На правах рукописи

Миняев Андрей Анатольевич

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

2.3.6. Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2021

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича» на кафедре защищенных систем связи.

Научный руководитель: кандидат технических наук, доцент
Красов Андрей Владимирович

Официальные оппоненты: **Беззатеев Сергей Валентинович**,
доктор технических наук, доцент,
Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра технологий защиты информации, заведующий кафедрой

Супрун Александр Федорович,
кандидат технических наук, доцент,
Санкт-Петербургский политехнический университет Петра Великого, Институт кибербезопасности и защиты информации, доцент

Ведущая организация: Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук», г. Санкт-Петербург

Защита состоится 01 декабря 2021 года в 16.00 на заседании объединенного диссертационного совета 99.2.038.03, созданного на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова», Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» по адресу: Санкт-Петербург, пр. Большевиков, д. 22, корп. 1, ауд. 554/1.

С диссертацией можно ознакомиться в библиотеке СПбГУТ по адресу Санкт-Петербург, пр. Большевиков, д. 22, корп. 1 и на сайте www.sut.ru.

Автореферат разослан 01 октября 2021 года.

Ученый секретарь
диссертационного совета 99.2.038.03,
канд. техн. наук, доцент А.Г. Владыко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Информационная безопасность (ИБ) в последние годы становится все более значимой и важной сферой национальной безопасности Российской Федерации (РФ), что отражено в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации 5 декабря 2016 г. № 646. Одновременно с ростом и развитием информационных технологий совершенствуются тактики, техники, способы и сценарии реализации атак и угроз безопасности информации (УБИ), расширяется инструментарий для нарушения состояния ИБ. Согласно отчетам крупных международных и российских копаний, количество утечек данных из информационных систем (ИС) растет из года в год. Изменить ситуацию можно путем разработки новых и совершенствования существующих подходов к обеспечению ИБ, способных предоставить надежную защиту от современных УБИ.

В настоящее время бизнес-процессы большинства компаний строятся с учетом географии их присутствия. Примером могут быть компании, имеющие свои филиалы, представительства и подразделения на всей территории страны и за ее пределами. Это относиться и к процессам государственного управления. Соответственно, современные ИС в большинстве случаев представляют собой сложные географически-распределенные (территориально-распределенные) системы с своей специфической ИТ-инфраструктурой, технологией обработки информации и информационными технологиями, реализующими бизнес-процессы или процессы государственного управления. В этой связи для территориально-распределенных информационных систем (ТРИС) возникают ряд сложностей, связанных с обеспечением ИБ.

Одной из важной задачей обеспечения ИБ является оценка эффективности системы защиты информации (СЗИ), качественные результаты которой влияют на уровень защищенности ИС. Под эффективностью СЗИ понимается ее способность противостоять УБИ и характеризует уровень защищенности ИС (в частности, ТРИС). Эффективность СЗИ зависит от множества взаимосвязанных между собой подсистем, модулей и элементов, как правило, оцениваемых совокупностью показателей. На сегодняшний день отсутствует общий подход к оценке эффективности СЗИ, что влечет за собой ряд проблем, связанных с процедурами оценивания и, как следствие, некорректное определение уровня защищенности ИС (ТРИС). Недостатки известных методов и методик оценки эффективности СЗИ связаны, в том числе, с определением показателей оценки, недостатками экспертных оценок, методик расчета количественных оценок, отсутствием автоматизированных инструментов. Все перечисленное влияет на эффективность СЗИ и может привести к возникновению различных рисков (киберрисков) для владельцев ИС (ТРИС).

Степень разработанности темы. Проблемы ИБ в ИС, в том числе, оценки эффективности и соответствия СЗИ, отражены в работах российских и зарубежных ученых: Зегжды Д.П., Ивашко А.М., Буйневича М.В., Барабанова А.В., Дорофеева А.В., Маркова А.С., Цирлова В.Л., Герасименко В.А., Котенко И.В., Саенко И.Б., Юсупова Р.М., Молдовяна Н.А., Молдовяна А.А., Зикратова И.А., Кустова В.Н., Домарева В.В., Scott Barman, Brian Carrie, Lendver K., D. Maclean, Norbert Wiener и др. В настоящей диссертационной работе также использованы результаты исследований, посвященных построению систем поддержки принятия решений в слабоструктурированных предметных областях, обработке трудно формализуемых и нечетких данных, ряда российских и зарубежных ученых: Л. Заде, Т. Саати, О.М. Полещука, Н.В. Хованова и др.

Эффективность СЗИ достигается путем создания СЗИ, способной максимально нейтрализовать актуальные УБИ, выполнить требования по защите информации, а также позволяющей минимизировать финансовые затраты на создание СЗИ. Известные методы и методики оценки эффективности СЗИ ТРИС не могут быть применены на всех этапах жизненного цикла, что не позволяет владельцам (операторам) ТРИС своевременно вносить изменения в СЗИ, тем самым снижая уровень защищенности ТРИС. Для математического аппаратов существующих методов остается актуальной задача уменьшения среднеквадратической ошибки (RMSE) работы адаптивных нечетких нейронных продукционных систем (adaptive neuro-fuzzy inference system, ANFIS), как наиболее подходящего аппарата для решения подобных задач.

На основании изложенного можно сделать вывод о необходимости совершенствования методик оценки эффективности СЗИ, что подтверждает актуальность настоящего диссертационного исследования.

Объектом исследования являются угрозы безопасности и требования по защите информации. **Предмет исследования** являются методы и методики моделирования актуальных угроз безопасности информации и оценки эффективности систем защиты информации.

Целью диссертационного исследования является повышение качества оценки эффективности систем защиты информации территориально-распределенных информационных систем за счет определения необходимых и достаточных показателей. Для достижения поставленной цели необходимо решить следующие **задачи:**

1. Провести анализ ТРИС: определить бизнес-процессы в ТРИС; информацию, обрабатываемую в ТРИС; группы пользователей, имеющих доступ к информации в ТРИС, их права и полномочия; выявить основные аспекты технологии обработки информации; проанализировать ИТ-инфраструктуру ТРИС (информационные технологий и программное обеспечение, реализующее бизнес-процессы ТРИС); провести анализ атак и УБИ в ТРИС, требований по защите информации; анализ

СЗИ ТРИС; анализ существующих методов и методик моделирования УБИ и оценки эффективности СЗИ ТРИС.

