ = 217,6 Вт и ЭИИМ ретранслятора на один луч МЛА составит $E_{РС} = P_л G_л$ = $6{,}5 \cdot 10^5$ Вт. Тогда на радиолинии спутниковой связи РС – АТ отношение сигнал/шум для угла места β^0=0 будет равно γ = 37,9, для угла места $\beta = 30^0$ будет равно γ = 43,65, для угла места $\beta = 60^0$ будет равно γ = 50,12 и для угла места $\beta = 90^0$ будет равно γ = 51,28.

График сравнения отношения сигнал/шум на радиолинии РС-АТ существующего и перспективного (предлагаемого) способа организации спутниковой связи при различных углах радиовидимости представлен на рисунке 2.

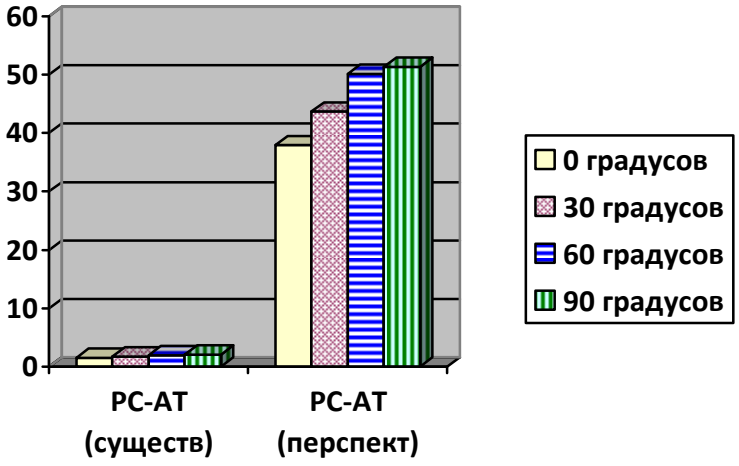


Рис. 2. Сравнение показателей сигнал/шум существующего и перспективного способа организации связи

Предлагаемый способ технически реализуем, поскольку базируется на известных и отработанных устройствах. Его можно использовать как в существующих, так и перспективных системах спутниковой связи с МЛА на РС.

Список используемых источников

1. **Челышев, В. Д.** Радиоинтерфейсы спутниковых систем персонального радиоинтерсервиса : учебное пособие / В. Д. Челышев, В. В. Якимовец. – СПб. : ВУС, 2003. – 364 с.

2. **Волков, Л. Н.** Системы цифровой радиосвязи: базовые методы и характеристики : учебное пособие / Л. Н. Волков, М. С. Немировский, Ю. С. Шинаков. – М. : Эко-Трендз, 2005. – С. 213–218.

Аннотация

В статье предлагается способ организации связи в спутниковой системе связи при использовании многолучевых антенн на борту ретранслятора связи. В качестве способа предполагается использовать возможность перераспределения энергетики и лучей многолучевой антенны ретранслятора связи по зонам обслуживания.

D. Zhuravlev, D. Salnikov, O. Svetlakova

Military Academy of Communications

A METHOD OF ORGANIZATION OF SATELLITE COMMUNICATION WHEN USING MULTIBEAM ANTENNAS ONBOARD REPEATER CONNECTION

Annotation

This article proposes a method of organization of communication in a satellite-based system using multibeam antennas onboard repeater links. As a way it is supposed to use the possibility of redistribution of energy and rays multibeam antenna relay communication in zones of maintenance.

Keywords: relay connection, multibeam antenna, signal/noise ratio.

References

1. **Chelyshev, V. D.** Radiointerfejsy sputnikovyh sistem personal'nogo radiointerservisa : uchebnoe posobie / V. D. Chelyshev, V. V. Jakimovec. – SPb. : VUS, 2003. – 364 s.
2. **Volkov, L. N.** Sistemy cifrovoj radiosvjazi: bazovye metody i harakteristiki : uchebnoe posobie / L. N. Volkov, M. S. Nemirovskij, Ju. S. Shinakov. – M. : Jeko-Trendz, 2005. – S. 213–218.

Журавлёв Дмитрий Анатольевич – кандидат технических наук, преподаватель, Федеральное государственное казённое военное образовательное учреждение высшего профессионального образования «Военная академия связи им. маршала Советского Союза С. М. Будённого», ZhuravlevDmitriy84@yandex.ru

Сальников Денис Владимирович – кандидат технических наук, старший преподаватель, Федеральное государственное казённое военное образовательное учреждение высшего профессионального образования «Военная академия связи им. маршала Советского Союза С. М. Будённого», denis_salnikov@mail.ru

Светлакова Оксана Викторовна – курсант, Федеральное государственное казённое военное образовательное учреждение высшего профессионального образования «Военная академия связи им. маршала Советского Союза С. М. Будённого»

УДК 621.395.36

В. Ю. Гойхман, Е. А. Коваленко

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

АНАЛИЗ ХРОНОЛОГИЧЕСКОГО СРЕЗА НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ ОТРАСЛЕВОЙ СИСТЕМЫ СЕРТИФИКАЦИИ СВЯЗЬ В КОНТЕКСТЕ ОХВАТА И КАТЕГОРИЗАЦИИ СЕТЕВЫХ ЭЛЕМЕНТОВ И ИХ ХАРАКТЕРИСТИК

нормативный правовой акт, сертификация, декларирование, сетевой элемент, технология.

Известно, что телекоммуникационная отрасль – одна из самых быстроразвивающихся в мире. Еще полвека назад люди радовались появлению в доме стационарного телефона, а теперь мы и дня не можем прожить без компьютера и мобильного телефона. Этот пример наглядно демонстрирует не только быстрый рост новых технологий, но и появление большого количества различных средств связи на рынке телекоммуникаций. И чтобы обеспечить целостность и устойчивость сети связи в России, были приняты законы, выдвигающие определенные требования к существующему оборудованию.

Федеральный закон «О связи» [1] устанавливает правила по подтверждению соответствия оборудования связи, направленные на обеспечение целостности, устойчивости функционирования и безопасности сети связи общего пользования. В этих правилах содержатся требования по электромагнитной совместимости, по устойчивости к климатическим и механическим воздействиям, по устойчивости к изменениям напряжения электропитания и т. п. Декларация о соответствии и сертификат соответствия в области связи являются подтверждением того, что приобретаемое оборудование отвечает определенным требованиям. Оборудование, в случае несоответствия которого существующим требованиям, может вызвать угрозу безопасности, устойчивости функционирования и целостности сети связи, подлежит подтверждению соответствия в форме сертификации, в остальных же случаях проводится декларирование. Ранее оборудование проверялось на соответствие общим техническим требованиям (ОТТ), но с 2005 года оно должно соответствовать требованиям,

изложенным в нормативных правовых актах (НПА). В НПА указываются конкретное оборудование, к которому предъявляются требования к параметрам и характеристикам, а также к процедуре подтверждения соответствия (сертификации или декларированию) [2–5].

Первые НПА были приняты в 2005 году, тогда же выпущены 3 первых документа, а уже в следующем году их общее количество увеличилось до 29. В 2007 году приняты новые правила подтверждения соответствия, и это дало толчок, для увеличения количества НПА: только за этот год их выпустили 35 (рис. 1). Далее, мы видим значительное уменьшение количества выпущенных нормативных правовых актов. Это связано, видимо, с тем, что чем больше НПА появлялось, тем больше оно покрывало необходимое для подтверждения соответствия оборудование. Таким образом, теперь нормативные правовые акты выпускаются только при появлении нового оборудования, или же при необходимости внесения изменений в существующие НПА (например, при изменении определенных характеристик оборудования).

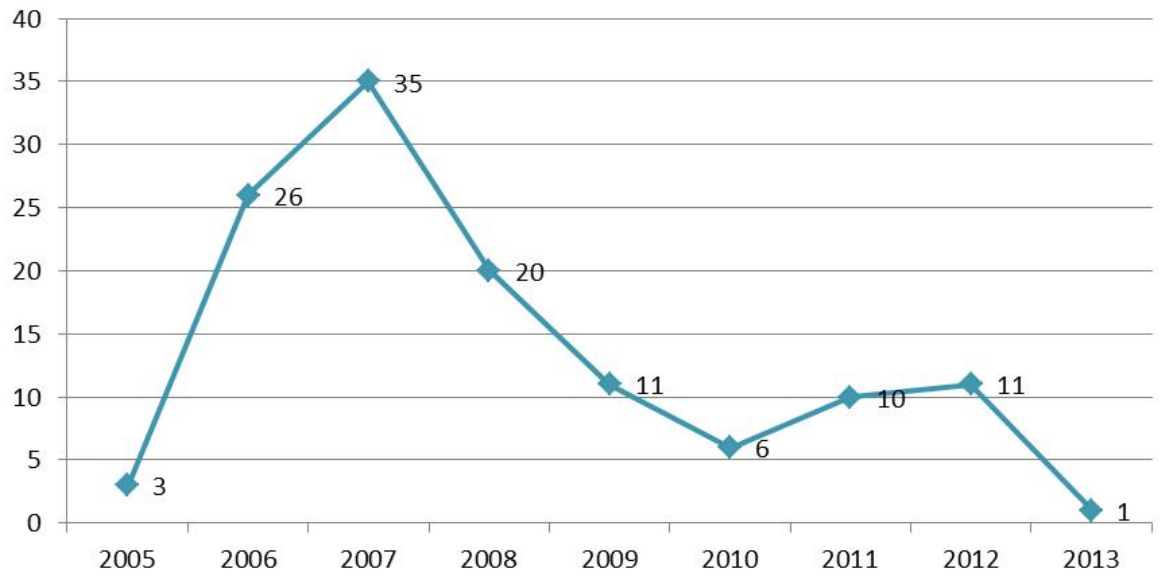


Рис. 1. Распределение НПА по годам выпуска

В итоге, в дальнейшем можно ожидать значительный рост количества выпускаемых нормативных правовых актов только в случае появления нового разнородного оборудования, которое не подходит под описание и критерии существующих НПА.

В ходе исследования проанализированы 123 нормативных правовых акта, выпущенных на данный момент, из которых взят перечень оборудования, составивший 419 пунктов. Из этого перечня произведена выборка сетевых элементов (при этом, всё повторное оборудование, совпадавшее по свойствам, было объединено), в результате которой получилось 189 сетевых элементов. То есть, количество сетевых элементов в

два с лишним раза меньше, чем количество оборудования, указанного в НПА (рис. 2).

Рис. 2. Выделение сетевых элементов из массива оборудования НПА

Выявление сетевых элементов проводилось в несколько этапов. Для начала, было объединено одинаковое по названию оборудование; при этом учитывалось, что в некоторых случаях данное обстоятельство вовсе не являлось гарантом того, что одинаковое по названию оборудование имеет различное применение. Далее сделано объединение по стандартам. Так, например, в один сетевой элемент «Абонентская радиостанция сетей подвижной радиосвязи» с учетом стандартов для дальнейшего анализа были объединены:

– абонентская радиостанция сетей подвижной радиосвязи стандарта TETRA;

– абонентская радиостанция сетей подвижной радиосвязи стандарта DMR;

– абонентская радиостанция сетей подвижной радиосвязи стандарта Цитран.

Аналогично, пункты «Городская автоматическая телефонная станция, использующая технологию коммутации пакетов информации» и «Городская автоматическая телефонная станция, использующая систему сигнализации ОКС № 7» были объединены в сетевой элемент «Городская автоматическая телефонная станция».

По 189 сетевым элементам, а также по всем НПА будет проводиться дальнейший анализ и классификация по различным критериям: год выпуска НПА; сеть, к которой относятся сетевые элементы; процедура под-

тверждения соответствия; характеристики и т. п. Все результаты были проанализированы, по ним получены соответствующие выводы, которые, в свою очередь, подтверждены в ходе дальнейшего анализа.

В качестве примера целесообразно привести список некоторых сетевых элементов, которые использованы в данном исследовании:

– абонентская подвижная земная станция спутниковой связи,
– абонентская радиостанция сетей подвижной радиосвязи,
– абонентская станция радиотелефонной связи,
– автоматизированные системы расчетов,
– антенно-фидерное устройство,
– антенные усилители двунаправленные,
– аттенюатор,
– интерфейсная плата,
– кабель связи оптический,
– кабель связи с металлическими жилами,
– кодер,
– комбинированная станция,
– коммутатор,
– концентратор,
– кроссовое оборудование,
– маршрутизатор,
– модулятор,
– мультиплексор,
– муфта для монтажа кабелей связи,
– оконечная установка телеграфной связи,
– оптический распределитель,
– преобразователь частоты,
– сетевая карта,
– сервер,
– таксофон,
– телефонный аппарат,
– трансформаторы абонентские,
– УАТС,
– узел управления услугами,
– циркулятор,
– центр эксплуатации и технического обслуживания.

Как можно заметить, представленные сетевые элементы крайне разнообразны как по областям применения, так и по структуре. Поэтому, следующий шаг исследования был направлен на упорядочение всех 189 сетевых элементов.

Для начала, все сетевые элементы были распределены по сетям, в которых они применяются. Для этого целесообразно воспользоваться моделью инфокоммуникационной системы, которая была предложена

ITU-T. Согласно этой модели, выделяются четыре сети: Сеть в помещении пользователя, Сеть доступа, Базовая сеть и Средства поддержки услуг (рис. 3).

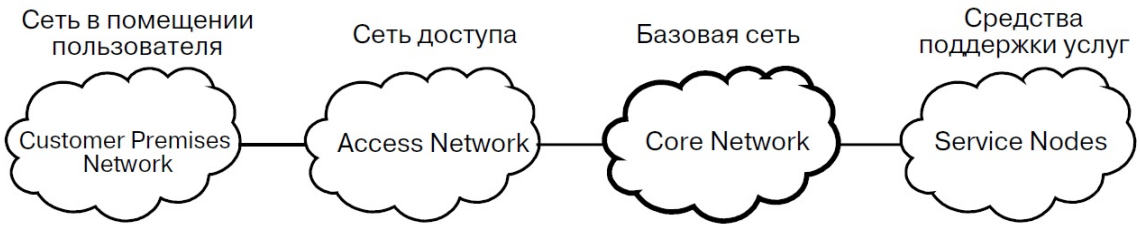


Рис. 3. Модель телекоммуникационной системы, предложенная ITU-T

После распределения сетевых элементов по данным сетям, получилось, что к Сети в помещении пользователя и к Сети доступа относятся по 25 сетевых элементов. К Средствам поддержки услуг принадлежат 10 элементов, а самой большой получилась Базовая сеть – 129 сетевых элементов. Таким образом, можно сделать вывод о том, что в сети оператора связи встречается самое разнообразное оборудование (рис. 4).

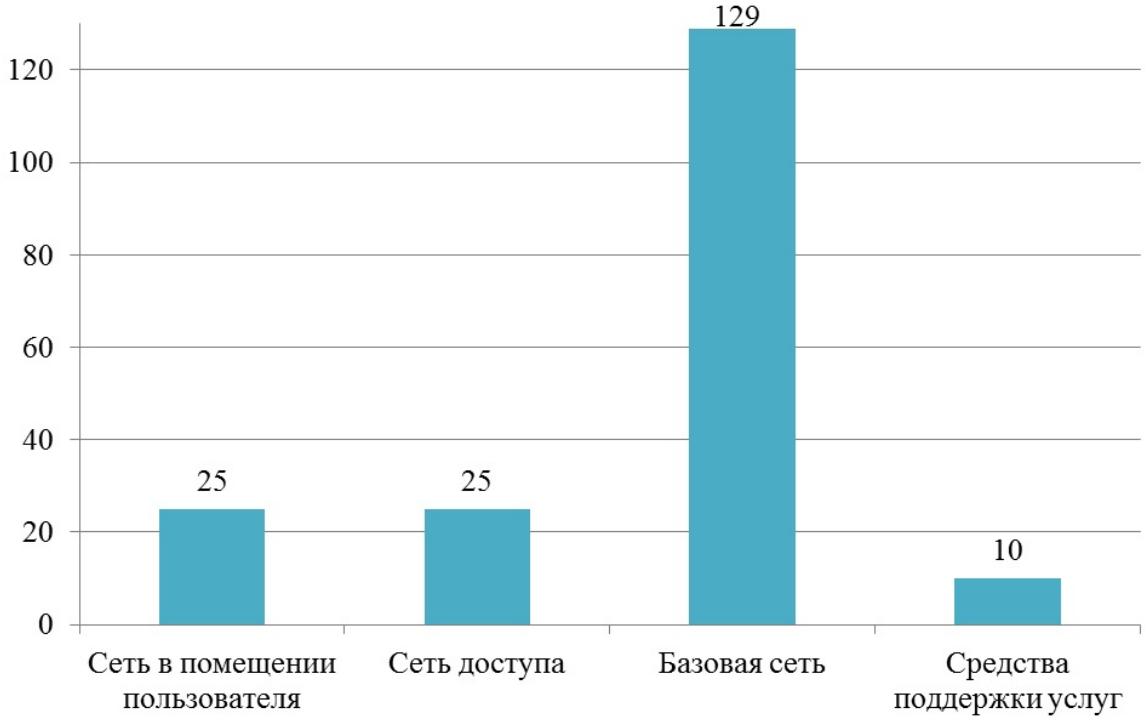


Рис. 4. Распределение сетевых элементов по сетям

Если говорить об общем массиве выделенных нами сетевых элементов, то после разделения по сетям, можно увидеть, что процедуре подтверждения соответствия подлежат 118 сетевых элементов, а, декларированию – 71 (рис. 5).

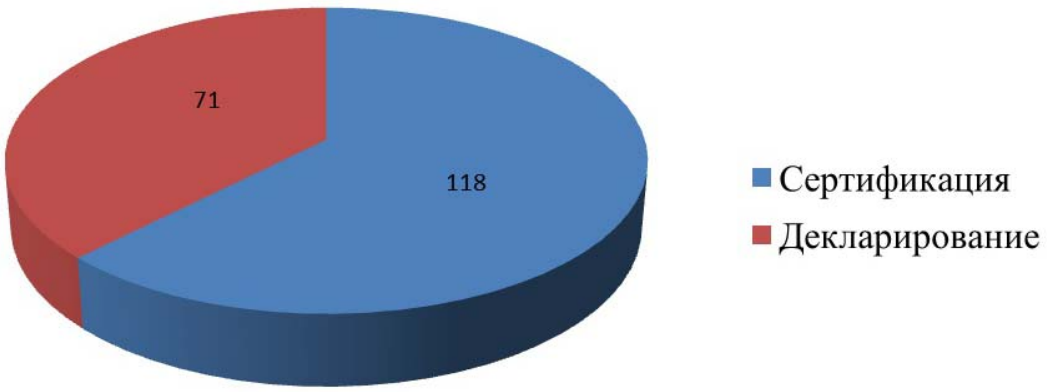


Рис. 5. Распределение сетевых элементов по процедуре подтверждения соответствия

Далее, распределив полученные данные по сетям и процедуре подтверждения соответствия, можно увидеть следующую диаграмму (рис. 6).

Рис. 6. Распределение сетевых элементов по сетям,
с учетом процедуры подтверждения соответствия

Так, можно заметить, что различные, например, абонентские устройства, принадлежащие Сети в помещении пользователя, равно как и сетевые элементы, относящиеся к Средствам поддержки услуг, в большинстве своем подлежат подтверждению соответствия в форме декларирования. В Сети доступа больше элементов должны проходить сертификацию, чем декларирование. Для Базовой сети число сетевых элементов, подлежащих сертификации соответствия, в несколько раз больше, чем декларируемых элементов; это говорит не только о много-

численности и разнообразности оборудования на сети оператора связи, но и о том, насколько сильно оно может, в случае нарушения работоспособности, повлиять на устойчивость и функциональность сети.

Если рассмотреть сертифицируемые сетевые элементы Базовой сети, то отметим, что значительную часть составляют сетевые элементы радиотелефонной связи – 29. В свою очередь, к радиовещанию относятся 4 сетевых элемента, к радиодоступу – 1, к радиорелейной связи – 5, к радиосвязи и радиоэлектронным средствам связи – по 2, а остальные не принадлежат ни к одной из вышеперечисленных групп и в большинстве своем составляют оборудование АТС, которое будет рассматриваться далее.

Что касается сетевых элементов радиотелефонной связи, то отметим, что основные их отличия заключаются в использовании различных технологий, что наглядно демонстрируется на рисунке 7.

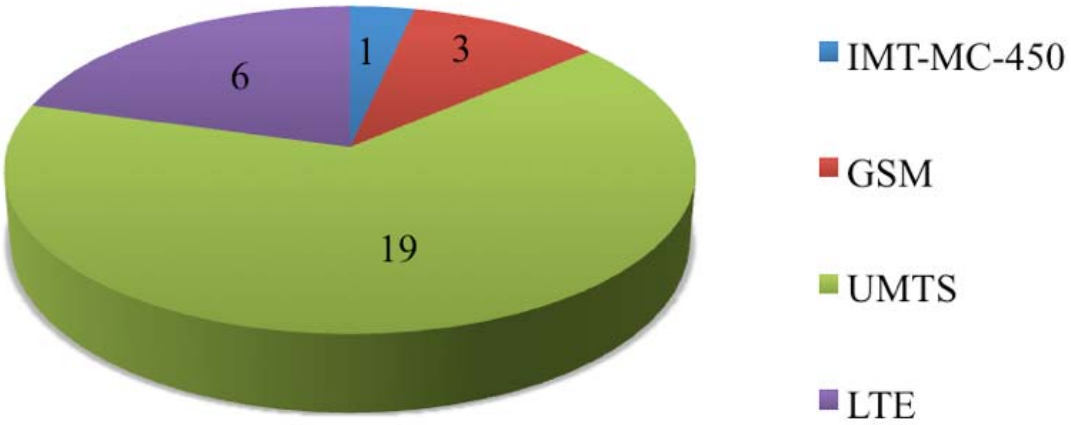


Рис. 7. Распределение сетевых элементов Базовой сети радиотелефонной связи по технологиям

Для рассмотрения полученных данных следует учитывать, что для технологии UMTS вышел нормативный правовой акт, в котором устанавливаются требования к перечню оборудования на основе IP Multimedia Subsystem (IMS), которое несколько изменило ожидаемую картину. Что же касается LTE, то уже в ближайшем будущем, в связи с развитием технологии, можно ожидать увеличение количества выпускаемых НПА, относящихся к LTE.

Если же вернуться к рассмотрению сетевых элементов, относящихся к АТС, то на рисунке 8 наглядно показано распределение по видам станций, причем под «Местной телефонной станцией» понимается как «Городская автоматическая телефонная станция», так и «Сельская автоматическая телефонная станция», указанные в НПА.

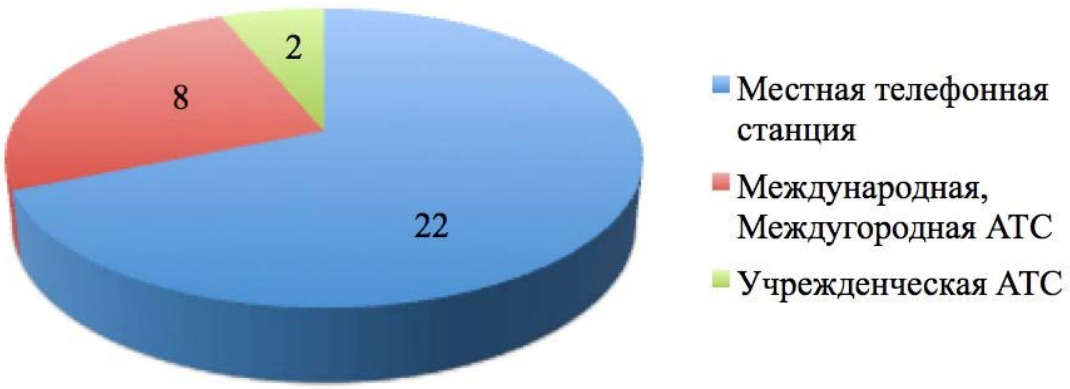


Рис. 8. Распределение сетевых элементов телефонных станций

При анализе данной диаграммы, как и в случае с радиотелефонной связью, следует учитывать влияние IMS на Местные телефонные станции, которое влияет на статистику. Также следует отметить выпуск НПА для станций, которые отличаются применением коммутации пакетов информации, или общеканальной сигнализацией № 7 (ОКС № 7).

Полученные в ходе исследования результаты показывают ситуацию с точки зрения государственного регулирования; для полной картины следует рассмотреть и проанализировать выданные сертификаты и декларации, чтобы увидеть положение вещей глазами производителей оборудования, а затем сравнить полученные результаты.

По результатам проводимого исследования создается база данных нормативных правовых актов. В качестве основы была выбрана система управления содержимым Drupal, архитектура которого позволяет применять различные модули для унифицирования работы сайта. Так, например, модуль таксономии позволяет категоризировать все НПА по определенным характеристикам, таким как год выпуска, сеть применения, процедура подтверждения соответствия и т. п.

На рисунке 9 показана выборка нормативных правовых актов по 2005 году. В конкретном случае можно продолжить поиск необходимого нормативного правового акта по сетям, или ознакомиться с текстом предложенных НПА.

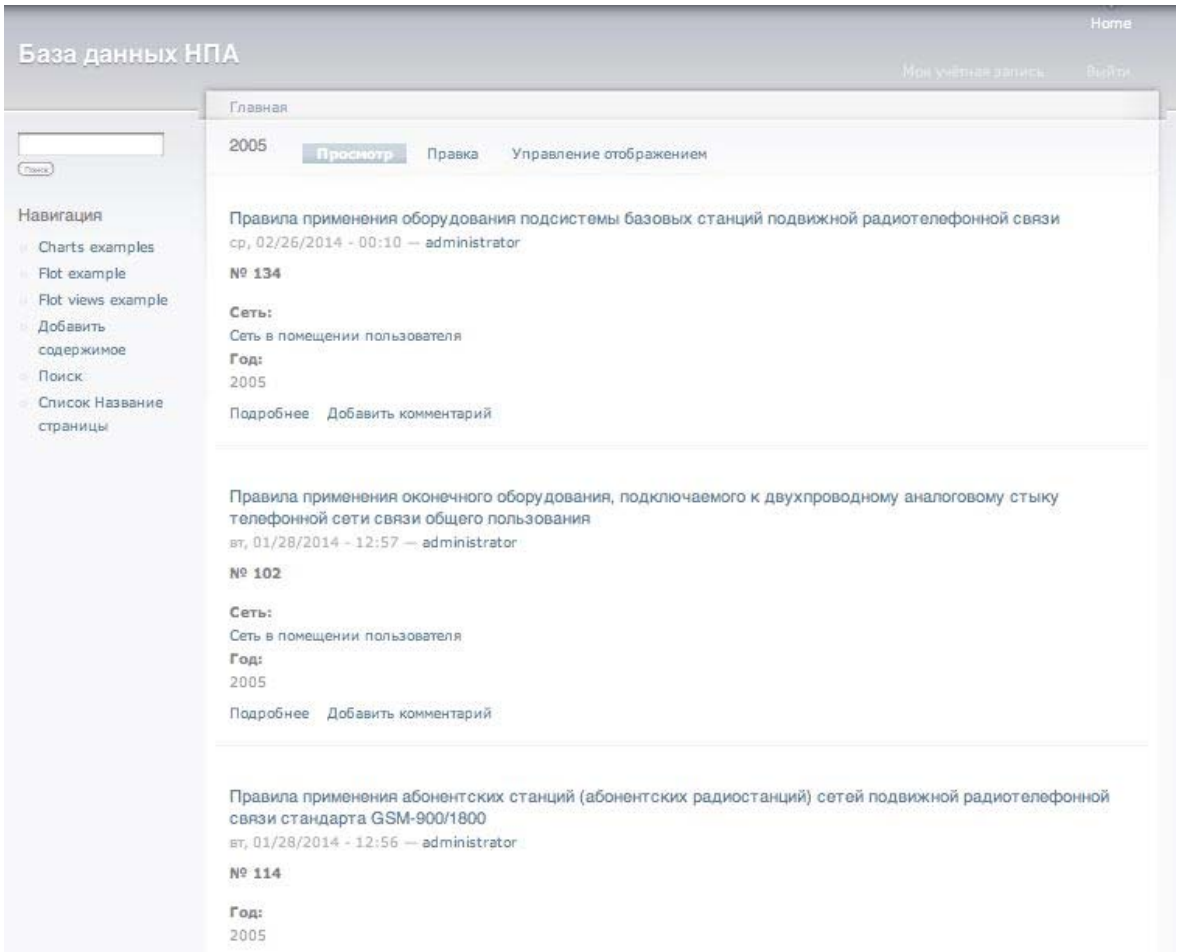


Рис. 9. База данных НПА

Также, помимо полных текстов нормативных правовых актов с приложениями, планируется размещение результатов, включающих в себя различные количественно-качественные диаграммы, анализ и выводы, полученные в данном и следующих исследованиях.

Всё это может быть использовано для проведения процедур подтверждения соответствия испытательными центрами и лабораториями, для прогнозирования, связанного с анализом рынка и его тенденций, а также для процесса обучения. На основании полученных планируется создать курс лабораторных работ, направленный на обеспечение студентами необходимых знаний в области подтверждения соответствия средств связи РФ и на ознакомление их с устройством, структурой и основными методами управления базами данных.

Библиографический список

1. **Федеральный закон** от 7 июля 2003 г. № 126 ФЗ «О связи».

2. **Юрасова, Л. В.** Проблемы разработки нормативных правовых актов по вопросам применения средств связи / Л. В. Юрасова, С. Ф. Кондрашов // Электросвязь. – 2007. – № 3.

3. **Духовницкий, О. Г.** Развитие подтверждения соответствия средств связи в Российской Федерации / О. Г. Духовницкий. // Электросвязь. – 2013. – № 9.

4. **Гойхман, В. Ю.** Процедура подтверждения соответствия оборудования корпоративных сетей / В. Ю. Гойхман // CIO. – 2008. – № 8.

5. **База данных НПА** [Электронный ресурс]. – Режим доступа: http://npa.sotsbi.ru.

Аннотация

В ходе данного исследования проанализирован весь объем существующих на сегодняшний день нормативных правовых актов. Произведена выборка и классификация НПА по различным критериям: год выпуска; сеть, к которой принадлежит оборудование, указанное в НПА; процедура подтверждения соответствия; характеристики и др. Все полученные результаты проанализированы, по ним сделаны соответствующие выводы. Тексты всех НПА, а также вся полученная в ходе исследования информация категоризирована и представлена в базе данных НПА.

V. Goikhman, E. Kovalenko

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

CHRONOLOGICAL ANALYSIS OF NORMATIVE LEGAL ACT IN CERTIFICATION SYSTEM COMMUNICATION WITH THE IDENTIFICATION AND CATEGORIZATION NETWORKS ELEMENTS AND CHARACTERISTICS

Annotation

The study analyzed all normative legal acts. Allocated normative legal acts and network elements according to the criteria: the year, the network, the procedure confirmation of compliance, characteristics, etc. All results were analyzed and conclusions are made. The texts of all normative legal acts and all information studies, recorded in the database.

Keywords: normative legal act, certification, declaration, network element, technology.

References

1. **Federal'nyj** zakon ot 7 ijulja 2003 g. № 126 FZ «O svjazi».

2. **Yurasova, L. V.** Issues of working out legal regulations for communications facilities' application / L. V. Yurasova, S. F. Kondrashov // Electrosvyaz. – 2007. – № 3.

3. **Dukhovnitsky, O. G.** Improvement of communication means' proof-of-compliance system in the Russian Federation / O. G. Dukhovnitsky // Electrosvyaz. – 2013. – № 9.

4. **Goikhman, V. Ju.** Conformation of compliance procedure equipment corporate networks / V. Ju. Goikhman // CIO. – 2008. – № 8.

5. **Baza dannyh NPA** [Electronic resource]. – Access mode: http://npa.sotsbi.ru.

Гойхман Вадим Юрьевич – кандидат технических наук, доцент кафедры инфокоммуникационных систем Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», vg@sotsbi.ru

Коваленко Екатерина Алексеевна – инженер испытательной лаборатории систем коммутации следующего поколения систем Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», kovalenko1101@gmail.com

UDK 338.516:339.132

S. Dotsenko, T. Popovich, A. Vladyko

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

A. Makshanov

St. Petersburg Institute for Informatics and Automation of RAS

APPLICATION OF AGGREGATED INDICES RANDOMIZATION METHOD FOR PROGNOSING THE CONSUMER DEMAND ON FEATURES OF MOBILE NAVIGATION APPLICATIONS

mobile navigation application, NNN-information, expert evaluation.

Introduction

One of the most relevant products on navigation market are mobile applications [8]. The market is full of vast selection of various navigating applications by different developers for any sort of devices [2]. Yet mobile apps producers are mostly focused on development aspect of their product [4, 6, 7]. Many articles dealing with app development pay much more attention to the technical side of the process [9–11], rather than exploring what features of the popular products make them market-leaders. In our paper we focus on the matter of developing of new mobile navigation application, competitive and able to satisfy a growing consumer demand, based on the analysis of distinctive features of existing successful products.