2. Повысить качество определения актуальных УБИ в ТРИС за счет определения необходимых и достаточных показателей, достижения наименьшей среднеквадратической ошибки работы методики на основе ANFIS, автоматизации процесса для исключения недостатков экспертных методов и применения технологий Data Science при обработке большого объема данных.

3. Повысить качество оценки эффективности СЗИ ТРИС за счет определения необходимых и достаточных показателей оценки, уменьшения значений среднеквадратической ошибки работы адаптивных нечетких нейронных продукционных систем по сравнению с известными методами, автоматизировать процесс для исключения недостатков экспертных методов.

4. Разработать методические рекомендации, позволяющие в автоматизированном режиме оценивать эффективность СЗИ на всех этапах жизненного цикла ТРИС с точки зрения нейтрализации актуальных УБИ, соответствия по требованиям ИБ, уменьшения финансовых затрат на создание СЗИ, за счет внесения изменений в алгоритмы известных методик.

5. Провести оценки эффективности предложенных методик и метода.

Научная задача диссертационного исследования состоит в том, чтобы повысить качество оценки эффективности СЗИ ТРИС, предложив автоматизированные метод и методики определения актуальных УБИ и оценки эффективности СЗИ, основанные на адаптивных нечетких нейронных продукционных системах, за счет определения необходимых и достаточных показателей и адаптации параметров таких систем.

Научная новизна результатов исследования заключается в следующем:

1. Предложенная методика определения актуальных УБИ, в отличие от известных, в автоматизированном режиме определяет перечень актуальных УБИ, гипотетически исключая ошибки экспертов.

2. Предложенный метод оценки эффективности СЗИ, в отличие от известных, основан на теории адаптивных нечетких нейронных продукционных системе и алгоритме нечеткого вывода Такаги-Сугено-Канга с применением технологий Data Science.

3. Разработанные методические рекомендации по оценке эффективности СЗИ в ТРИС, в отличие от известных, позволяют сократить количество не учтенных актуальных УБИ, снизить финансовые затраты на создание СЗИ, применимы на всех этапах жизненного цикла систем, могут быть адаптированы под требования владельцев ТРИС. Рекомендации не требуют привлечения высококвалифицированных специалистов по ИБ, не требуют больших вычислительных ресурсов, предлагают автоматизированный режим работы, что, в

совокупности, исключает недостатки известных методик и повышает эффективность СЗИ в ТРИС.

Теоретическая ценность работы заключается ее вкладом в развитие теории и методов обеспечения ИБ, а именно: в выборе необходимых и достаточных показателей определения актуальных УБИ и оценки эффективности СЗИ; в расширении класса методов оценки эффективности СЗИ в части адаптации регулятора адаптивной нечеткой нейронной продукционной системы, достигаемой применением нейрона с последовательным методом обучения; в доказательстве достижения наименьшей среднеквадратической ошибки работы ANFIS при применении алгоритма нечеткого вывода Такаги-Сугено-Канга для решения поставленной задачи; в использовании технологий Data Science при обработке большого объема данных в части очистки и преобразования наборов данных, выбора наиболее полезных и создание новых более репрезентативных признаков.

Практическая ценность работы заключается в следующих результатах:

1. Проведенный анализ ТРИС позволил определить бизнес-процессы, выполняемые системами; виды и категории информации; группы пользователей и методы доступа к ТРИС; аспекты технологий обработки информации и ИТ-инфраструктуры систем. Анализ атак и УБИ в ТРИС, требований по защите информации, анализ СЗИ ТРИС, анализ существующих методов и методик моделирования УБИ и оценки эффективности СЗИ позволил использовать полученные результаты при определении необходимых и достаточных показателей моделирования УБИ и оценки эффективности СЗИ ТРИС.

2. Предложенная методика определения актуальных угроз безопасности информации позволяет определять на 5% больше актуальных УБИ, гипотетически исключая недостатки экспертов и минимизирует трудоемкость процесса и вычислительные ресурсы, в отличие от известных методик.

3. Предложенные метод и методические рекомендации по оценке эффективности СЗИ ТРИС позволяют проводить оценку на основе необходимых и достаточных показателей, определенных в настоящем диссертационном исследовании, предоставляют владельцам ТРИС возможность оценивать эффективность СЗИ в реальном времени на всех этапах жизненного цикла существования ТРИС, гипотетически исключая ошибки экспертов, что, в свою очередь, позволяет своевременно вносить корректировки в проектные решения СЗИ для нейтрализации УБИ и выполнения требований по защите информации, учитывая финансовую составляющую при создании СЗИ. Показатели оценки эффективности могут быть изменены в зависимости от целей и потребностей владельца ТРИС в проведении оценки эффективности СЗИ ТРИС.

4. Разработанные в рамках диссертационного исследования программы для ЭВМ «Модель угроз и нарушителя» и «Оценка системы защиты информации»

автоматизируют процессы определения актуальных УБИ и оценки эффективности СЗИ.

Внедрение результатов работы. Результаты диссертации использованы при определении перечня актуальных угроз безопасности и проведении оценки эффективности СЗИ ТРИС в ЗАО «ДИДЖИТАЛ ДИЗАЙН», ООО «Рэйдикс» и ЗАО НПФ «УРАН». Разработана программа для ЭВМ «Модель угроз и нарушителя», реализующая предложенную методику определения актуальных угроз безопасности информации и автоматизирующее этот процесс. Разработана программа для ЭВМ «Оценка системы защиты информации», реализующая предложенный метод оценки эффективности СЗИ. Результаты работы были внедрены в учебный процесс СПбГУТ на старших курсах обучения бакалавров по направлению подготовки 10.03.01 «Информационная безопасность» по дисциплине «Методы оценки безопасности компьютерных систем» и магистров первого года обучения по направлению подготовки 10.04.01 «Информационная безопасность» по дисциплине «Сертификация средств защиты информации» при чтении курсов лекций, проведении практических занятий и лабораторных работ.