Research problem

Considering the fact that navigation application market is already quite full [3, 5], in order to successfully win over the market niche for a new application, the idea behind new GIS navigation product should be to satisfy more vast and sophisticated set of consumer needs than building a shortest rout from A to B. We shall use the aggregated indices randomization method to make the closest to accurate prediction about the short-term future needs of the consumers. We shall analyse the number of most popular navigation apps existing (see part IV), and single out the most distinctive features of each product. Then, according to the method given in part III, using the “expert data”, we shall range the features according to their “relevance”. Thus yielding the set of features our future product ought to possess in order to be commercially successful.

Method

In this project we regard the stage of designing features our product shall hold. The method we use is based on the Bayesian model of uncertainty randomization [1]. Additional non-numeric, non-exact, and non-complete expert knowledge (NNN-knowledge, NNN-information) is used for final estimation of the alternatives' probabilities.

General scheme of the method [1]:

Consider at a present time-point t_1 a complex system, which can proceed to one of the finite number of alternatives $A_1,...,A_r$ at a future time-point t_2. Suppose that a decision maker has m different sources of information (experts) about probabilities $p_i = P(A_i), i = 1,...,r, p_i \geq 0, p_1 + ... + p_r = 1$ of the system transition into alternative states $A_1,...,A_r$ at the time-point t_2. The decision maker obtains NNN-knowledge I_j from "experts", which can be presented as a vector $I = (I_1,...,I_m)$ that consists of systems of equalities and inequalities for probabilities $p_1,...,p_r$. The decision maker has NNN-knowledge J about the comparative ''weights" of the sources of information. So, the whole NNN-knowledge constitutes vector $(I;J) = ((I_1,...,I_m);J)$ $(I;J) = ((I_1,...,I_m);J)$, where I_j, is information obtained from jth source, and system J is NNN-knowledge that expresses preferences of the decision maker about the comparative significance of sources of information. If we take into account information I_j, we can form a set $P(r;I_j)$ of all admissible (according to information I_j), probability vectors $p = (p_1,...,p_r)$. Modelling uncertain choice of vector $p = (p_1,...,p_r)$ from the set $P(r;I_j)$ by a random choice, we obtain random probability vector $\tilde{p}_1(I_j) + ... + \tilde{p}_r(I_j) = 1$ $\tilde{p}(I_j) = (\tilde{p}_1(I_j),...,\tilde{p}_r(I_j)), \tilde{p}_i(I_j) \geq 0,$ which has uniform distributionon set $P(r;I_j)$. Component $\tilde{p}_i(I_j)$ of random vector $\tilde{p}_i(I_j)$ represents random estimation of probability of alternative A_i according to information I_j, obtained from jth source. Vector of mathematical expectations $\overline{p}(I_j) = (\overline{p}_1(I_j),...,\overline{p}_r(I_j))$ we will interpret as numerical image of NNN-information I_j. In other words, vector $\tilde{p}_i(I_j)$ is a result of information I_j quantification. In these terms random vector $\tilde{p}_i(I_j)$ is a stochastic quantification of NNN-information I_j.

Implementation

For designing our application using method above, we analyse most popular navigation products of the competitors.

Top apps for Android:

1. Google Maps [12]

The app allows you to see your location on a map, even if you don't have GPS, load offline maps, shows traffic, brows for local places of interest and rate and review them, can get you routes and schedules to travel via subway, bus, bike, or on foot and provides street view imagery, indoor maps, and 3D maps and etc.

2. Navfree [13]

Allows instant rooting and offline maps, option of viewing the map in 2D, 3D or a safety screen, automatic switching to Day & Night maps, browsing for POI, provides in-app purchasing of additional options (safety camera data, live parking information) and etc.

3. TomTom [14]

This app supplies offline maps, stored on your phone, and free lifetime maps, biggest database of real travel time, spoken instructions include street names, supports multitasking capability, 2D and 3D view, browsing for POI, provides lane guidance and in-app purchasing of additional options (speed cameras location, live traffic) and etc.

4 Sygic [15]

Provides up-to-date reports on traffic jams, road works and incidents, shows speed limit, current speed and speed cameras.

5. Waze [16]

Is a community-based traffic and navigation app (drivers in your area share real-time traffic and road information). Provides alerts before you approach police, accidents, road hazards or traffic jams, gas prices. Coordinates with Facebook and provides information about your friends vehicles, helps coordinate arrival time.

After analyzing and comparing the market leading products, we compile the list of features necessary for any future competitive app.

Our next step is contemplating which options existing in competitors' products are most significant for the future app.

We consult several groups of “experts” to range the features according to their relevance.

The NNN-information one group provides as an example:

Street view representation:

$$2D\ street\ view \geq 3D\ street\ view > Imagery\ street\ view$$

According to the method above, numeralization of experts' estimations looks as follows (Table 1).

TABLE 1. Distribution Estimations

	2D street view	3D street view	Imagery street view
Means	0,5345	0,3103	0,1552
Dispersions	0,0209	0,0278	0,0209
Correlation matrix	1,0000	0,5000	0,3333
	0,5000	1,0000	0,6667
	0,3333	0,6667	1,0000
Covariance matrix	0,0209	0,0139	0,0070
	0,0139	0,0278	0,0139
	0,0070	0,0139	0,0209

Suppose, we have our experts divided into three groups according to the level of trust we hold in them.

$$w(1), w(2), w(3); w(2) \geq w(3) > w(1)$$

Numeralization of expert groups are presented in Table 2.

TABLE 2. Distribution Estimations

	First group	Second group	Third group
Means	0,1452	0,5000	0,3548
Dispersions	0,0183	0,0183	0,0243
Correlation matrix	1,0000	0,3333	0,5000
	0,3333	1,0000	0,5000
	0,5000	0,5000	1,0000
Covariance matrix	0,0183	0,0061	0,0122
	0,0061	0,0183	0,0122
	0,0122	0,0122	0,0243

We execute a correction of our earlier estimation of means of distribution in accordance with the ranking of our experts (Table 3).

TABLE 3. Resulting Estimations

	2D street view	3D street view	Imagery street view
Means	0,5122	0,1792	0,3086
Dispersions	0,0397	0,0135	0,0194
Correlation matrix	0,0397	0,0159	0,0221
	0,0159	0,0135	0,0119
	0,0221	0,0119	0,0194
Covariance matrix	1,0000	1,1771	1,1366
	1,1771	1,0000	0,6096
	1,1366	0,6096	1,0000

Executing our method yields list of results as follows:

Street view representation:

1. 2D street view,
2. Imagery street view,
3. 3D street view.

These are some of the qualities, ranked by preference, that, according to our “experts”, can guarantee the profitability of future navigation application. This set was selected and sorted by relevance by using experts' NNN-information and applying aggregated indices randomization method.

Conclusion

Aggregated indices randomization method has shown accurate and consistent results. By using it it is possible to distinguish quite successfully between a number of similar alternatives. Yet the main imperfection of this method is that we wholly on our chosen experts and their opinion. Thus for this method to be consistent the chosen experts have to be highly qualified in the field of sturdy.

References

1. **Hovanov, N.** Multicriteria estimation of probabilities on basis of expert non-numeric, non-exact and non-complete knowledge / N. Hovanov,

M. Yudaeva, K. Hovanov // European Journal of Operational Research. – 2009. – Vol. 195, Issue 3. – PP. 857–863.

2. **Brown, A. D.** The best GPS App for Android OS Phones [Electronic resource] / A. D. Brown. – June, 2012. – Access mode: http://www.brighthand.com/default.asp?newsID=18949&news=Android+Apps+GPS+Navigation

3. **Crovitz, L. G.** Disruption Is the New Normal [Electronic resource] / L. G. Crovitz. – January, 2014. – Access mode: http://online.wsj.com/news/articles/SB10001424052702303370904579300482080488054

4. **Donovan, F.** Enterprise mobility fuels demand for mobile app development platform vendors [Electronic resource] / F. Donovan November, 2013. – Access mode: http://www.fiercemobileit.com/story/enterprise-mobility-fuels-demand-mobile-app-development-platform-vendors/2013-11-15

5. **Drege, S.** Mobile apps revenues tipped to reach $26bn in 2013 [Electronic resource] / S. DREGE. – Access mode: http://www.theguardian.com/technology/appsblog/2013/sep/19/gartner-mobile-apps-revenues-report

6. **James, J.** Analysis of mobile development approaches [Electronic resource] / J. James August, 2011. – Access mode: http://www.techrepublic.com/blog/software-engineer/analysis-of-mobile-development-approaches/4224/

7. **Kolodny, l.** Telenav Acquires Mapping Startup Skobbler for $24 Million [Electronic resource] / l. Kolodny. – January, 2014. – Access mode: http://online.wsj.com/news/articles/SB10001424052702303743604579353154250725732

8. **Leber, J.** A Shrinking Garmin Navigates the Smartphone Storm [Electronic resource] / J. Leber. – March, 2013. – Access mode: http://www.technologyreview.com/news/511786/a-shrinking-garmin-navigates-the-smartphone-storm/

9. **McMahan, T.** The Ins and Outs of Mobile Apps [Electronic resource] / T. McMahan. – June, 2011. – Access mode: http://online.wsj.com/news/articles/SB10001424052748704570704576275132869170342?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052748704570704576275132869170342.html

10. **Vyas, R.** Mobile Application Development Guidelines [Electronic resource] / R. Vyas. – November, 2013. – Access mode: http://www.hitechito.com/blog/mobile-application-development-guidelines.php

11. **Wayner, P.** 13 essential programming tools for the mobile Web [Electronic resource] / P. Wayner. – June, 2011. – Access mode: http://www.infoworld.com/d/mobile-technology/13-essential-programming-tools-the-mobile-web-246

12. **Features** in Google Maps Android Version 6.14.4 & below [Electronic resource]. – Access mode: https://support.google.com/gmm/answer/1645766?hl=en

13. **GPS** Satnav Features [Electronic resource]. – Access mode: http://www.navmii.com/GPSNavigation/Features

14. **Sygic** GPS Navigation [Electronic resource]. – Access mode: http://www.sygic.com/en/gps-navigation

15. **TomTom** app for Android [Electronic resource]. – Access mode: http://www.tomtom.com/en_gb/products/your-drive/smartphone-navigation/android/tomtom-navigation-for-android/index.jsp

16. **WAZE.** Outsmarting traffic, together [Electronic resource]. – Access mode: https://www.waze.com/

Annotation

The issue of this paper is to implement aggregated indices randomization method for prognosing the consumer demand on features of mobile navigation applications. Modern consumers are eager for the applications to provide them with more vast and sophisticated set of options than just building a shortest rout from A to B. Our goal is to analyse and compare the market leading navigating products and to compile the number of necessary and useful features the future product ought to possess for it to be competitive and profitable. After we examined a set of competing products we distinguish the most popular properties they possess. Using the «NNN-information» from several groups of experts, we then range this properties according to their «value» to the predicted success of future application.

С. М. Доценко, Т. В. Попович, А. Г. Владыко

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

А. В. Макшанов

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ПРИМЕНЕНИЕ МЕТОДА РАНДОМИЗИРОВАННЫХ СВОДНЫХ ПОКАЗАТЕЛЕЙ ДЛЯ ПРОГНОЗИРОВАНИЯ СПРОСА НА ФУНКЦИИ МОБИЛЬНЫХ НАВИГАТОРОВ

Аннотация

Темой данной работы является применение метода рандомизированных сводных показателей для прогнозирования спроса потребителей на функции мобильных навигаторов. Современные потребители ожидают от приложений более разнообразных наборов функций, нежели простое построение кратчайшего пути из точки А в точку В. Целью данной работы является проанализировать и сравнить ведущие

12. **Features** in Google Maps Android Version 6.14.4 & below [Electronic resource]. – Access mode: https://support.google.com/gmm/answer/1645766?hl=en

13. **GPS** Satnav Features [Electronic resource]. – Access mode: http://www.navmii.com/GPSNavigation/Features

14. **Sygic** GPS Navigation [Electronic resource]. – Access mode: http://www.sygic.com/en/gps-navigation

15. **TomTom** app for Android [Electronic resource]. – Access mode: http://www.tomtom.com/en_gb/products/your-drive/smartphone-navigation/android/tomtom-navigation-for-android/index.jsp

16. **WAZE.** Outsmarting traffic, together [Electronic resource]. – Access mode: https://www.waze.com/

Annotation

The issue of this paper is to implement aggregated indices randomization method for prognosing the consumer demand on features of mobile navigation applications. Modern consumers are eager for the applications to provide them with more vast and sophisticated set of options than just building a shortest rout from A to B. Our goal is to analyse and compare the market leading navigating products and to compile the number of necessary and useful features the future product ought to possess for it to be competitive and profitable. After we examined a set of competing products we distinguish the most popular properties they possess. Using the «NNN-information» from several groups of experts, we then range this properties according to their «value» to the predicted success of future application.

С. М. Доценко, Т. В. Попович, А. Г. Владыко

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

А. В. Макшанов

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ПРИМЕНЕНИЕ МЕТОДА РАНДОМИЗИРОВАННЫХ СВОДНЫХ ПОКАЗАТЕЛЕЙ ДЛЯ ПРОГНОЗИРОВАНИЯ СПРОСА НА ФУНКЦИИ МОБИЛЬНЫХ НАВИГАТОРОВ

Аннотация

Темой данной работы является применение метода рандомизированных сводных показателей для прогнозирования спроса потребителей на функции мобильных навигаторов. Современные потребители ожидают от приложений более разнообразных наборов функций, нежели простое построение кратчайшего пути из точки

А в точку В. В статье проанализированы и сравнены ведущие на рынке навигационные продукты и составлен набор необходимых и полезных свойств, которым должен обладать разрабатываемый продукт, чтобы быть конкурентоспособным и рентабельным. После рассмотрения ряда конкурирующих продуктов, выделяются наиболее популярные свойства, которыми они обладают. Используя «ННН-информацию» от нескольких групп экспертов, эти свойства ранжируются в соответствии с их «ценностью» для прогнозируемого успеха будущего приложения.

Ключевые слова: мобильные навигационные приложения, ННН-информация, экспертное оценивание.

Доценко Сергей Михайлович – доктор технических наук, профессор, проректор по научной работе Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

Владыко Андрей Геннадьевич – кандидат технических наук, начальник Управления организации научной работы и подготовки научных кадров Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

Попович Татьяна Владимировна – аспирантка, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», popovich-tatiana@yandex.ru

Макшанов Андрей Владимирович – доктор технических наук, профессор, ведущий научный сотрудник Федерального государственного бюджетного учреждения науки «Санкт-Петербургский институт информатики и автоматизации Российской академии наук», makshanov@oogis.ru.

country is now faced with the need to establish mechanisms for the protection and defense of these information and telecommunication its public bodies, authorities and threats related to computer systems infrastructure.

For this reason the state has decided to strengthen its capacity in safety through the creation of a strategic committee of safety information and the general direction of the security of information systems as systems Decree № 2-11-508 in 21 September 2011....

The strategic priorities are:

- Evaluation of risks to vital information systems within government, public agencies and infrastructure;
- The protection and defense of public administration information systems, public agencies and vital infrastructure;
- Strengthening the foundations of security: legal, education, training and research and development;
- The promotion and development of national and international cooperation.

For this purpose, a survey conducted by the Ministry of new technologies on a sample comprising fifty Moroccan organizations in different tissues resulted the following:

- The interest for the development of information technology: 95 % of organizations use the Internet and their websites can be considered a potential impact on the image of their organizations;
- The expectations of those bodies in relation to the future national strategy exceed more than 80 % favorable opinion.

To establish Morocco among the countries in these dynamic emerging information technologies Morocco launched in 2009 and Morocco in 2013 Numeric strategy to retain the trust and therefore the digital cyber security accompanying measure to the anchor of Morocco the digital economy. For this it is necessary to provide adequate human dimensions, legal, economic and technological responses security needs of digital infrastructures and users to generate economic development in all sectors of society.

I. *Preparing a strategy for the security of information systems in Morocco:*

To develop an approach to cybersecurity accordance with the guidelines of the International Telecommunication Union, it is important to correctly identify the values and assets to be protected in order to define the security perimeter set up. This requires a global, multidisciplinary and systemic approach to security.

Cybersecurity must understand in a comprehensive manner because it is not enough to protect the information during transfer but also when they are processed and stored. Security solutions to technological only cannot compensate for a lack of consistent and rigorous management needs, measures, procedures and security tools.

The definition of a strategy for security of information systems through:

- Consideration of risk analysis to cyberspace in a dynamic and continuous process to guide the approach recommended safety;
- Defining a Security Policy for Information Systems (PSSI) to translate the understanding of risks and their impacts on security measures to be implemented;
- The deployment of solutions able to secure computer systems and telecommunications infrastructure;
- The establishment of a process of detection and response to threats.
- The establishment of an appropriate legal framework;
- The encouragement of research and development in the field of IT security and the obligation of compliance with minimum standards;
- Awareness of all stakeholders to promote a culture of cybersecurity.

II. *Strategic priorities*:

In this context and in response to the urgent need for a clear strategy for cybersecurity four strategic areas have been identified, namely:

- Assessment of risks to information systems within administration information systems, public agency and vital infrastructure;
- The protection and defense of public administration information systems, public agencies and vital infrastructure;
- Strengthening the foundations of security: Legal, Advocacy, Training and Research & Development;
- The promotion and development of national and international cooperation.

To assess the risks to information systems and before putting in place preventive safety measures must conduct a risk analysis to estimate potential losses related to a failure of availability , integrity or yet data confidentiality without losing sight that the main impact is often the loss of reputation and trust in the entity. So the consistent implementation and effective security systems within the state requires the adoption of risk analysis , policies and security standards, consistent and appropriate to the context methods. The organizational security measures and techniques described in these policies and standards must be applied by different authorities, public administration and vital infrastructure.

Risk assessment is a prerequisite for the development of guidelines and the definition of the axes of efforts to help managers at all levels to protect their information systems.

This axis will be implemented in two programs:

➢ Develop plans for assessing risks and threats:

- Define a grid for assessing the degree of criticality of SI administrations, public organism and vital infrastructure;

- Identify, classify and identify SI administrations , public organizations and vital infrastructure;
- Periodically assess the level of risk to the SI administrations , public organizations and vital infrastructure;
- Assess risk management plans adopted by governments, government agencies and vital infrastructure;
- Identify SI administrations and public organizations to be supervised by the maCERT (Moroccan intelligence center, detection and response to cyber-attacks).

➢ Develop tools to support decision making:

- Conduct surveys to collect technical and procedural related to IT security legal orders data;
- Produce statistical data and monitoring indicators;
- Ensure technological, legal and regulatory.

For the protection and defense of public administration information systems, public agencies and vital infrastructure. Information systems require tangible and intangible protection against all types of threats. However, it is based on the observation that no information system, regardless of its level of protection is not completely secure. Therefore, it is necessary to have sufficient capacity to detect intrusions and to respond in the event of incident detection, to deal effectively and quickly restore the operability of systems affected.

This axis will be implemented in three programs:

➢ Development of benchmarks and national standards:

- Identify standards and best security practices information technology;
- Define Policy Security Information Systems (PSSI) national benefit of administrations, public organizations and vital infrastructure;
- Develop guidelines and standards for implementing security policies of specific information systems.

➢ Strengthen IT security administrations, public institutions and infrastructure of vital importance:

- Ensure the implementation of the ISSP;
- Study the feasibility and initiate the gradual establishment of a network of inter secure transmission;
- Involve operators and Internet service providers in the security of information systems;
- Encourage governments, government agencies and infrastructure vital to be audited to be certified ISO 27001 or equivalent.

➢ Strengthening structures for monitoring, detection and response to cyber incidents:

- Strengthen the capacity of maCERT to provide key services and integrate the many stakeholders in accordance with international standards;
- Encourage governments, public organizations infrastructure of vital importance in terms of the scope of their SI to have focal points or to set up centers of Operational Security of Information Systems;
- Formalize and implement mechanisms for the exchange of information relating to the processing of alerts and incidents between maCERT and stakeholders.

For strengthening the foundations of security: Legal, Awareness, Training, and Research & Development, it is therefore important to regularly check whether the existing legal bases are still appropriate. The need for legal monitoring result, moreover, the trans boundary nature of the crime which undermines, to some extent, the principle of the territorial application of the rules Disclaimer. It is also important to develop education programs and specific training in IT security. Managers should be able to acquire the skills necessary to participate actively in understanding and solving cyber threats.

Research and development must provide acceptable autonomy and contribute to an in-depth security information systems. In this wake, the technology forefront and whose control is crucial rest those operating systems and cryptography.

This axis will be implemented in four programs:

➢ Strengthen the legal framework to create digital trust:

- Upgrade the legal and regulatory framework to take into account the specific requirements of the IT security including those relating to the provision of electronic certification and cryptography;
- Consider recommendations from regional and international institutions for possible application in the national regulations.

➢ Identify and organize training programs for technical and legal issues posed by cybersecurity:

- Define Profiles adequate competence in the field of cybersecurity;
- Stop training programs in cybersecurity and ensure their implementation;
- Promote the development and distribution of educational materials.

➢ Awareness on cyber ethics and the threats and risks to the security of information systems:

- Implement programs to raise awareness of security of information systems;
- Educate the population including children and individual users on cyber ethics and the threats and risks to the security of information systems.

➢ Support research and development of products for the security of national information systems to ensure the scientific and technical autonomy:

- Encourage the development of national solutions in the field of computer security;
- Identify academic research in the field of security of information systems and monitor their evolution;
- Identify national and international experts who could assist to solve problems cyber security.

For the promotion and development of national and international cooperation. The need for cooperation either on the national or international level due to the global nature essence of communication networks. At the national level, cooperation and effective interaction between all stakeholders is necessary to have a coherent strategy.

At the international level, the dialogue on cybersecurity should promote the exchange of experience, identification and application of rules and compatible standards.

This axis will be implemented in two programs:

➢ Identify themes and cooperation mechanisms:
- Identify programs and areas of cooperation;
- Explore opportunities for cooperation with academia, regulators, private sector, etc. . . ;
- Identify and establish mechanisms and modalities of cooperation.

➢ Develop partnerships and implement:
- Develop partnerships with stakeholders identified in the field of security of information systems;
- Implement and evaluate programs of cooperation.

This strategy sets out the broad lines of the programs and projects that will be launched. It will be broken down into operational action plans. These plans must describe the program for each concrete implementation according to a determined while specifying the actors to contribute to their achievement by quantified objectives schedule measures.

To create favorable conditions for the implementation of operational action plans conditions, involved in the development of the National Cyber Security Strategy will be involved in the definition of these plans while paying special attention to their needs, priorities and constraints.

This strategy will be periodically revised to be adapted, where necessary, new realities and requirements.

Annotation

This article describes the strategic directions of the state in terms of the security of information systems for the protection of information, integrity and continuity of the operation of information systems vital infrastructure following a training seminar organized by the Administration of National Defence 16 to 19 September 2013 for the benefit of those responsible for the security of information

Ахмаммуш Файза

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

СТРАТЕГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ МАРОККО

Аннотация

В этой статье описаны стратегические направления государственной политики Марокко в области безопасности информационных систем, защиты информации, целостности и устойчивости критически важных объектов инфраструктуры, рассмотренные на семинаре, организованном Администрацией Национальной Обороны в период с 16 по 19 сентября 2013 года в интересах лиц, ответственных за безопасность информации.

Ключевые слова: безопасность в киберпространстве, политика безопасности информационных систем, стандарты, «цифровое» Марокко, «Марокканский» CERT, цифровое доверие.

Ахмаммуш Файза – аспирантка кафедры защищённых сетей связи Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», fahmammouch@hotmail.fr

УДК 004.6:004.94

И. Д. Летенко, Е. М. Герасимова

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

НЕЧЕТКАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ К РЕСУРСАМ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ НА ОСНОВЕ ОЦЕНКИ РИСКОВ

хранение данных, управление доступом, оценка риска, программно-конфигурируемые сети.

Введение

Программно-конфигурируемые сети (ПКС) отличаются от традиционных сетевых инфраструктур за счет существенного переосмысления отношений между уровнем данных и уровнем управления сетевого устройства. Наиболее распространенным протоколом для ПКС сейчас является протокол OpenFlow (OF). Для современных сетей, в которых всё чаще встают задачи виртуализации и динамического переноса сетевых приложений, протокол OpenFlow может предложить гибкость, необходимую для динамического сетевого администрирования, выходящего за рамки традиционных сетей. В OpenFlow правила потока определяют базовые инструкции, которые регулируют, пересылку, изменение или удаление каждого пакета, который попадает в OF-коммутатор. Уровень управления в коммутаторе упрощен, коммутатор только передает статистику и обращается за новыми правилами потоков к внешнему OpenFlow контроллеру.

В иерархии OpenFlow контроллер находится выше OF-коммутаторов, обычно реализуемых на более дешевом оборудовании. Контроллер содержит логику определения, обновления и адаптации правил потоков. Контроллер может взаимодействовать с несколькими коммутаторами одновременно, он может распределить набор согласованных правил потоков через коммутаторы для прямой маршрутизации или оптимизировать туннелирование, что позволяет значительно повысить эффективность транспортных потоков. Контроллер также предоставляет программный интерфейс (API), позволяющий разрабатывать OpenFlow приложения, которые реализуют логику, необходимую, чтобы сформулировать правила потоков. Протокол OpenFlow предлагает для исследователей беспрецедентный контроль над сетью и определяет единую точ-

ку управления маршрутизацией потоков данных для множества коммутаторов в сети.

OpenFlow приложения могут реализовывать сложную логику различных состояний потоков, например, для обеспечения комплекса карантинных процедур, или перенаправления рискованных сетевых потоков для их специализированной обработки.

Актуальные вопросы управления доступом к данным

Новые возможности программно-конфигурируемых сетей открывают пути решения актуальных проблем управления доступом к данным, решение которых было крайне затруднительно в сетях с традиционной архитектурой.

Необходимость в динамическом управлении правами доступа к данным и ресурсам сети

К современным сетям подключается множество разнородных пользователей и часто возникают события, когда необходимо динамически изменить права доступа к данным и ресурсам сети, в ответ на эти события. Например, ситуация когда файрвол обнаруживает, что хост заражен вирусом; если это компьютер «гостя» то его можно просто заблокировать, однако если это компьютер директора то требуются другие более гибкие решения.

Реализация сложных сценариев требует частого изменения низкоуровневых параметров сети

В сети предприятия постоянно регистрируются «гости», которым нужен доступ к определенным ресурсам, или сотрудники могут использовать несколько устройств (ноутбук, планшет, смартфон), перемещаться по предприятию, запрашивать различные ресурсы сети, например для выполнения срочных поручений, всё это значительно усложняет управление сетью и требует постоянного изменения низкоуровневых конфигураций.

Организация хранения и доступа к данным для множества владельцев и пользователей

Наиболее экономически выгодный и гибкий способ хранения большого объема данных это облачные хранилища. Требуется обеспечить надежный и эффективный механизм хранения, доступа и управления данными в сети. Основными сложностями в данной области является то, что имеется множество владельцев данных (ресурсов) и множество пользователей, которые должны иметь различные права доступа и быть надежно изолированы друг от друга, а так же то, что данные физически распределены.

Модели доступа и хранения данных

В последнее время как ответ на необходимость динамической адаптации политик доступа в зависимости от эксплуатационных нужд и текущей обстановки, появились модели управления доступом на основе оценки риска [1]. Несмотря на то, что подобные модели достаточно сложны с точки зрения большого числа правил и параметров, которые их определяют, гибкость программно-конфигурируемых сетей открывает возможности их практической реализации.

Предлагаемая в данной работе модель основывается на том, что в процессе принятии решений при управлении доступом есть некоторые степени неопределенности и риски и должна быть возможность адаптации к таким рискам. Рассматриваемая модель, позволяет разрешать рискованные потоки информации при условии, что риск может быть вычислен и контролируется, принцип пояснен на рисунке 1.

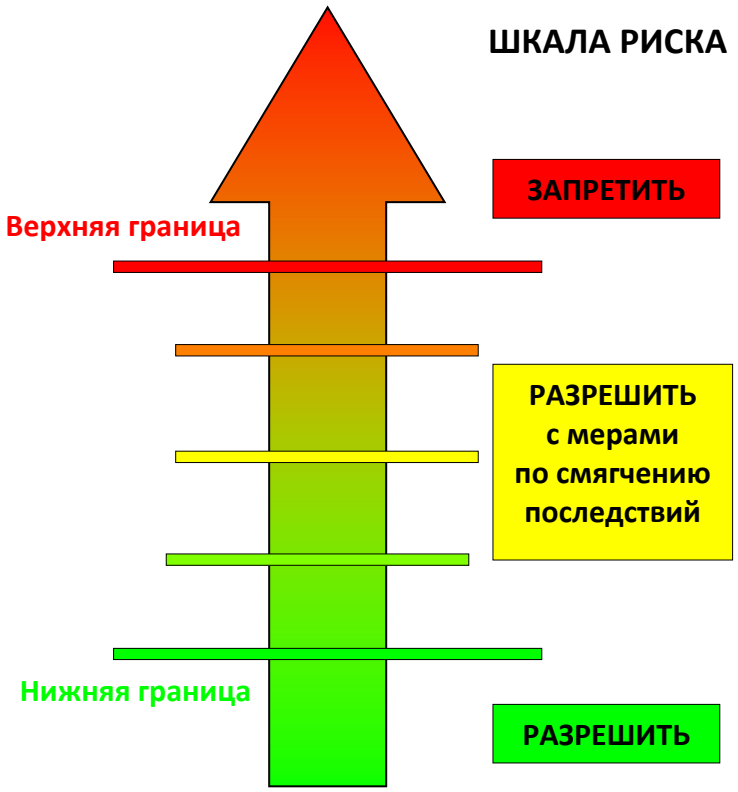


Рис. 1. Адаптивное управление доступом

Для хранения данных предлагается использовать шифрование на основе атрибутов, так как такой способ хранения данных хорошо отражает предложенную модель управления доступом на область данных [2]. Шифрование на основе атрибутов – это разновидность алгоритмов шифрования с открытым ключом, в которых закрытый ключ, применяемый пользователем для расшифрования данных, зависит от некоторых атри-

бутов пользователя (например, должности, места жительства, типа учетной записи).

В схеме шифрования участвуют владелец данных (передающий данные), пользователь (принимающий данные) и третья сторона (доверенный центр), чья роль заключается в том, чтобы генерировать ключи для шифрования и расширования данных владельцами данных и пользователями.

Ключи (в частности, открытый ключ и универсальный ключ) генерируются по установленному полному набору атрибутов. Если к системе присоединится пользователь с новым атрибутом, атрибут будет добавлен к набору, а открытый и универсальный ключи будут сгенерированы заново.

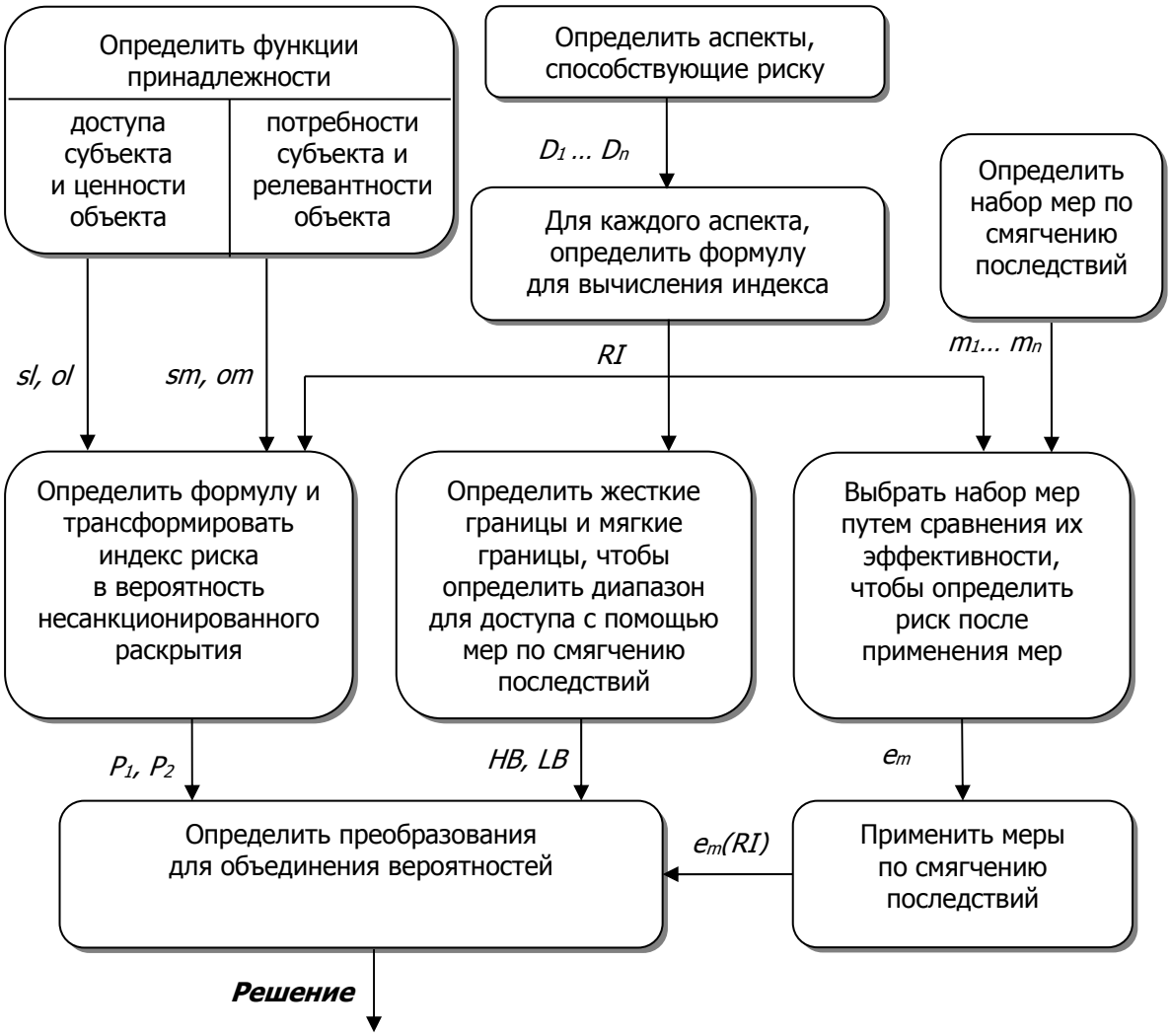
Владелец данных шифрует данные при помощи открытого ключа и некоторого набора атрибутов.