Методы исследования. В работе использованы методы неявного перебора, теории вероятности и математической статистики, динамического программирования, теории адаптивных нечетких нейронных продукционных систем, алгоритмы нечеткого вывода.

Основные результаты, выносимые на защиту:

1. Методика определения актуальных угроз безопасности информации.
2. Метод оценки эффективности систем защиты информации.
3. Методические рекомендации по оценке эффективности систем защиты территориально-распределенных информационных систем.

Достоверность результатов, выносимых на защиту диссертационного исследования, выводов научного характера подтверждаются математическим обоснованием результатов исследований, системным подходом к решению поставленных задач, обоснованием выбранных методов и показателей определения актуальных УБИ и оценки эффективности СЗИ, доказательствами и результатами экспериментальной проверки предложенных метода и методик, анализом работ существующих зарубежных и отечественных практик решения аналогичных задач, апробацией результатов работы на международных и российских конференциях, а также подтверждением о внедрении предложенных метода и методик в организациях и предприятиях.

Апробация результатов исследования. Результаты, полученные в рамках работы над диссертацией, представлялись и обсуждались на следующих конференциях: IX и X Международная научно-техническая и научно-методическая конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Россия, Санкт-Петербург, 2020–2021); XII Международный конгресс

по ультрасовременным системам телекоммуникаций и управления (The 12th International Congress on Ultra Modern Telecommunications and Control Systems). Brno, Czech Republic, 2020, online; X Международная научно-техническая конференция «Технологии разработки информационных систем» (Россия, г. Геленджик, 2020, online); Всероссийская межведомственная научно-техническая конференция «НАУКА И АСУ – 2020» (Россия, г. Москва, 2020, online); XX Международная конференция «Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь». DCCN-2017 (г. Москва, 2017); IV–VI Всероссийская конференция «Проблема комплексного обеспечения информационной безопасности и совершенствование образовательных технологий подготовки специалистов силовых структур» (Россия, Санкт-Петербург, 2015–2017).

Диссертация выполнена при поддержке гранта для студентов вузов, расположенных на территории Санкт-Петербурга, аспирантов вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга (Россия, Санкт-Петербург, 2015 г.). Диплом № 15542 от 27.11.2015 г.

Подготовлено учебно-методическое пособие «Сертификация средств защиты информации» (Россия, Санкт-Петербург, СПбГУТ).

Публикации. По теме диссертации опубликованы 16 печатных работ, 6 из которых – в изданиях из перечня рецензируемых научных журналов ВАК при Минобрнауки России, в том числе 2 из них без соавторства; 2 – в международных изданиях, индексируемых в базах данных Web of Science и Scopus; 2 свидетельства о государственной регистрации программы для ЭВМ; 6 работ, опубликованных в других изданиях.

Соответствие паспорту специальности. Все результаты, выносимые на защиту, соответствуют п.п. 1, 3 и 10 паспорта научной специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Личный вклад автора. В работе предложены методика определения актуальных угроз безопасности информации, метод и методические рекомендации по оценке эффективности систем защиты в территориально-распределенных информационных системах, разработаны программы для ЭВМ, реализующие предложенные методики и методы, положения работы были внедрены в учебный процесс СПбГУТ. Перечисленные результаты получены автором лично.

Объем и структура диссертации. Диссертационная работа состоит из введения, четырех глав, заключения и списка литературы. Материал изложен на 216 страницах, включает 34 таблицы, 37 рисунков и схем, а также 6 приложений. Список литературы содержит 107 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В введении приводиться обоснование актуальности темы, определяются цели и задачи, предмет и объекты диссертационного исследования. Обоснованы научная новизна и практическая ценность выносимых на защиту результатов. Дана краткая характеристика содержания работы, приведены сведения о внедрении и об апробации результатов диссертационного исследования.

В первой главе приведены результаты анализа основных бизнес-процессов, выполняемых ТРИС; видов и категорий обрабатываемой информации; описание групп пользователей и методов доступа в ТРИС; определены ключевые аспекты ИТ-инфраструктуры ТРИС и их СЗИ; приведены результаты анализа моделей и методов моделирования ИС, моделей атак и УБИ, методов и методик оценки эффективности СЗИ, а также результаты анализа международных стандартов и нормативных правовых актов регуляторов в области обеспечения ИБ.

Установлено, что известные методики определения актуальных УБИ имеют ряд своих недостатков, связанных с выбором недостаточных показателей, ошибками экспертов, с необходимостью привлечения высококвалифицированных специалистов по ИБ, отсутствием автоматизированных инструментов, а также с проблемами, связанными с обработкой большого объема данных при определении перечня актуальных УБИ.

Отмечено, что известные методы и методики оценки эффективности СЗИ не в полной мере удовлетворяют всем показателям защищенности ИС, таких как ИТ-инфраструктура ТРИС, перечень актуальных УБИ, требования по защите информации, оценка рисков (негативных последствий) при реализации УБИ, стоимость финансовых затрат на создание СЗИ. Не имеют автоматизированных инструментов, требуют привлечения высококвалифицированных специалистов по ИБ, имеют недостатки, свойственные экспертным оценкам.

В первой главе сформулирована цель диссертационного исследования. Определены задачи, решение которых позволит повысить эффективность СЗИ (уровень защищенности ТРИС), а также научных и практических основ оценки эффективности СЗИ ТРИС.

Во второй главе предложена методика определения актуальных УБИ, основанная на теории адаптивных нечетких нейронных продукционных систем и алгоритмах нечеткого вывода, которая, в отличии от известных, использует необходимые и достаточные показатели, автоматизирована и гипотетически исключает ошибки экспертов. Методика позволяет определять количество актуальных УБИ на 5% больше, снижать финансовые затраты на закупку средств защиты информации от 15% до 30% по сравнению с известными. Учитывает необходимые и достаточные показатели: уровень мотивации и возможности нарушителей в ТРИС (источник УБИ, актуальный нарушитель), ИТ-инфраструктуру ТРИС (объекты воздействия), перечень существующих СрЗИ в

ТРИС, тактики, техники и способы реализации (процедуры) проведения атак. Преимущества методики:

– процесс определения актуальных УБИ автоматизирован;

– отсутствует необходимости привлечения высококвалифицированных специалистов в области ИБ;

– отсутствуют недостатков экспертных оценок;

– предложенная методика позволяет определять перечень актуальных УБИ в ИС различных типов и классов;

– учитывает БДУ ФСТЭК России;

– может быть адаптирована для работы с международными базами данных УБИ (MITRE CVE, OSVDB, NVD, Secunia);

– использует перспективные научные исследования в области адаптивных нечетких нейронных продукционных систем, алгоритмов нечеткого вывода и технологий Data Science при обработке большого объема данных.