Пользователь может расшифровать данные при помощи собственного закрытого ключа, который он получает от доверенного центра. Проверяется соответствие между атрибутами, которые составляют закрытый ключ пользователя, и атрибутами зашифрованных данных.

Модель управления доступом на основе оценки риска

Основной аспект предлагаемой нечеткой модели это принятие решения управления доступом, основанные на восприятии уровня потенциального риска, связанного с запрошенным доступом [3]. Вместо обычного жесткого решения «разрешить» или «запретить», решения о предоставлении доступа от нечеткой модели будет «разрешить», «запретить», или «разрешить, но с определенными мерами снижения риска, которые будут приняты для ограничения доступа». Чем больше риск, тем больше мер по его смягчению нужно применить.

Рассмотрим метод аппроксимации риска и принятия решения о предоставлении доступа в соответствии с предложенной моделью, блок-схема которого изображена на рисунке 2.



$D_1 \dots D_n$ аспекты, способствующие риску
RI формула индекса риска
HB жесткие верхние и *LB* нижние границы (между fuzzy)
$m_1 \dots m_n$ комплекс мер для снижения риска
e_m эффективность мер
sl риск раскрытия информации субъектом, который характеризует его надежность (fuzzy)
ol уровень «чувствительности» объекта который указывает его ценность (fuzzy)
sm потребность субъекта в информации из категории
om соответствие (релевантность) объекта к категории
P_1 вероятность того, что субъект допустит утечку информации злонамеренно
P_2 вероятность случайного раскрытия, независимо от намерений субъекта

Рис. 2. Структурно-параметрическая модель

На основе экспертных оценок определяют исходные параметры для функционирования модели. Исходными данными являются: аспекты, влияющие на безопасность, функции принадлежности для субъектов и объектов, а так же меры по смягчению последствий.

На основе исходных данных для каждого параметра, способствующего риску, определяют формулу, которая вычисляет индексы риска

(*RI*), которые соизмеримы с интуицией (больший индекс указывает высокий шанс несанкционированного разглашения).

Например, определим формулу для вычисления индекса риска от уязвимости. Для информационного потока индекс риска от уровня уязвимости объекта к уровню доступа субъекта может быть определен так, что индекс увеличивается, когда увеличивается уровень уязвимости или когда уменьшается уровень доступа. Диапазон индекса риска $(0, +\infty)$. Индекс риска всегда больше нуля, чтобы отразить тот факт, что всегда есть определенный риск, каким бы малым он не был.

Роль индекса не ограничена тем, чтобы обеспечить более высокую точность определения уровня риска. Индексы риска относительны методам измерений риска. Чтобы сделать их полезными, они должны быть откалиброваны.

Для каждого аспекта, определяют другую формулу для преобразования индекса риска в вероятность несанкционированного разглашения. Формула должна быть монотонно возрастающей по отношению к индексу риска. Желательно, чтобы формула включала в себя настраиваемые параметры, так чтобы они могли быть доработаны для аппроксимации статистики или интуиции. Эта формула и калибровка отображает вероятностный процесс, который характеризует индекс риска в качестве входных данных и производит логический вывод, чтобы указать, происходит ли несанкционированное раскрытие.

Для индексов риска всех аспектов рассчитывают, жесткие верхние (*HB*) и нижние границы (*LB*), таким образом значения риска выше *HB* является неприемлемым, запрос на доступ будет отклонен; риск ниже *LB* является приемлемым. Значения в диапазоне от *HB* и *LB* являются элементом гибкости нечеткой модели.

Для каждого аспекта, определяют комплекс мер для снижения риска m и их эффективность e_m. Для оценки эффективности меры рассчитывают вероятность с учетом принятых мер как функцию от *RI*.

Для принятия решения определим преобразования, чтобы объединить вероятности для разных аспектов и параметров. На основе вычисленной объединенной вероятности вычислим риск. Предпочтительно, чтобы преобразования включали в себя настраиваемые параметры для более точной обработки в соответствии с реальной ситуацией. Более подробная информация о вероятности и математических преобразованиях приведена ниже.

Математический аппарат нечеткой многоуровневой модели

Многоуровневая мандатная модель [4] Белла-Ла Падула может быть представлена как оценка такой вероятности P от двух независимых вероятностей, P_1 и P_2, и комбинации их.

$$P_1 = \begin{cases} 0, & \text{уровень допуска объекта} \geq \text{уровня уязвимости субъекта} \\ 1, & \text{иначе} \end{cases}$$

$$P_2 = \begin{cases} 0, & \text{набор категорий объекта} \supseteq \text{набора категорий субъекта} \\ 1, & \text{иначе} \end{cases}$$

$$P = P_1 + P_2 - P_1 P_2.$$

Нечеткая модель определяет P_1 как вероятность того, что субъект (пользователь) допустит утечку информации злонамеренно и P_2 как вероятность случайного раскрытия, независимо от намерений субъекта. Модель оценивает P_1 и P_2, но они больше не являются жесткими. Таким образом, Нечеткая модель MLS определяет количество риска, который является проблемой простой модели Белла-Ла Падула; это свойство определяет, к чему субъект не может получить доступ, чтобы предотвратить неразрешенное разглашение информации субъектом.

Существуют различные подходы к количественной оценке рисков, релевантные для соответствующих областей применения.

Хотя есть много различных способов расчета P_1 и P_2, выберем сигмовидную функцию для того, чтобы провести параллель со ступенчатой функцией модели многоуровневого доступа.

P_1 определяется как:

$$P_1 = \frac{1}{1 + \exp((-k) \cdot (RI - mid))},$$

$$RI(sl, ol) = (a^{-(sl-ol)}) / (m - ol),$$

где, параметр *mid* является значением *RI* при $P_1 = 0{,}5$; параметр *k* определяет падение кривой P_1.

P_2 определяется через W_c – готовность принять раскрытие для категории *C*,

$$WI_c = (b^{-(om-sm)}) / (m_{\max} - sm),$$

$$W_c = \frac{1}{1 + \exp((-k') \cdot (WI_c - mid'))}.$$

Если P_c обозначает вероятность непреднамеренного раскрытия для категории *C*, то

$$P_2 = Maximum\ \{P_c(1 - W_c)\}.$$

Факторы, определяющие риск и меры по его снижению

Основные факторы, определяющие риск неправомерного использования информации, а так же факторы определяющие потребность субъекта (пользователя) в доступе к информации:

- степень доверия к пользователю (уровень допуска субъекта),
- ценность информации (секретность),
- роль пользователя, должность,
- критичность информации для роли,
- история доступа пользователя,
- наличие уязвимостей в системе (открытые порты, вирусы),
- текущая обстановка (ситуация).

Опишем общие меры по снижению риска [5]. Хотя набор мер для снижения риска сильно зависят от конкретной ситуации и сценария использования, некоторые подходы, которые могут быть применимы включают в себя:

- системы обнаружения и предотвращения вторжений (IDS / IPS): применение решений рассмотренных в [6] и [7] позволяет во многих случаях значительно снизить риск;
- ограничение скорости: ограничение скорости, с которой субъект может получать информацию для ограничения величины потенциальной утечки информации;
- ревизия во время и после доступа. Аудит может включать в себя: виды активности (деятельности субъекта), параметры и атрибуты этой деятельности, оценка временных параметров деятельности и т. д.;
- уменьшение прав доступа субъекта после доступа. Таким образом, доступ предоставляется разово, без возможности получить связанные материалы;
- уменьшение прав доступа субъекта после получения достаточно большого количества ценной информации. Это означает, что если субъект знает слишком много, то он становится потенциально слабой точкой и, следовательно, необходим более высокий уровень предосторожности.

Заключение

Таким образом, развитие программно-конфигурируемых сетей открывает возможности для эффективной реализации, основанной на оценке риска нечеткой модели управления доступом. Предложенное решение позволяет обеспечить надежный и эффективный механизм хранения, доступа и управления данными и ресурсами сети для множества пользователей в динамически меняющихся условиях.

Библиографический список

1. **Cheng, P. C.** Fuzzy multi-level security: An experiment on quantified risk-adaptive access control / P. C. Cheng et al. // Security and Privacy, 2007. SP'07. IEEE Symposium on. – IEEE, 2007. – PP. 222–230.

2. **Sahai, A.** Fuzzy identity-based encryption / A. Sahai, B. Waters // Advances in Cryptology–EUROCRYPT 2005. – Springer Berlin Heidelberg, 2005. – PP. 457–473.

3. **Буйневич, М. В.** Выбор рациональной системы экономических механизмов управления рисками в интересах обеспечения техногенной безопасности отрасли (региона) / М. В. Буйневич, А. Г. Владыко, Е. В. Радова // Проблемы управления рисками в техносфере. – 2012. – № 4 (24). – С. 77–83.

4. **Bell, D. E.** Secure computer system: Unified exposition and multics interpretation / D. E. Bell, L. J. La Padula. – MITRE CORP BEDFORD MA, 1976. – №. MTR-2997-REV-1.

5. **Пат. 8087090** США. Fuzzy multi-level security / Cheng P. C. et al. – 2011.

6. **Доценко, С. М.** Системы обнаружения вторжений на основе встраиваемых микропроцессорных систем / С. М. Доценко, А. Г. Владыко, И. Д. Летенко // Телекоммуникации. – 2013. – № S7. – С. 15–18.

7. **Пат.** на полезную модель Российской Федерации 133954, МПК U1 G06F21/00. Устройство защиты сети / Владыко А. Г., Летенко И. Д., Доценко С. М.; заявитель и патентообладатель Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича» (СПбГУТ). – № 2013120643/08 ; заявл. 29.04.2013 ; опубл. 27.10.2013, Бюл. № 30.

Аннотация

В данной работе исследуются актуальные вопросы управления доступом к ресурсам сети и хранения данных, кроме того рассмотрены новые возможности, связанные с развитием программно-конфигурируемых сетей. Предлагается нечеткая модель управления доступом к данным, основанная на оценке риска неправомерного использования информации. Приведен метод количественной оценки риска и рассмотрены факторы, определяющие риск и меры по его снижению.

I. Letenko, E. Gerasimova

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

FUZZY ACCESS CONTROL MODEL RESOURCES PROGRAM-CONFIGURABLE NETWORKS BASED ON RISK ASSESSMENT

Annotation

This paper examines current issues of access control to network recourses and data storage, also discusses the new opportunities arising from the development of software-defined networks. Fuzzy data access control model is proposed, which based on the risk estimation of information leakage. A method for quantitative risk assessment is proposed and examined the factors that determine the risk and mitigation measures.

Keywords: data storage, access control, risk assessment, software-defined networks.

References

1. **Cheng, P. C.** Fuzzy multi-level security: An experiment on quantified risk-adaptive access control / P. C. Cheng et al. // Security and Privacy, 2007. SP'07. IEEE Symposium on. – IEEE, 2007. – PP. 222–230.

2. **Sahai, A.** Fuzzy identity-based encryption / A. Sahai, B. Waters // Advances in Cryptology–EUROCRYPT 2005. – Springer Berlin Heidelberg, 2005. – PP. 457–473.

3. **Bujnevich, M. V.** Vybor racional'noj sistemy jekonomicheskih mehanizmov upravlenija riskami v interesah obespechenija tehnogennoj bezopasnosti otrasli (regiona) / M V. Bujnevich, A. G. Vladyko, E. V. Radova // Problemy upravlenija riskami v tehnosfere. – 2012. – № 4 (24). – S. 77–83.

4. **Bell, D. E.** Secure computer system: Unified exposition and multics interpretation / D. E. Bell, L. J. La Padula. – MITRE CORP BEDFORD MA, 1976. – №. MTR-2997-REV-1.

5. **Pat 8087090** SShA. Fuzzy multi-level security / Cheng P. C. et al. – 2011.

6. **Docenko, S. M.** Sistemy obnaruzhenija vtorzhenij na osnove vstraivaemyh mikroprocessornyh sistem / S. M. Docenko, A. G. Vladyko, I. D. Letenko // Telekommunikacii. – 2013. – № S7. – S. 15–18.

7. **Pat.** na poleznuju model' Rossijskoj Federacii 133954, MPK U1 G06F21/00. Ustrojstvo zashhity seti / Vladyko A. G., Letenko I. D., Docenko S. M.; zajavitel' i patentoobladatel' Federal'noe gosudar-stvennoe obrazovatel'noe bjudzhetnoe uchrezhdenie vysshego professio-nal'nogo obrazovanija «Sankt-Peterburgskij gosudarstvennyj universitet telekommunikacij im. prof. M. A. Bonch-Bruevicha» (SPbGUT). – № 2013120643/08 ; zajavl. 29.04.2013 ; opubl. 27.10.2013, Bjul. № 30.

Летенко Иван Дмитриевич – аспирант кафедры информатики и компьютерного дизайна Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», letenko@gmail.com

Герасимова Екатерина Михайловна – аспирантка кафедры информатики и компьютерного дизайна Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

УДК 004.491.22

С. И. Штеренберг, А. В. Красов

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

ВАРИАНТЫ ВЛОЖЕНИЯ ИНФОРМАЦИИ В ИСПОЛНИМЫЙ ФАЙЛ ФОРМАТА .Intel HEX

компьютерный вирус, язык Ассемблера, стеганография, контейнер, исполнимый файл, формат elf.

В современной компьютерной стеганографии существует два основных типа файлов: сообщение – файл, который предназначен для скрытия, и контейнер – файл, который может быть использован для скрытия в нём сообщения. При этом контейнеры бывают двух типов. Контейнер-оригинал (или «Пустой» контейнер) – это контейнер, который не содержит скрытой информации. Контейнер-результат (или «Заполненный» контейнер) – это контейнер, который содержит скрытую информацию. Под ключом понимается секретный элемент, который определяет порядок занесения сообщения в контейнер [1–20].

Основная проблема заключается в выполнении синхронизации, определении начала и конца последовательности. Если в данных контейнера существуют биты синхронизации, заголовки пакетов и т. д., то скрытая информация может следовать сразу же после них. Сложность организации синхронизации является преимуществом с точки зрения обеспечения скрытности передачи. Скрытие информации, которая преимущественно имеет большой объем, выдвигает существенные требования к контейнеру, размер которого должен, по меньшей мере, в несколько раз превышать размер встраиваемых данных. Во многих случаях также желательна устойчивость полученного стеганосообщения к искажениям (в том числе и злоумышленным). Для таких преобразований очень подходит исполнимый файл формата Intel HEX.