Алгоритм работы предложенной методики заключается в реализации нечеткой продукционной модели, основанной на правилах типа:

$$R_i : IFx_i ISA_{i1} AND...ANDx_j ISA_{ij} AND...ANDx_{im} ISA_{im}, THEN$$

По результатам анализа были определены необходимые и достаточные показатели определения актуальных УБИ и сформирована база правил для определения актуальных УБИ. В основу легли данные об источниках УБИ, определенных в работе рисков и негативных последствий от их наступления, объектах воздействия, тактиках, техниках, способов и сценариев реализации атак, существующих средств защиты информации, используемых в СЗИ и способных нейтрализовать ряд возможных УБИ. Набор данных в предложенной методике учитывает возможные способы и сценарии реализации УБИ, основанные на известных тактиках, техниках и процедур проведения атак (ФСТЭК России и MITRE Adversarial Tactics, Techniques & Common Knowledge).

Фрагмент базы правил на основании сформированного в данной работе набора данных приведен в таблице 1.

Актуальность в соответствии с методическими документами ФСТЭК России определяется на основании возможных сценариев реализации УБИ с учетом имеющихся средств защиты информации.

УБИi = [Н; ОВ; СР УБИ; СрЗИ; НП],

где *УБИi – i* угроза безопасности информации из Банка данных угроз ФСТЭК России (далее – БДУ); *Н* – актуальный нарушитель; *ОВ* – объект воздействия; *СР УБИ* – способ реализации УБИ; *СрЗИ* – средство защиты информации, предназначенное для нейтрализации УБИ; *НП* – негативные последствия.

Таблица 1 – Фрагмент базы правил методики определения актуальных УБИ

№ п/п	ЕСЛИ (IF)			ТО (THEN)
	Тип нарушителя (источник воздействия)	**ИТ – инфраструктура (объект воздействия, версия ПО)**	**Сценарий реализации (тактики, техники и процедуры)**	
1	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Виртуальная машина VMWare 6.5 (VMWare Workstation), от 7.0.0 до 7.1.4 включительно (VMWare Workstation)	T1.3 T1.4 T1592.004 T1205	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин (УБИ.079)
2	Внешний нарушитель с высоким потенциалом	Мобильное устройство (аппаратное устройство) на базе iOS (Android), до 10.3.3 включительно (iOS)	T3.1 T7.4 T1204 T1399	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве (УБИ.196)
…				
N	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Средство защиты информации 12.4 (Cisco IOS), 12.4 (Cisco IOS), 15.0 (Cisco IOS), 15.0 (Cisco IOS), 15.1 (Cisco IOS), 15.1 (Cisco IOS), 12.2 (Cisco IOS), 12.2 (Cisco IOS), 15.2 (Cisco IOS), 15.2 (Cisco IOS)	T6.1 T7.21 T1562 T1056	Угроза несанкционированного воздействия на средство защиты информации (УБИ.187)

Анализ оценки эффективности предложенной методики определения актуальных УБИ представлен в таблице 2.

Таблица 2 – Анализ оценки эффективности предложенной методики определения актуальных УБИ

Показатель	**Известные методики**	**Предложенная методика**
RMSE	0,017 – 0,068	0,012-0,023
Определение количества актуальных УБИ	~ 71	~ 76
Стоимость СЗИ	снижение до 15%	снижение до 30%

Среднеквадратичная ошибка предложенного метода, вычисляемая по формуле:

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2},$$

где $y_i, \hat{y}_i$ – наборы данных (обучения, проверки), N – число элементов в обучающей выборке, достигает значения в диапазоне 0,012-0,023, что является локальным минимумом на заданном интервале и позволяет доказать выполнение поставленной в настоящем диссертационном исследовании задачи.

В третьей главе определены необходимые и достаточные показатели и предложен метод оценки эффективности СЗИ, основанный на адаптивной нечеткой нейронной продукционной системе и алгоритме нечеткого вывода Такаги-Сугено-Канга. Метод позволяет достигать наименьшего значения среднеквадратической ошибки работы системы, таким образом повышает эффективность СЗИ (уровень защищенности ТРИС) до 97%, что на 15% больше по сравнению с известными методам. Финансовые затраты на создание СЗИ позволяют достигать уменьшения стоимости до 30%. Предложенный метод позволяют владельцам систем автоматически оценивать эффективность СЗИ в режиме реального времени на всех этапах жизненного цикла системы, что позволяет своевременно вносить корректировки в проектные решения СЗИ для нейтрализации актуальных УБИ и выполнения требований по защите информации, учитывая финансовую составляющую.

Определены показатели оценки, исходя из определения и целей достижения эффективности СЗИ:

– перечень актуальных УБИ;

– перечень требований по ИБ с учетом классификации конкретной ИС;

– перечень СрЗИ, который формируется по результатам разработки СЗИ ТРИС и их стоимость (информация от производителей/вендоров).

Показатели оценки эффективности для предложенного метода могут быть изменены в зависимости от целей и потребностей владельца системы.

Установлено, что для решения задач проведения оценки эффективности СЗИ ТРИС целесообразно использовать ANFIS с алгоритмом нечеткого вывода Такаги-Сугено-Канга.