Intel HEX – формат файла, предназначенного для представления произвольных двоичных данных в текстовом виде. По историческим причинам является стандартом де-факто при прошивке разнообразных микросхем с памятью (микроконтроллеров, ПЗУ, EEPROM и т. п.). Соответственно большинство инструментов подготовки образов прошивки (компиляторы, редакторы и т. п.) умеют работать с этим форматом. Поскольку файл состоит из символов ASCII, а не двоичных кодов, появляется возможность хранить данные на бумаге, перфоленте или перфокартах, выводить их на терминал, принтер и т. д. Восьмибитовый HEX-

формат файлов предусматривает размещение данных и кода в 16-разрядном линейном адресном пространстве для 8-разрядных процессоров Intel. 16-разрядный HEX-формат файлов дополнительно позволяет использовать 20-разрядное сегментное пространство адресов 16-разрядных процессоров Intel. И, наконец, 32-разрядный формат позволяет оперировать линейным 32-разрядным адресным пространством 32-разрядных процессоров [21].

Шестнадцатиричное представление двоичных данных в виде ASCII требует использование двух символов для записи одного байта, при этом первый символ всегда соответствует старшей тетраде битов одного байта. Такой подход увеличивает количество символов вдвое по сравнению с количеством двоичных данных.

Формат файла организован в виде набора записей, содержащих сведения о типе, количестве данных, адрес их загрузки в память и дополнительные сведения. В настоящее время определены шесть различных типов записей, однако не все их комбинации определены для разных форматов данных.

Встречаются две модификации: intel-standart и intel-extended. Intel-standart поддерживает только 16 бит адрес (до 64 кБайт). Intel-extended имеет расширенный список типов записей и 32-бит адрес.

Достоинством формата является возможность указывать только определенные области адресов (с точностью до байта). Многие микроконтроллерные архитектуры имеют несколько областей программирования с обширными пустотами в адресации между ними.

Файл состоит из текстовых ASCII строк. Каждая строка представляет собой одну запись. Каждая запись начинается с двоеточия (:), после которого идет набор шестнадцатеричных цифр кратных байту:

Начало записи (0).

Количество байт данных, содержащихся в этой записи. Занимает один байт (две шестнадцатеричных цифры), что соответствует 0…255 в десятичной системе.

Начальный адрес блока записываемых данных – 2 байта. Этот адрес определяет абсолютное местоположение данных этой записи в двоичном файле.

Один байт, обозначающий тип записи. Определены следующие типы записей:

0 – запись содержит данные двоичного файла.

1 – запись обозначает конец файла, данных не содержит. Имеет характерный вид «:00000001FF».

2 – запись адреса сегмента.

4 – запись расширенного адреса.

Байты данных, которые требуется сохранить в EPROM (их число указывается в начале записи, от 0 до 255 байт).

Последний байт в записи является контрольной суммой. Рассчитывается так чтобы сумма всех байтов в записи была равна 0.

Строка заканчивается стандартной парой CR/LF (0Dh 0Ah) [22].

Файл формата Intel HEX может содержать записи для процессоров i8086, которые определяют адрес сегмента (иначе говоря — номер параграфа, один параграф – это 16 байт). Если используется директива H167, то этот тип записи заменяет запись расширенного линейного адреса. Номер параграфа используется как смещение адреса для всех записей данных, следующих за этой записью. Смещение представляет собой сдвиг адреса на четыре бита влево. Например, смещение равное 0x1234 даст реальный адрес 0x12340. Пример записи:

020000021000EC где:
02 Количество байт данных
0000 В этом типе записи всегда равно 0000
02 Тип записи 02 (запись адреса сегмента).
1000 Номер параграфа (реальный адрес будет равен 0x10000).
EC Контрольная сумма.

После успешной сборки проекта будет сгенерирован 16-тиричный файл FirstProject.hex, содержащий в символьном виде машинный код программы:

```
:020000020000FC
:100000001FC0FECFFDCFFCCFFBCFFACFF9CFF8CF8B
:10001000F7CFF6CFF5CFF4CFF3CFF2CFF1CFF0CFCC
:06002000EFCFEECFEDCFA3
:100040000FE50DBF04E00EBFC298BA9A04E018B3E2
:10005000102718BB01D0FBCFB3ECA0E51197F1F747
:02006000089501
:00000001FF
```

Сгенерирован 16-тиричный файл FirstProject.hex

Рассмотрим формат данных hex-файл на примере второй строки текста (маркером начала строки всегда является символ “:”):

```
NN AAAA CC DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD SS
: 10 0000 00 1FC0FECFFDCFFCCFFBCFFACFF9CFF8CF 8B
```

Поле NN определяет количество байтов данных в строке (в нашем случае 16 байтов). Поле AAAA – это начальный адрес, с которого данные будут записаны в память микроконтроллера.

За адресом следует поле команды CC. Программатор, ориентируясь на поле CC, распознает функциональное назначения строки. Ассемблер и другие компиляторы языков высокого уровня для AVR могут установить следующие значения данного параметра:

00 – в строке находятся данные для записи в память,
01 – последняя строка в файле,
02 – строка содержит начальный адрес сегмента памяти,
04 – строка содержит адрес в пределах сегмента памяти.

В данной строке CC=00 (т. е. строка предназначена для записи данных). За полем CC (кроме команды 01) идут непосредственно данные в количестве, определяемом параметром NN. Последнее поле SS – контрольная сумма. Сумма всех байтов в неповрежденной строке без учета переполнения всегда нулевая:

$$10 + 00 + 00 + 00 + 1F + \ldots + CF + F8 + CF + 8B = 0. \qquad (1)$$

Каждый hex-файл (рисунок) должен завершаться строкой :00000001FF.

```
:10010000214601360121470136007EFE09D2190140
:100110002146017EB7C20001FF5F16002148011988
:10012000194E79234623965778239EDA3F01B2CAA7
:100130003F0156702B5E712B722B732146013421C7
:00000001FF
```

Маркер записи
Кол-во данных
Смещение
Тип записи
Данные
Контрольная сумма

Рисунок. Пример содержимого файла формата Intel HEX

Чрезвычайно важно, чтобы отладчик умел дизассемблировать команды. При подходе к точке останова или пошагового события каждый поток исследуемого процесса по-прежнему указывает на определенную команду. Используя функции структуры CONTEXT, можно определить адрес памяти, где хранится команда, но это не позволяет узнать, какая именно команда была использована.

Ассемблер — это программа, которая переводит текст с языка, понятного человеку, в язык, понятный процессору, то есть говорят, что она переводит язык ассемблера в машинный код. Вместе с ассемблером обязательно должна быть еще одна программа – компоновщик (linker), которая и создает исполнимые файлы из одного или нескольких объектных модулей, полученных после запуска ассемблера [23].

Рассмотрим первый пример вложения информации. Как обычно, прежде чем работать со структурой, необходимо задать ее шаблон. Да-

лее для работы со структурой в файле необходимо создать ее экземпляр. В программе ниже шаблон структуры называется element, а соответствующий ему экземпляр структуры – si. Отметим лишь, что не стоит искать в приведенных ниже примерах какой-либо смысл, так как они предназначены только для демонстрации механизма вложенности структур (и объединений).

```
:prg02_01.asm – программа, демонстрирующая описание и использование структуры
; в программе на ассемблере.
elementstruc
INN dd 0;ИНН
name db 30 dup C ');Ф.И.О.
y_birthday dw 1962:год рождения
m birthday db 05;месяц рождения
d_birthday db 30:месяц рождения
nationality db 20 национальность
;и так далее
ends
.data
si element<>
.code
mov al,si.m_birthday
```

Информацию о дате рождения можно оформить в виде отдельной структуры, вложенной в текущую структуру, так как это сделано в программе ниже:

```
:prg02_02.asm – программа, демонстрирующая вложение структуры
;в текущую структуру в программе на ассемблере.
:
elementstruc
INN dd 0:ИНН
fiodb 30 dup (' ');Ф.И.О.
struc
y_birthday dw 1962;год рождения
m_birthday db 05;месяц рождения
d_birthday db 30;месяц рождения
ends
nationality db 20 национальность
;и так далее
ends
.data
si element<>
.code
mov al,sl.m_birthday
```

Синтаксис ассемблера допускает вынести описание вложенной структуры за пределы текущей структуры. При этом можно инициали-

зировать необходимые поля структуры birthday внутри отдельного экземпляра структуры element. Но работает такое описание структуры только в режиме IDEAL, что и продемонстрировано в программе ниже.

```
:prg02_03.asm – программа, демонстрирующая вложение структуры в другую
; структуру в программе на ассемблере.
birthday struc
y_bi rthday dw 1962:год рождения
m_birthday db 05:месяц рождения
d_birthday db 30:день рождения
ends
element struc
INN dd 0;ИНН
Birthday struc (m_birthday-06 .d_birthday=21)
fio db 30 dup C ');Ф.И.О.
nationality db 20 национальность
;и так далее
ends
.data
si element <.<>>
.code
ideal
mov al,si.m_birthday masm
```

Кстати, в описание структур можно вкладывать не только описания других структур, но и описание объединений, так как это показано в следующей программе.

```
:prg02_04.asm – программа, демонстрирующая взаимное вложение объединений
;и структур в программе на ассемблере.
elementstruc INN del 0:ИНН fiodb 30 dup C '):Ф.И.О .union
struc
y_birthday_1 dw 1962:год рождения
m_birthday_1 db 06;месяц рождения
d_birthday_1 db 03;месяц рождения
ends
struc
d_birthday_2 db?;месяц рождения
m_birthday_2 db?:месяц рождения
y_birthday_2 dw?;год рождения
ends
ends;конец объединения nationality db 20 – . национальность:и так далее
ends.data si element<>
!code"
mov al.si.m_bi rthday_l
mov sl.m_birthday_2.0ffh mov al,sl.m_birthday_2
```

Рассмотрим другой вариант вложения информации.

Запускам редактор, переходим в точку входа и смотрим на неё очень внимательно:

```
..... ! entrypoint:
..... !   pop       esi
80482c1 !   xor       ebp, ebp
80482c3 !   mov       ecx, esp
80482c5 !   and       esp, 0fffffff0h
80482c8 !   push      eax
80482c9 !   push      esp
80482ca !   push      edx
80482cb !   push      __libc_csu_fini
80482d0 !   push      __libc_csu_init
80482d5 !   push      ecx
80482d6 !   push      esi
80482d7 !   push      main
80482dc !   call      wrapper_8049630_80482a0
80482e1 !   hlt
80482e2 !   nop
80482e3 !   nop
```

Можно теперь заменить pop esi/xor ebp,ebp на jmp на наш код, откуда мы сможем сделать все, что задумано, выполнить эти команды и вернуться обратно. Для начала необходимо подготовить код, который мы будем внедрять. Для простоты выведем короткое приветствие на экран. Можно расширить последний сегмент и внедрится сюда, но это будет слишком заметно. На языке ассемблера это звучит приблизительно так:

```
mov eax, 4                  ; системный вызов write
mov ebx,1                   ; идентификатор стандартного вывода
mov ecx, offset begin_msg   ; указатель на первый символ выводимого сообщения
mov edx, offset end_msg     ; указатель на последний символ выводимого сообщения
int 80h                     ; вывод на экран
pop esi                     ; сохраненные команды
xor ebx,ebp
jmp 80482C3h                ; возврат в программу
```

Это не самый оптимальный вариант и его можно здорово оптимизировать, если переписать так:

```
xor eax,eax
add al, 4
xor ebx,ebx
inc ebx
mov ecx, offset begin_msg
mov edx,ecx
add edx, sizeof(msg)
```

```
int 80h
pop esi
xor ebp, ebp
jmp 80482C3h
```

Теперь прокручивая файл в hex-редакторе, найдем и выпишем стартовые адреса всех цепочек NOP'ов, пригодных для внедрения. А какие цепочки пригодны для внедрения? Если две соседние цепочки расположены в пределах досягаемости короткого перехода (грубо – в пределах сотни байт), трех NOP'ов будет вполне достаточно (2 байта на команду перехода, один – на любую однобайтовую команду полезного кода, например, inc ebx или pop esi). В противном случае нам необходимо иметь цепочку, по крайней мере, из 6-ти NOP'ов – пять на команду близкого перехода и один на полезную команду.

В нашем случае получается:

```
8048306h      10 байт
80483a2       14 байт
8048464       12 байт
```

Итого – 36 байт. Вполне достойное место для демонстрационной программы! Начинаем заполнять цепочки NOP'ов полезным кодом. С первой попытки у нас получается:

```
8048306     31 c0          xor    eax, eax
8048308     04 04          add    al, 4
804830a     e9 93 00 00 00    jmp    80483a2h
804830f     90             nop
```

При этом один последний NOP остается потерян, но по-другому не получается. Команда XOR EBX,EBX занимает два байта и сюда не лезет. А что, если переставить команды местами? [24] Перенести add al,4 в следующую цепочку NOP, а вместо нее вставить XOR EBX,EBX/INC EBX

```
8048306     31c0           xor    eax, eax
8048308     31db           xor    ebx, ebx
804830a     43             inc    ebx
804830b     e9 92 00 00 00    jmp    80483a2h
```

Тогда следующая цепочка будет заполнена так:

```
80483a2     0404           add    al, 4
80483a4     b9 ?? ?? ?? ??    mov    ecx, offset begin_msg
80483a9     89ca           mov    edx, ecx
80483ab     e9 b4 00 00 00    jmp    8048464h
```

В третью, последнюю, цепочку NOP'ов остаток кода уже не вмещается, не хватает одного единственного байта! Можно попытаться еще

немного ужать наш код. Например, пары инструкций mov edx,ecx/add edx,sizeof(msg), которые занимают 5 байт, можно использовать lea edx,[ecx+sizeof(msg)]. Сообщение также можно разместить в сегменте данных. Поскольку свободного места там не очень много, ограничимся строкой "hello". Завершающий нуль в конце ставить необязательно, поскольку системный вызов write выводит ровно столько символов, сколько ему задано вывести.

В данной статье исследованы три варианта вложения информации в исполнимый файл. В качестве контейнера были выбраны исполнимые файлы формата .Intel HEX. Такие файлы очень хорошо подходят на роль стегоконтейнеров для скрытой передачи личных сообщений. Были представлены способы вложения информации в исполнимый файл при помощи языка Ассемблера, а также применен вариант, сводящийся к беглому просмотру дизассемблерного листинга на предмет поиска основных способов внедрения информации при помощи различных директив. Все три варианта вложения информации достаточно просты. Особое внимание стоит уделить способу вложения с использованием замены операнд pop esi/xor ebp,ebp на jmp на наш код, откуда мы сможем сделать все, что задумано, выполнить эти команды и вернуться обратно. Факт вложения информации в исполняемый код, осуществив замены операнд, обнаружить гораздо сложнее, так как не существует однозначной связи между исходным кодом программы и скомпилированным исполняемым кодом. Одному и тому же исходному коду может быть сопоставлен разный исполняемый код в зависимости от компилятора и его настроек.

Библиографический список

1. **Вострикова, З. П.** Программирование на языке ассемблера ЕС ЭВМ / З. П. Вострикова. – М. : Наука, 1985.
2. **Галисеев, Г. В.** Ассемблер для Win 32. Самоучитель / Г. В. Галисеев. – М. : Диалектика, 2007. – С. 368.
3. **Зубков, С. В.** Ассемблер для DOS, Windows и UNIX / С. В. Зубков. – 3-е изд., стер. – М. : ДМК Пресс ; СПб. : Питер, 2004. – 608 с.
4. **Кип, Ирвин** Язык ассемблера для процессоров Intel = Assembly Language for Intel-Based Computers. — М. : Вильямс, 2005. – 912 с.
5. **Калашников, О. А.** Ассемблер? Это просто! Учимся программировать / О. А. Калашников. – БХВ-Петербург, 2011. – 384 с.
6. **Грибунин, В. Г.** Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.
7. **Cachin, C.** An Information-Theoretic Model for Steganography / C. Cachin // Proceeding of the Workshop on Information Hiding, 1998.

8. **Магда, Ю. С.** Ассемблер. Разработка и оптимизация Windows-приложений / Ю. С. Магда. – СПб. : БХВ-Петербург, 2003.

9. **Нортон, П.** Язык ассемблера для IBM PC / П. Нортон, Д. Соухэ. – М. : Компьютер, 1992.

10. **Пирогов, Владислав** Ассемблер для Windows / Владислав Пирогов. – СПб. : БХВ-Петербург, 2002. – 896 с.

11. **Основы языка Assembler** : методические указания к лабораторным работам по дисциплине «Машинно-ориентированные языки» / Сост. Л. А. Макушкина, И. А. Макушкин; Волгоград. гос. техн. ун-т. – Волгоград, 2008. – 107 с.

12. **Касперски, Крис** Искусство дизассемблирования / Крис Касперски. – СПб. : БХВ-Петербург, 2008. – 896 с.