Алгоритм работы метода заключается в реализации нечеткой продукционной модели, основанной на правилах типа:

$$R_i : IFx_i ISA_{i1} AND...ANDx_j ISA_{ij} AND...ANDx_{im} ISA_{im}, THEN$$

$$y = c_{i0} + \sum_{j=1}^{m} (c_{ij} x_j), j = 1,...,n$$

На основании результатов проведенного в работе анализа была сформирована базы правил для оценки эффективности СЗИ, фрагмент которой представлен ниже:

$$R_m : "REG\_NUM"(C) AND УБИ."BDU\_NUM"(H) ANDCOST(MIN) THENEVALSZI(Д)$$
$$R_{m+1} : "REG\_NUM"(C) AND УБИ."BDU\_NUM"(H) ANDCOST(MAX) THENEVALSZI(Д)$$
$$R_{m+2} : "REG\_NUM"(C) AND УБИ."BDU\_NUM"(HH) ANDCOST(MIN) THENEVALSZI(НД)$$
$$R_{m+3} : "REG\_NUM"(C) AND УБИ."BDU\_NUM"(HH) ANDCOST(MAX) THENEVALSZI(НД)$$
$$R_{m+4} : "REG\_NUM"(ЦС) AND УБИ."BDU\_NUM"(H) ANDCOST(MIN) THENEVALSZI(Д)$$
$$R_{m+5} : "REG\_NUM"(ЦС) AND УБИ."BDU\_NUM"(H) ANDCOST(MAX) THENEVALSZI(Д)$$
$$R_{m+6} : "REG\_NUM"(ЦС) AND УБИ."BDU\_NUM"(HH) ANDCOST(MIN) THENEVALSZI(НД)$$
$$R_{m+7} : "REG\_NUM"(ЦС) AND УБИ."BDU\_NUM"(HH) ANDCOST(MAX) THENEVALSZI(НД)$$
$$R_{m+8} : "REG\_NUM"(ЧС) AND УБИ."BDU\_NUM"(H) ANDCOST(MIN) THENEVALSZI(Д)$$
$$R_{m+9} : "REG\_NUM"(ЧС) AND УБИ."BDU\_NUM"(H) ANDCOST(MAX) THENEVALSZI(НД)$$
$$R_{m+10} : "REG\_NUM"(ЧС) AND УБИ."BDU\_NUM"(HH) ANDCOST(MIN) THENEVALSZI(НД)$$
$$R_{m+11} : "REG\_NUM"(ЧС) AND УБИ."BDU\_NUM"(HH) ANDCOST(MAX) THENEVALSZI(НД)$$
$$R_{m+12} : "REG\_NUM"(H) AND УБИ."BDU\_NUM"(H) ANDCOST(MIN) THENEVALSZI(Д)$$
$$R_{m+13} : "REG\_NUM"(H) AND УБИ."BDU\_NUM"(H) ANDCOST(MAX) THENEVALSZI(НД)$$
$$R_{m+14} : "REG\_NUM"(H) AND УБИ."BDU\_NUM"(HH) ANDCOST(MIN) THENEVALSZI(НД)$$
$$R_{m+15} : "REG\_NUM"(H) AND УБИ."BDU\_NUM"(HH) ANDCOST(MAX) THENEVALSZI(НД)$$

где, «REG_NUM» – идентификатор меры из требований по ИБ (требований приказов ФСТЭК России), «BDU_NUM» – идентификатор УБИ (БДУ ФСТЭК России), «COST» – стоимость СрЗИ. Терм-множествами лингвистических переменных являются следующие: «С» – соответствует, «ЦС» – в целом соответствует, «ЧС» – частично соответствует, «Н» – не соответствует, «Н» – УБИ нейтрализована, «НН» – УБИ не нейтрализована, «min» – цена СЗИ минимальная, «max» – цена СЗИ максимальная. Оценка эффективности: «Д» – достигается, «НД – не достигается.

Стоимость средств защиты информации определяется на основе данных производителей (вендоров). В качестве данных для набора используются прайс-литы.

Количественные значения лингвистических переменных устанавливаются экспертами на этапе формирования базы правил и установления порогового

значения достижения необходимого уровня защищенности системы (эффективности СЗИ). Значения формируются по результатам определения рисков и негативных последствий от их наступления для владельца ТРИС.

С помощью технологий Data Science был сформирован набор данных для реализации метода.

Предложенный метод базируется на следующих положениях:

– входные переменные являются четкими;

– функции принадлежности (ФП) определены функцией Гаусса:

$$\mu_{A_{ij}}(x_j) = \exp(-\frac{1}{2}(\frac{x_j - a_{ij}}{b_{ij}})^2),$$

где x_j – входные сети a_{ij}, b_{ij} – настраиваемые параметры ФП.

– нечеткая импликация Ларсена – нечеткое произведение;

– Т-норма – нечеткое произведение;

– композиция не производится;

– метод дефаззификации – метод центроида.

Функциональная зависимость после дефаззификации для получения выходной переменно принимает следующий вид:

$$y' = \frac{\Sigma_i^n((c_{i0} + \Sigma_{j=1}^m c_{ij}x_j)\Pi_j^m \mu_{A_{ij}}(x_j'))}{\Sigma_{i=1}^n \Pi_j^m \mu_{A_{ij}}(x_j')} = \frac{\Sigma_i^n((c_{i0} + \Sigma_{j=1}^m c_{ij}x_j))\Pi_j^m \exp\left[-(\frac{x_j' - a_{ij}}{b_{ij}})^2\right]}{\Sigma_{i=1}^n \Pi_j^m \exp\left[-(\frac{x_j' - a_{ij}}{b_{ij}})^2\right]} \quad (1)$$

Выражение 1 лежит в основе сети ANFIS с применением алгоритма TSK, которая включает в себя пять слоев.

Выходную переменную из выражения (1) представляем в следующем виде:

$$y' = \sum_{i=1}^n w_i'(c_{i0} + \sum_{j=1}^m c_{ij}x_j),$$

где

$$w_i' = \frac{\Pi_{j=1}^m \mu_{A_{ij}}(x_j')}{\sum_{i=1}^n \Pi_j^m \mu_{A_{ij}}(x_j')} = \frac{\Pi_j^m \exp\left[-(\frac{x_j' - a_{ij}}{b_{ij}})^2\right]}{\sum_{i=1}^n \Pi_j^m \exp\left[-(\frac{x_j' - a_{ij}}{b_{ij}})^2\right]} = const.$$

При K обучающих примерах $x_1^{(k)}, x_2^{(k)}, ..., x_m^{(k)}, y^{(k)}$, где $k=1,...,K$ и замене значений выходных переменных $y'^{(k)}$ значениями эталонных переменных $y^{(k)}$, получим систему из K линейных уравнений вида:

$$\begin{bmatrix} w_1^{'(1)} & w_1^{'(1)}x_1^{(1)} & \dots & w_1^{'(1)}x_m^{(1)} & \dots & w_n^{'(1)} & w_n^{'(1)}x_1^{(1)} & \dots & w_n^{'(1)}x_m^{(1)} \\ w_1^{'(2)} & w_1^{'(2)}x_1^{(2)} & \dots & w_1^{'(2)}x_m^{(2)} & \dots & w_n^{'(2)} & w_n^{'(2)}x_1^{(2)} & \dots & w_n^{'(2)}x_m^{(2)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ w_1^{'(k)} & w_1^{'(k)}x_1^{(k)} & \dots & w_1^{'(k)}x_m^{(k)} & \dots & w_n^{'(k)} & w_n^{'(k)}x_1^{(k)} & \dots & w_n^{'(k)}x_m^{(k)} \end{bmatrix} x \begin{bmatrix} c_{10} \\ \dots \\ c_{1m} \\ \dots \\ c_{n0} \\ \dots \\ c_{nm} \end{bmatrix} = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \dots \\ y^{(k)} \end{bmatrix}, \quad (2)$$

где $w_i^{'(k)}$ агрегированная степень истинности предпосылок по i -му правилу при предъявлении k -го входного вектора $(x_1^{(k)}, x_2^{(k)}, ..., x_m^{(k)})$.

Таким образом, (2) в сокращенном виде:

$$W \times c = y .$$

Размерность матрицы W равна $K \times (m+1)n$, при этом, как правило, количество строк k значительно больше количества столбцов: $K \times (m+1)n$.

По результатам уточнения нелинейных параметров процесс адаптации нейрона запускался до тех пор, пока не достиг повторения результатов. Алгоритм является гибридным, его особенность заключается в разделении этапов обучения. Такой алгоритм является наиболее эффективным, что и позволило достичь наилучшего результата.

Итоговая оценка эффективности СЗИ рассчитывается по формуле:

$$W = \frac{\sum_{j=1}^{m} X_j}{m} \quad (3),$$
$$0 \le W \le 1,$$

где X_j – выполнение требований одного из показателей оценки эффективности СЗИ, $j = 1, m$; m – перечень показателей.

С учетом важности выполнения требований оценка эффективности СЗИ рассчитывается следующим образом:

$$W = \sum_{j=1}^{m} x_j a_j ,$$
$$0 \le W \le 1,$$

где a_j – коэффициент важности требования, $0 \le a \le 1$, $\sum_{j=1}^{m} a_j = 1$.

Пример расчета оценки эффективности СЗИ на основе предложенного метода:

экспертным путем определяются оценки соответствия по требованиям ИБ (значения терм-множеств, описанных выше, условно равны 0; 0,3; 0,5; 0,7; 1, соответственно).

То есть,

$$A=\begin{bmatrix}0,7 & 1 & 1 & 1 & 0,7\\ 1 & 1 & 1 & 0,5 & 0,5\\ 0,5 & 0,7 & 1 & 0,7 & 0,5\\ 0,7 & 1 & 1 & 0,7 & 0,5\\ 0,7 & 0,7 & 1 & 0,7 & 0,7\end{bmatrix}=\begin{bmatrix}0,88\\ 0,8\\ 0,68\\ 0,78\\ 0,76\end{bmatrix}=0,78$$

На основании результатов определения перечня актуальных УБИ и предполагаемых технических решений СЗИ ТРИС итоговая оценка эффективности СЗИ исследуемой ТРИС для перечня из 5 УБИ, 5 требований по ИБ и 5 СрЗИ рассчитывается в соответствии с (3):

$$W=(\frac{1+0+1+1+0}{5}+\frac{0,72+0,88+1+0,72+0,58}{5}+\frac{1+0+0+0+1}{5})/3=$$
$$=(0,6+0,78+0,4)/3=0,59$$

Для исследуемой ТРИС условно допустимым значением о достижении эффективности СЗИ, считается 0,85. Значение рассчитано, исходя из определенных рисков (киберрисков) в компании. Таким образом, текущая эффективность СЗИ (уровень защищенности системы) не соответствует заявленной владельцем ТРИС, т.е. эффективность СЗИ не достигается при условленной приемлемой для владельца ТРИС значения (квантиля). Результаты проведенной оценки были проанализированы и даны рекомендации по достижению приемлемого уровня защищенности исследуемой ТРИС.

Результатам проведенной оценки показали не эффективность предлагаемых решений по защите информации, а именно:

– проектные решения не учитывают нейтрализацию всех актуальных УБИ в ТРИС;

– эффективность СЗИ ТРИС можно повысить за счет уменьшения стоимости планируемых к закупке СрЗИ.

Для нейтрализации УБИ.121, УБИ.122, УБИ.124 в существующей СЗИ ТРИС не предусмотрены меры по защите информации, для части СрЗИ возможно уменьшение стоимости. Выводы по причинам не соответствия эффективности СЗИ заданному значению определяются по результатам выявления наихудших значений показателей в предложенном методе.

Результаты проведения оценки эффективности СЗИ ТРИС позволяют внести корректировки в проектные решения по СЗИ а раннем этапе, что позволяет предотвратить возможные риски утечки данных и снизить финансовые затраты на создание СЗИ.

Графики результатов экспериментов представлены на рисунке 1.