13. **Пирогов, Владислав** Ассемблер и дизассемблирование / Владислав Пирогов. – СПб. : БХВ-Петербург, 2006. – 464 с.

14. **Саймон, Ричард** Microsoft Windows API Справочник системного программиста / Ричард Саймон. – М. : ООО ТИД "ДС", 2004. – 1217 с. + CD-диск.

15. **Фрунзе, А. В.** Микроконтроллеры? Это же просто! Т. 1. / А. В. Фрунзе. – М. : ООО "ИД СКИМЕН", 2002. – 336 с.

16. **Юров, В.** Assembler : учебный курс / В. Юров, С. Хорошенко. – СПб., 1999. – С. 672.

17. **Аблязов, Р. З**. Программирование на ассемблере на платформе x86-64 / Р. З. Аблязов. – М. : ДМК Пресс, 2011. – С. 304.

18. **Свидетельство** о государственной регистрации программы для ЭВМ № 2013612237 Российской Федерации. Программа для внедрения цифровых водяных знаков в исполняемые и библиотечные файлы / Красов А. В., Верещагин А. С. ; заявитель и правообладатель Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича». – № 2012661637 ; заявл. 25.12.2012 ; зарег. 18.02.2013; опубл. 20.03.2013.

19. **Красов, А. В.** Методы скрытого вложения информации в исполняемые файлы / А. В. Красов, А. С. Верещагин, В. С. Абатуров, М. В. Резник // Известия СПбГЭТУ «ЛЭТИ». – 2012. – № 8. – С. 51–55.

20. **Красов, А. В.** Аутентификация программного обеспечения при помощи вложения цифровых водяных знаков в исполняемый код / А. В. Красов, А. С. Верещагин, А. Ю. Цветков // Телекоммуникации. – 2013. – Спецвыпуск. – С. 27–30.

21. **Формат Intel-HEX** [Электронный ресурс] / Сайт Студии разработки "СпецПромДизайн". – Режим доступа: http://spd.net.ru/Article/Intel-HEX.aspx.

22. Intel HEX File Format Specification

23. http://assmbler.ru/2/HTML/ch01_01.htm

24. **InsidePro Software** [Электронный ресурс] / InsidePro Password Recovery Software. – Режим доступа: http://www.insidepro.com/kk/091/091r.shtml

Аннотация

Объект исследования включает в себя скрытое вложение информации в исполнимые файлы формата Intel HEX.

Целью статьи является исследование способов вложения информации в исполнимый файл формата .Intel HEX при помощи языка программирования «Ассемблер», для того чтобы определить наиболее простой вариант. Актуальность заключается в изучении проблемы выполнения синхронизации, определении начала и конца последовательности. Если в данных контейнера существуют биты синхронизации, заголовки пакетов и т. д., то скрытая информация может следовать сразу же после них. Сложность организации синхронизации является преимуществом с точки зрения обеспечения скрытности передачи. Скрытие информации, которая преимущественно имеет большой объем, выдвигает существенные требования к контейнеру, размер которого должен, по меньшей мере, в несколько раз превышать размер встраиваемых данных. Во многих случаях также желательна устойчивость полученного стеганосообщения к искажениям (в том числе и злоумышленным). Для таких преобразований очень подходит исполнимый файл формата Intel HEX. .

Тип реализующего ЭВМ (персональные компьютеры и рабочие станции), язык программирования (язык Ассемблера), вид и версия операционной системы (Linux, Mac OS, Windows), исполнимые файлы формата Intel HEX.

S. Shterenberg, A. Krasov

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

METHODS OF EMBEDDING INFORMATION IN THE EXECUTABLE FILE FORMAT . INTEL HEX

Annotation

The object of study involves embedding hidden information in the executable file format Intel HEX.

The aim of paper is to study ways of embedding information in the executable file format. Intel HEX using the programming language "Assembler " in order to determine the most simple option . The urgency is to examine the problems of the synchronization, defining the beginning and end of the sequence. If there are data bits container synchronization packet headers etc., the hidden information may follow immediately afterwards. The complexity of synchronization is an advantage in terms of stealth gear. Hiding information, which advantageously has a large volume , highlights the essential requirements for the container , the size of which should , at least several times the size of embedded data. In many cases it is also desirable obtained steganosoobscheniya resistance to distortion (including malicious) . For such transformations is very suitable executable file format Intel HEX. .

Type implements computers (PCs and workstations), a programming language (assembly language), the type and version of the operating system (Linux, Mac OS, Windows), executable file format Intel HEX.

Keywords: computer virus, assembly language, steganography, container, executable file format elf.

References

1. **Vostrikova, Z. P.** Programmirovanie na jazyke assemblera ES JeVM / Z. P. Vostrikova. – M. : Nauka, 1985.

2. **Galiseev, G. V.** Assembler dlja Win 32. Samouchitel' / G. V. Galiseev. – M. : Dialektika, 2007. – S. 368.

3. **Zubkov, S. V.** Assembler dlja DOS, Windows i UNIX / S. V. Zub-kov. – 3-e izd., ster. – M. : DMK Press ; SPb. : Piter, 2004. – 608 s.

4. **Kip, Irvin** Jazyk assemblera dlja processorov Intel = Assembly Language for Intel-Based Computers. — M. : Vil'jams, 2005. – 912 s.

5. **Kalashnikov, O. A.** Assembler? Jeto prosto! Uchimsja programmirovat' / O. A. Kalashnikov. – BHV-Peterburg, 2011. – 384 s.

6. **Gribunin, V. G.** Cifrovaja steganografija / V. G. Gribunin, I. N. Okov, I. V. Turincev. – M. : SOLON-Press, 2002. – 272 s.

7. **Cachin, C.** An Information-Theoretic Model for Steganography / C. Cachin // Proceeding of the Workshop on Information Hiding, 1998.

8. **Magda, Ju. S.** Assembler. Razrabotka i optimizacija Windows-prilozhenij / Ju. S. Magda. – SPb. : BHV-Peterburg, 2003.

9. **Norton, P.** Jazyk assemblera dlja IBM PC / P. Norton, D. Souhje. – M. : Komp'juter, 1992.

10. **Pirogov, Vladislav** Assembler dlja Windows / Vladislav Pi-rogov. – SPb. : BHV-Peterburg, 2002. – 896 s.

11. **Osnovy jazyka Assembler** : metodicheskie ukazanija k labora-tornym rabotam po discipline «Mashinno-orientirovannye jazyki» / Sost. L. A. Makushkina, I. A. Makushkin; Volgograd. gos. tehn. un-t. – Volgograd, 2008. – 107 s.

12. **Kasperski, Kris** Iskusstvo dizassemblirovanija / Kris Kas-perski. – SPb. : BHV-Peterburg, 2008. – 896 s.

13. **Pirogov, Vladislav** Assembler i dizassemblirovanie / Vladislav Pirogov. – SPb. : BHV-Peterburg, 2006. – 464 s.

14. **Sajmon, Richard** Microsoft Windows API Spravochnik sistemnogo programmista / Richard Sajmon. – M. : OOO TID "DS", 2004. – 1217 s. + CD-disk.

15. **Frunze, A. V.** Mikrokontrollery? Jeto zhe prosto! T. 1. / A. V. Frunze. – M. : OOO "ID SKIMEN", 2002. – 336 s.

16. **Jurov, V.** Assembler : uchebnyj kurs / V. Jurov, S. Horoshenko. – SPb., 1999. – S. 672.

17. **Abljazov, R. Z.** Programmirovanie na assemblere na platforme h86-64 / R. Z. Abljazov. – M. : DMK Press, 2011. – S. 304.

18. **Svidetel'stvo** o gosudarstvennoj registracii programmy dlja JeVM № 2013612237 Rossijskoj Federacii. Programma dlja vnedrenija cifrovyh vodjanyh znakov v ispolnjaemye i bibliotechnye fajly / Krasov A. V., Vereshhagin A. S. ; zajavitel' i pravoobladatel' Federal'noe gosudarstvennoe obrazovatel'noe bjudzhetnoe uchrezhdenie vysshego professional'nogo obrazovanija «Sankt-Peterburgskij gosudarstvennyj universitet

telekommunikacij im. prof. M. A. Bonch-Bruevicha». – № 2012661637 ; zajavl. 25.12.2012 ; zareg. 18.02.2013; opubl. 20.03.2013.

19. **Krasov, A. V.** Metody skrytogo vlozhenija informacii v ispolnjaemye fajly / A. V. Krasov, A. S. Vereshhagin, V. S. Abaturov, M. V. Reznik // Izvestija SPbGJeTU «LJeTI». – 2012. – № 8. – S. 51–55.

20. **Krasov, A. V.** Autentifikacija programmnogo obespechenija pri pomoshhi vlozhenija cifrovyh vodjanyh znakov v ispolnjaemyj kod / A. V. Krasov, A. S. Vereshhagin, A. Ju. Cvetkov // Telekommunikacii. – 2013. – Specvypusk. – S. 27–30.

21. **Format Intel-HEX** [Electronic resource] / Sajt Studii razrabotki "SpecPromDizajn". – Access mode: http://spd.net.ru/Article/Intel-HEX.aspx.

22. **Intel** HEX File Format Specification

23. http://assmbler.ru/2/HTML/ch01_01.htm

24. **InsidePro** Software [Electronic resource] / InsidePro Password Recovery Software. – Access mode: http://www.insidepro.com/ kk/091/091r.shtml

Штеренберг Станислав Игоревич – аспирант кафедры защищенных сетей связи Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», shterenberg.stanislaw@yandex.ru

Красов Андрей Владимирович – кандидат технических наук, доцент, профессор кафедры защищенных сетей связи Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», krasov@pisem.net

УДК 338.246

В. В. Макаров

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

Т. А. Блатова

Санкт-Петербургский филиал «Ленинградское отделение центрального научно-исследовательского института связи»

ИННОВАЦИИ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЯХ КАК АТРИБУТ ЭКОНОМИКИ ЗНАНИЙ

экономика знаний, информационно-коммуникационные технологии, знания, инновации, информация.

Одной из предпосылок появления инноваций являются новые знания. Именно знания становятся драйвером роста производительности труда и, как следствие этого, улучшения других экономических показателей: валового внутреннего продукта, национального дохода, заработной платы и т. д. То есть прослеживается явная взаимосвязь между информацией, новыми технологиями и эффективностью обучения с экономическими показателями развития общества. В связи с этим начинают говорить о переходе от традиционной экономики к экономике, основанной на знаниях, или к экономике знаний, имеющей определенные особенности.

Основным источником роста в экономике знаний являются нематериальные ресурсы. Именно революционные прорывы в информационно-коммуникационных технологиях (ИКТ) и их проникновение во все сферы деятельности сделали возможным появление экономики знаний [1]. ИКТ-отрасль охватывает разработку и производство телекоммуникационного и компьютерного оборудования, программного обеспечения, а также услуг по хранению, передаче и воспроизведению информации и данных. В настоящее время ИКТ являются одной из самых динамично развивающихся отраслей во многих странах. Для объективной оценки состояния экономики знаний в масштабах региона или страны огромное значение имеет определение уровня развития информационно-коммуникационных технологий, которые обеспечивают неоспоримые преимущества в распространении знаний и доступа к ним.

Определения термина «экономика знаний», которое являлось бы универсальным и всеобъемлющим, не существует. В публикациях различных авторов можно найти разные его трактовки. Организация экономического сотрудничества и развития (ОЭСР) определяет экономику знаний как экономику, которая непосредственно основана на производстве, распределении и использовании знаний и информации. Такая экономика характеризуется ростом инвестиций в сфере высоких технологий, ускорением внедрения инноваций в отрасли ИКТ, более высококвалифицированной рабочей силой и связанным с ними ростом производительности труда.

Рядом исследователей обобщены основные характеристики экономики знаний, которая, по их мнению:

− не является новой экономикой с новыми законами;

− присутствует во всех секторах экономики;

− отличается высокой степенью и постоянно растущей интенсивностью использования ИКТ высокообразованными работниками;

− характеризуется растущей долей нематериальных активов (интеллектуального капитала) по сравнению с долей физического капитала в ВВП [2];

− базируется на инновационных организациях, использующих новые технологии для инновационных процессов.

Управление развитием экономики знаний требует проведения регулярного мониторинга. Поэтому измерение экономики знаний является актуальной проблемой и становится неотъемлемой частью экономических исследований. Различными международными организациями разрабатываются системы индикаторов экономики знаний и методики их количественной оценки, позволяющие проследить динамику изменения этих показателей.

Одним из критериев формирования экономики знаний являются капитальные вложения в знания. ОЭСР создан интегральный показатель - «инвестиции в знания». Этот показатель включает в себя инвестиции в исследования и разработки, в высшее образование, в ИКТ и программное обеспечение. На основе этого показателя страны, входящие в ОЭСР, были разделены на три группы: с высокими (инвестируют около 6 % ВВП в знания), со средними (3–4 % ВВП) и с низкими инвестициями в знания (2–3 % ВВП).

Главным препятствием для объективного измерения экономики знаний является нехватка соответствующих данных. Согласно концептуальным положениям ОЭСР необходимо совершенствовать индикаторы экономики знаний: они должны фокусироваться на измерениях на входе (материальные затраты и человеческие ресурсы), измерениях на выходе (продукции), измерениях запасов знаний, сетей знаний, а также на измерениях образования и обучения.

Европейская стратегия экономического развития «Европа – 2020», принятая в 2010 году, определила три основные взаимодополняющие цели:

− умный рост: развитие экономики, основанной на знаниях и инновациях;

− устойчивый рост: эффективное использование ресурсов и повышение конкурентоспособности экономики;

− инклюзивный рост: содействие высокому уровню занятости, социальному и территориальному сплочению различных групп населения.

Отправной точкой для создания конкурентоспособной экономики знаний является функционирование такой системы высшего образования, которая не только может гибко реагировать на потребности регионов и работодателей, но и способна одновременно использовать новейшие результаты исследований и разработок.

Одним из возможных способов оценки экономики знаний, является методика, разработанная Всемирным банком. В настоящее время она состоит из 109 структурных и качественных переменных для оценки деятельности 146 стран по основным четырем группам экономики знаний: экономические стимулы и институциональный режим, образование и квалификация, инновационная система и информационно-коммуникационные технологии. Результаты оценки экономики знаний Всемирным банком представляются двумя основными показателями – индексом знаний и индексом экономики знаний. Структура этих индексов представлена на рисунке.

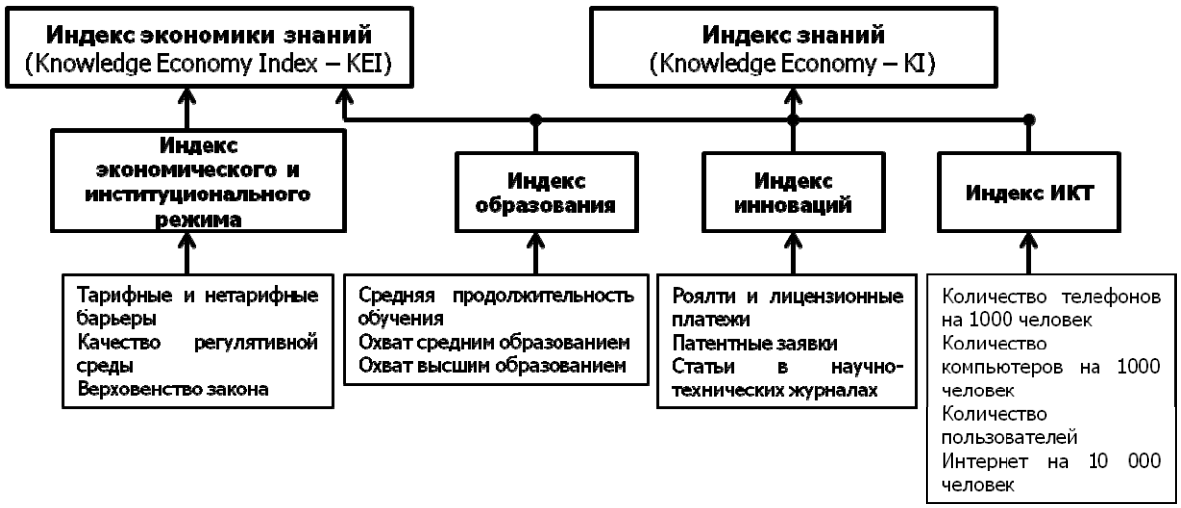


Рисунок. Структура индексов для оценки экономики знаний по методике Всемирного банка

Индекс знаний измеряет способность страны генерировать, принимать и распространять знания. Его значение указывает на общий потенциал развития знаний во всех странах. Индекс экономики знаний опре-

деляет, благоприятствует ли обстановка в стране эффективному использованию знаний для экономического развития. Это сводный индекс, который представляет собой общий уровень развития экономики знаний в той или иной стране или регионе. Значения индексов могут изменяться от 0 до 10. Чем выше индекс, тем выше уровень экономики знаний.