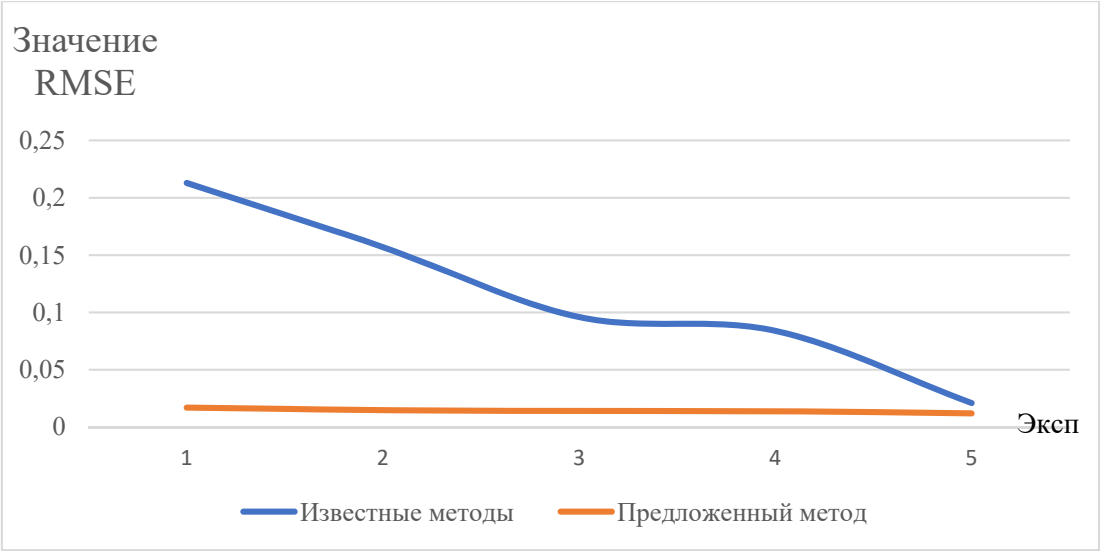

Рисунок 1 – Графики результатов экспериментов

Анализ оценки эффективности предложенного метода представлен в таблице 3.

Таблица 3 – Анализ оценки эффективности предложенного метода

Показатель	**Известные методы**	**Предложенный метод**
RMSE	0,021 – 0,213	0,012 – 0,017
Эффективность СЗИ	85,7 %	97 %
Стоимость СЗИ	снижение до 15%	снижение до 30%

RMSE достигает значения в диапазоне 0,012-0,017, что является локальным минимумом на заданном интервале и позволяет доказать выполнение поставленной в настоящем диссертационном исследовании задачи.

В четвертой главе предложены методические рекомендации по оценке эффективности СЗИ ТРИС, в отличие от известных, позволяющие владельцам ТРИС в режиме реального времени выполнять оценку эффективности СЗИ, снижать финансовые затраты на создание СЗИ от 15 до 30%, сокращать количество не учтенных актуальных УБИ на 5%. Методические рекомендаций не требует привлечения высококвалифицированных специалистов по ИБ, больших вычислительных ресурсов. Эффективность СЗИ в ТРИС достигает до 97%.

Предложенные методические рекомендации позволяют:

– учитывать все аспекты процесса проведения оценки эффективности СЗИ ТРИС;

– минимизировать количество этапов оценки;

– учитывать требования регуляторов в области обеспечения ИБ;

– могут быть адаптированы под конкретные условия владельцев ТРИС;

– процесс автоматизирован, исключает недостатки экспертных методов, не требует привлечения высококвалифицированных специалистов в области ИБ.

Оценка эффективности СЗИ ТРИС в соответствии с предложенными рекомендациями состоит из следующих шагов:

1. Проводится обследование ТРИС, по результатам которого формируется протокол, включающий в себя описание бизнес-процессов; перечень информации, обрабатываемой системой; описание групп пользователей, их прав и полномочий; описание технологии обработки информации; описание ИТ-инфраструктуры, а также существующей СЗИ.

2. Определение перечня актуальных УБИ в соответствии с методическими документами регуляторов и на основании БДУ ФСТЭК России (MITRE ATT&CK, CVE, CWE, OSVDB, NVD, Secunia). Определяется тип и класс, уровень защищенности, категория значимости ТРИС. Перечень актуальных УБИ формируются на основе предложенной в настоящем диссертационном исследовании методики определения актуальных УБИ.

3. Формируется перечень требований по защите информации на основании классификации и перечня актуальных УБИ.

4. Формируется набор данных, включающий в себя: сведения об ИТ-инфраструктуре ТРИС, перечень актуальных УБИ в ТРИС, перечень требований по защите информации, перечень возможных к использованию средств защиты информации в СЗИ ТРИС, их стоимость. С помощью технологий Data Science набор данных очищается и преобразуется.

5. Формируются экспертные оценки соответствия ТРИС по требованиям защиты информации (терм-множества лингвистических переменных).

6. На основании предложенного метода оценки эффективности СЗИ рассчитывается уровень защищенности ТРИС (программа для ЭВМ «Оценка системы защиты информации).

7. На основании результатов оценки эффективности СЗИ ТРИС при необходимости вносятся корректировки в проектные решения по защите информации.

Структурная схема проведения оценки эффективности СЗИ ТРИС представлена на рисунке 2.

Процесс проведении оценки эффективности состоит из пяти подсистем:

1. Подсистема обследования ТРИС.
2. Подсистема моделирования УБИ.
3. Подсистема формирования требований по защите информации.
4. Подсистема оценки эффективности СЗИ ТРИС.
5. Подсистема корректировки проектных решений по СЗИ ТРИС.

Такое разбиение на подсистемы обусловлено независимостью друг от друга каждой из них, что, в свою очередь, позволяет вносить корректировки в процессе

проведения оценки эффективности СЗИ ТРИС без внесения изменений в смежные подсистемы.