В таблице представлен рейтинг стран (первые десять стран и Россия) в соответствии с Индексом экономики знаний (Knowledge Economy Index – KEI) в 2012 году, а также приведены данные по миру (средний показатель для 146 стран). Как следует из таблицы, Россия занимает 55 место в этом рейтинге. В рейтинге стран по индексу ИКТ Россия занимает 44 место (значение индекса 7,16), что также достаточно далеко от стран-лидеров.

Устойчивое развитие мировой экономики в последнем десятилетии прошлого века, происходящее на фоне цифровизации сетей связи и бурном развитии сети Интернет, создало предпосылки для внедрения программ поддержки ИКТ в различных странах. Выделяют два основных подхода к развитию ИКТ в различных странах:

– ИКТ как сектор производства;

– ИКТ как катализатор социально-экономического развития страны.

В последние годы первое место и позицию самой передовой экономики знаний в мире занимает Швеция, ее показатели особенно сильны в области инноваций и ИКТ. Конкурентоспособность Швеции в ИКТ во многом связана с увеличением пользователей сети Интернет. От инвестиций в инфраструктуру ИКТ и услуг на базе ИКТ зависит развитие информационного общества. ИКТ могут сами по себе быть инновациями либо обеспечивать технологическую основу других нововведений. Кроме того, с использованием сетей широкополосного доступа знания могут более легко распространяться и быть доступны практически в любое время в любом месте.

Современное распространение Интернет, мобильной связи, телевидения, навигационных систем показывает, насколько всепроникающими являются эти технологии. Кроме того, благодаря своим многочисленным проявлениям, ИКТ можно позиционировать, как технологии широкого применения, которые создают инфраструктуру, обеспечивающую жизнеспособность инновационных процессов компаний. Инновации, как правило, рассматриваются в качестве важнейшего фактора экономического роста. Создание новых рабочих мест и повышение социальных стандартов связано также с проникновением инфокоммуникационных технологий и услуг в отдаленные районы страны.

ТАБЛИЦА. Рейтинг стран по развитию экономики знаний в 2012 году

Рейтинг по KEI	Страна	KEI	KI	Индексы			
				Экономического и институционального режима	Инноваций	Образования	ИКТ
1	Швеция	9,43	9,58	9,58	9,74	8,92	9,49
2	Финляндия	9,33	9,65	9,65	9,66	8,77	9,22
3	Дания	9,16	9,63	9,63	9,49	8,63	8,88
4	Нидерланды	9,11	8,79	8,79	9,46	8,75	9,45
5	Норвегия	9,11	9,47	9,47	9,01	9,43	8,53
6	Новая Зеландия	8,97	9,09	9,09	8,66	9,81	8,30
7	Канада	8,92	9,52	9,52	9,32	8,61	8,23
8	Германия	8,90	9,10	9,10	9,11	8,20	9,17
9	Австралия	8,88	8,56	8,56	8,92	9,71	8,32
10	Швейцария	8,87	9,54	9,54	9,86	6,90	9,20
…							
55	Россия	5,78	6,96	2,23	6,93	6,79	7,16
…							
	Мир	5,12	5,01	5,45	7,72	3,72	3,58

Для повышения места России в международных рейтингах, оценивающих развитие информационного общества и экономики знаний, необходимо совершенствовать инфраструктуру доступа, позволяющую использовать ИКТ на любом уровне (населением, бизнесом, государственными структурами) в соответствии с выбранной стратегией. Участие в международных рейтингах имеет не только экономическое, но и политическое значение, а также позволит разработать собственные критерии и методики оценки с учетом национальной специфики.

Библиографический список

1. **Макаров, В. В.** Методический подход к оценке информационных ресурсов [Электронный ресурс] / В. В. Макаров, В. И. Гусев, С. А. Синица // Информационные технологии и телекоммуникации. Электронный научный журнал. – 2013. – № 3. – С. 72–78. – Режим доступа: http://www.sut.ru/doci/nauka/review/3-13.pdf.

2. **Макаров, В. В.** Методологическая парадигма исследования интеллектуального капитала в условиях информационного общества / В. В. Макаров, В. И. Гусев, А. Г. Воронин // Российский гуманитарный журнал. – 2012. – Т. 1. – № 1. – С. 78–83.

Аннотация

Термин «экономика знаний» широко используется для определения типа экономики, в которой решающую роль играют знания, а их создание и использование становится определяющим фактором конкурентоспособности. Подход Всемирного банка к измерению экономики знаний определяет развитие информационно-коммуникационных технологий как один из четырех важнейших показателей.

V. Makarov

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

T. Blatova

St. Petersburg branch "Leningrad branch of the Central Research Institute of Communications"

INNOVATIONS IN INFORMATION AND COMMUNICATION TECHNOLOGIES AS AN ATTRIBUTE OF A KNOWLEDGE ECONOMY

Annotation

The term «knowledge economy» is widely used to determine the type of economy in which the decisive role is played by knowledge, and its creation and use is becoming a decisive factor of competitiveness. The approach of the World Bank for measurement of knowledge economy determines the development of information and communication technologies as one of the four most important indicators.

Keywords: knowledge economy, information and communication technology, knowledge, innovations, information

References

1. **Makarov, V. V.** Methodical approach to the evaluation of information resources [Electronic resource] / V. V. Makarov, V. I. Gusev, S. A. Sinitsa // Information Technology and Telecommunications. Electronic representative of the Journal. – 2013. – № 3. – PP. 72–78. – Access mode: http://www.sut.ru/doci/nauka/review/3-13.pdf.

2. **Makarov, V. V.** Metodologicheskaja paradigma issledovanija intellektual'nogo kapitala v uslovijah informacionnogo obshhestva / V. V. Makarov, V. I. Gusev, A. G. Voronin // Rossijskij gumanitarnyj zhurnal. – 2012. – T. 1. – № 1. – S. 78–83.

Макаров Владимир Васильевич – доктор экономических наук, профессор, заведующий кафедрой экономики и управления в связи Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

Блатова Татьяна Александровна – начальник Технопарка Санкт-Петербургского филиала «Ленинградское отделение центрального научно-исследовательского института связи», nsnlon@gmail.com

ISSN 2307-1303
ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ СПбГУТ
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

ТРЕБОВАНИЯ К РУКОПИСЯМ НАУЧНЫХ СТАТЕЙ, ПОДАВАЕМЫМ ДЛЯ ПУБЛИКАЦИИ

ОБЩИЕ ТРЕБОВАНИЯ И УСЛОВИЯ

1.1 Редакция принимает материалы (рукописи научных статей на русском или английском языках и сопроводительные документы), в которых приводятся результаты научной деятельности автора(ов).
1.2 Прием материалов осуществляется лично от авторов (наб. р. Мойки 61, каб. 269)**, через сайт журнала www.itt.sut.ru**.
1.3 В журнале не публикуются ранее опубликованные результаты научной деятельности автора(ов).
1.4 Подаваемые для публикации рукописи должны быть законченными работами, однако могут быть продолжающимися (разбитые на части и имеющие выводы по частям).
1.5 Результаты исследований должны соответствовать одной из научной отрасли: физико-математической (01.02.00, 01.04.00); технической (05.12.00, 05.13.00, 05.27.00), экономической (08.00.05 - экономика и управление в сфере IT и телекоммуникаций).
1.6 Материалы представляются в электронном виде (архив rar/zip) в следующем комплекте:

Файл 1 – рукопись научной статьи в формате MS Word (.doc). Если в рукописи присутствуют рисунки, необходимо приложить их в исходных форматах.
Файл 2 – скан первой страницы рукописи, подписанной автором(ами) - не представляется при личной подаче.
Файл 3 – информация об авторах, включая персональные данные и согласие на их обработку (фамилия, имя отчество полностью, дата рождения, место работы, ученая степень и звание, должность, паспортные сведения (серия, номер, дата выдачи, кем выдан), контактный е-мейл, телефон) в формате MS Word (.doc).
Файл 4 – информация об авторах (без персональных данных) на английском языке в формате MS Word (.doc).
Файл 5 – экспертное заключение о возможности опубликования рукописи в открытом доступе, заверенное по месту обучения или работы в сканированном виде. Авторам следует предусмотреть наличие письменного согласия на публикацию от лиц или организаций, по заказу которых производились те или иные исследования, прямые или косвенные результаты которых планируются к публикации в журнале. Отказ в представлении такого согласия может послужить отказом в публикации рукописи.
Файл 6 (для студентов-исследователей, магистров, аспирантов и соискателей ученых степеней) – рецензия научного руководителя, подпись научного руководителя заверяется по месту его работы в сканированном виде.
Рецензия должна содержать:
- актуальность рассматриваемых результатов;
- научную новизну предполагаемых решений;
- критический обзор статьи (включая замечания и предложения по их устранению);
- определение возможности публикации статьи в журнале.
- подпись и дату рецензирования, заверение подписи.

1.7 После получения материалов в полном объеме (п. 1.6) автору отправляется для заключения лицензионный договор о передаче неисключительных прав на использование произведения (может быть в виде оферты) и квитанция на оплату организационного взноса.
Редакция оставляет за собой право отбора рукописей для журнала и затребовать дополнительные документы.
1.8 Рукописи и носители информации авторам не возвращаются, гонорар не выплачивается.
1.9 Все рукописи проходят внешнюю экспертную оценку – рецензирование. При отрицательном заключении рукопись отклоняется для публикации.
1.10 При наличии положительной рецензии с рекомендацией рукописи к публикации или рекомендацией доработать рукопись (устранить замечания) и оплаченного организационного взноса, рукопись передается на предпечатную подготовку. При передаче на предпечатную подготовку рукописи, устанавливается срок ее выхода из печати. При отрицательной повторной рецензии рукопись отклоняется для публикации.
1.11 В процессе предпечатной подготовки рукопись вычитывается редактором/корректором. В это время редактор/корректор будет обращаться к автору(ам) для исключения неточностей, ошибок, опечаток и пр. по указанным автором(амии) е-мэйлу/телефону.
1.12 После второй корректуры рукопись ставится в выпуск, подписывается в печать. Внесение авторских исправлений после подписания рукописи/выпуска в печать невозможно.

Важная информация. Неисключительные права на все материалы, опубликованные в журнале принадлежат СПбГУТ. Все материалы, авторские права на которые принадлежат СПбГУТ, могут быть воспроизведены при наличии письменного разрешения от СПбГУТ. Ссылка на первоисточник обязательна. Настоящие требования могут быть изменены без оповещения. Актуальные требования будут расположены на сайте журнала - http://www.itt.sut.ru.

ТРЕБОВАНИЯ К ФАЙЛУ РУКОПИСИ

2.1 Объем текста научной статьи – не менее 8 и не более 12-ти машинописных страниц (с рисунками, таблицами, библиографией). Формат страницы – А4, при этом каждое поле должно быть 25 мм, за исключением левого - 30 мм. Абзацный отступ 10 мм.
2.2 На первой странице рукописи до текста указываются УДК, фамилии, инициалы авторов, название статьи, ключевые слова.
2.3 Структура рукописи следующая:
УДК (размер шрифта 14, расположение текста по левому краю); для определения УДК используйте on-line классификатор www.udcc.org;
фамилия, инициалы автора (авторов) (с расстановкой по алфавиту) с указанием места обучения или работы (размер шрифта 14, расположение текста по левому краю);
название рукописи (размер шрифта 14, заглавные буквы, расположение текста по левому краю);
ключевые слова (размер шрифта 12, расположение текста по ширине);
текст рукописи (размер шрифта 14, расположение текста по ширине):
- введение;
- пункты и подпункты;
- заключение (выводы);
- библиографический список (размер шрифта 14, расположение текста по ширине);
- аннотация (размер шрифта 14, расположение текста по ширине) приводится на отдельной странице после библиографического списка.

На английском языке (на русском, если язык рукописи английский) представляются: фамилия и имя автора, место работы или учебы, название статьи, аннотация (абстракт), ключевые слова, библиографический список, сведения об авторе(ах).
При написании аннотации рекомендуем использовать статью «Сысоев, П. В. Правила написания аннотации / П. В. Сысоев // Иностранные языки в школе / гл. ред. Н. П. Каменецкая.– 2009.– N4.– С.81-83».
2.4 Текст рукописи должен быть тщательно вычитан и подписан всеми авторами на первой странице, правка текста и исправление рисунков, корректировка аннотации выполняются редактором журнала совместно с автором(ами).
2.5 Верстку производить с межстрочным интервалом «1» по приведенным требованиям, стили и макросы не применять.
2.6 Буквы в тексте и формулах латинского алфавита набираются курсивом, буквы греческого и русского алфавитов – прямым шрифтом. Математические символы lim, lg, ln, arg, sin, min и т. д. набираются прямым шрифтом.
2.7 Не следует применять сходные по начертанию буквы латинского, греческого и русского алфавитов, использовать собственные макросы и рисунки для букв.
2.8 Следует различать букву О и ноль 0; дефис «-», знак минуса и тире «–».
2.9 Формулы должны быть набраны только в редакторе MS Equation, а отдельные символы и буквы формул в тексте статьи должны быть набраны в редакторе MS Word (не в Equation!). Длинные формулы следует разбивать на независимые фрагменты (каждая строка – отдельный объект). Нумеровать нужно только те формулы, на которые есть ссылки в тексте.
2.10 Нельзя использовать рисунки и таблицы для размещения формул.
2.11 Рисунки и фотографии располагаются в тексте. Все надписи на рисунках и фотографиях должны быть вполнены таким же начертанием и размером шрифта как и основной текст.
2.12 Ширина таблиц (шрифт 12 pt) не должна превышать ширину страницы.
2.13 Все таблицы, графики, схемы и рисунки должны быть подписаны и обязательно оформлены с переводом в формат MS Word.
2.14 На рисунках буквы латинского алфавита в сканированном виде также набираются курсивом, а буквы греческого и русского алфавитов – прямым шрифтом.
2.15 Перечень источников приводится общим списком в конце статьи. Составляется в соответствии с последовательностью ссылок в тексте. Ссылки на источники в тексте приводятся в квадратных скобках.
2.16 Примеры оформления библиографических описаний различных изданий приведены в ГОСТ Р 7.0.5 2008 «Библиографическая ссылка. Общие требования и правила составления».

ISSN 2307-1303
9 772307 130308 80413>

НАУЧНОЕ ИЗДАНИЕ

Информационные технологии и телекоммуникации

Электронный научный журнал

Выпуск 4-2013

Минимальные системные требования для просмотра издания:
Тип компьютера, процессор, сопроцессор, частота: Pentium IV и выше / аналогичное; оперативная память (RAM): 256 Мб и выше; необходимо на винчестере: не менее 64 Мб; ОС MacOS, Windows (XP, Vista, 7) / аналогичное; видеосистема: встроенная; дополнительное ПО: Adobe Reader версия от 7.X или аналогичное. Защита от незаконного распространения: реализуется встроенными средствами Adobe Acrobat.

Неисключительные права на все материалы, опубликованные в данном издании принадлежат СПбГУТ.
Все материалы, авторские права на которые принадлежат СПбГУТ, могут быть воспроизведены при наличии письменного разрешения от СПбГУТ.
Ссылка на первоисточник обязательна.
По вопросом приобретения неисключительных прав и использования журнала обращайтесь по тел. (812) 326-31-63, добавочный 1388, e-mail telecomsut@gmail.com

Идея создания журнала состоит в полноформатном информировании сообщества о тенденциях развития IT и телекоммуникационной отраслей, в сочетании новейших достижений науки и их внедрения в производство. Наш журнал это не только окно информации, но и площадка для научных дискуссий. Мы готовы предоставить площадку как для ученых с именем, так и для только делающих первые шаги в науке. Журнал ориентирован на статьи в области физико-математических; технических (05.12.00, 05.13.00, 05.27.00), исторических (07.00.10), экономических (08.00.05 - управление инновациями, связь, экономические аспекты IT и телекоммуникаций) наук.

Подписано в печать 30.12.2013
Вышло в свет 30.01.2013
Уст. объем 4,5 печ. л. Заказ № 005-ИТТ-2013.
191186, СПб, наб. р. Мойки, 61
E-mail: telecomsut@gmail.com
www.itt.sut.ru