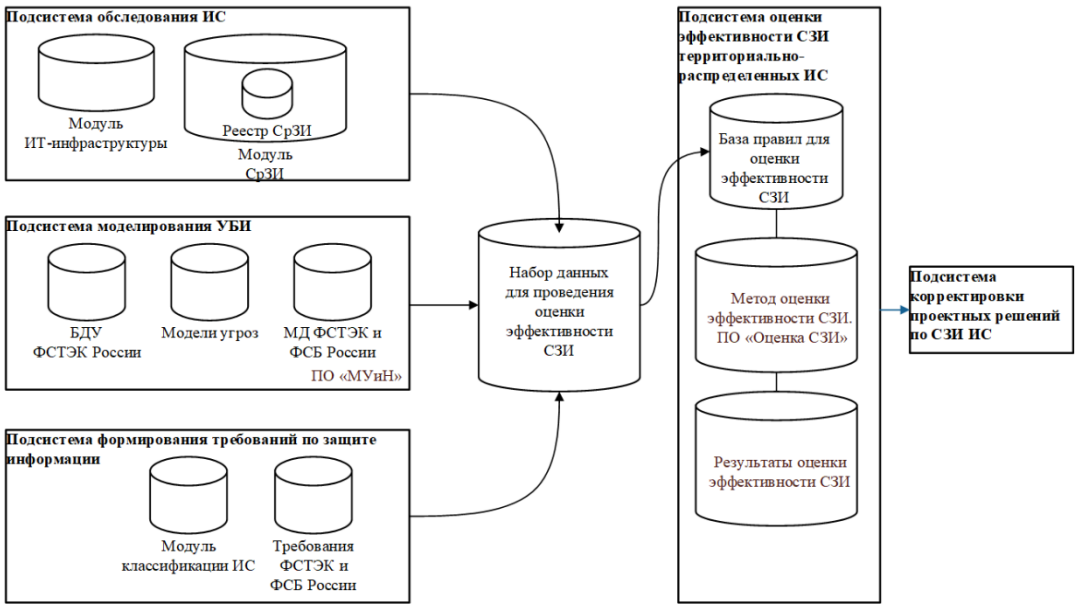

Рисунок 2 – Структурная схема проведения оценки эффективности СЗИ ТРИС

ЗАКЛЮЧЕНИЕ

Поставленная в диссертационном исследовании цель по повышению качества оценки эффективности систем защиты информации территориально-распределенных информационных систем за счет определения необходимых и достаточных показателей **достигнута**.

Для достижения цели были поставлены и выполнены задачи, получены научные результаты, составляющие следующие итоги исследования:

1. Проведен анализ ТРИС: определены основные бизнес-процессы; информация, обрабатываемая в ТРИС; группы пользователей, имеющих доступ в ТРИС, их права и полномочия; выявлены основные аспекты технологии обработки информации; исследована ИТ-инфраструктура ТРИС (информационные технологий и программное обеспечение, реализующее бизнес-процессы ТРИС); проведен анализ атак и угроз безопасности информации в ТРИС, требований по защите информации в ТРИС; проведен анализ СЗИ ТРИС; анализ существующих методов и методик моделирования УБИ и оценки эффективности СЗИ ТРИС.

2. Предложена методика определения актуальных угроз безопасности информации, в отличие от известных, позволяющая в автоматизированном режиме формировать перечень актуальных УБИ, гипотетически исключая ошибки экспертов. Позволяющая определять большее количество актуальных УБИ, минимизировать трудоемкость процесса и вычислительные ресурсы.

3. Предложен метод оценки эффективности систем защиты информации, в отличие от известных, основанный на теории адаптивных нечетких нейронных продукционных системах и алгоритме нечеткого вывода Такаги-Сугено-Канга с применением технологий Data Science. Метод позволяет проводить оценку эффективности СЗИ на основе необходимых и достаточных показателей, определенных в настоящем диссертационном исследовании. RMSE работы системы ANFIS достигает наименьшего значения, что позволяет утверждать об эффективности работы метода и о достижении поставленной задачи.

4. Разработаны методические рекомендации по оценке эффективности систем защиты информации в территориально-распределенных информационных системах, в отличие от известных, позволяющие владельцам ТРИС в режиме реального времени выполнять оценку эффективности СЗИ, снижать финансовые затраты на создание системы защиты информации от 15 до 30%, сокращать количество не учтенных актуальных угроз безопасности информации на 5%. Использование методических рекомендаций не требует привлечения высококвалифицированных специалистов по информационной безопасности, больших вычислительных ресурсов, эффективность систем защиты информации в территориально-распределенных информационных системах достигает до 97%.

Разработанные методические рекомендации позволяют:

– учитывать все аспекты процесса проведения оценки эффективности СЗИ ТРИС;

– минимизировать количество этапов оценки;

– учитывать требования регуляторов в области обеспечения ИБ;

– могут быть адаптированы под конкретные условия владельцев ТРИС;

– процесс автоматизирован, исключает недостатки экспертных методов, не требует привлечения высококвалифицированных специалистов в области ИБ.

5. Проведена оценка эффективности предложенных методики и метода.

Доказано, что предложенные методика и метод обладают большей эффективностью для решения задач, связанных с определением перечня актуальных УБИ и оценки эффективности СЗИ за счет определения необходимых и достаточных показателе. Определены наилучшие параметры работы адаптивной нечеткой нейронной продукционной системы с алгоритмом нечеткого вывода. Применены технологии Data Science при обработке большого объема данных.

Эффективность предложенных методики и метода подтверждается:

– достоверными результатами определения перечня актуальных угроз безопасности информации и достижения эффективности СЗИ;

– отсутствием необходимости привлечения высококвалифицированных специалистов в области ИБ;

– возможностью адаптации под конкретные цели владельцев ИС при проведении оценки эффективности СЗИ: выбором показателей, путем изменения параметров работы системы ANFIS и выбора алгоритма нечеткого вывода.

СПИСОК РАБОТ ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых изданиях из перечня ВАК при Минобрнауки России:

1. Миняев А.А. Моделирование угроз безопасности информации в территориально-распределенных информационных системах // Наукоемкие технологии в космических исследованиях Земли. – 2021. № 2. – С 52-65.

2. Миняев А.А. Метод и методика оценки эффективности системы защиты территориально-распределенных информационных систем // Информатизация и связь, 2020, № 6. С. 29-36.

3. Миняев А.А., Красов А.В., Сахаров Д.В. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник СПГУТД. № 1. 2020. С. 29-33.

4. Миняев А.А., Красов А.В. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник СПГУТД. № 3. 2020. С. 26-32.

5. Миняев А.А., Будько М.Ю. Метод оценки эффективности системы защиты информации территориально распределенных информационных систем // Информатизация и связь. 2017. № 3, С. 119-121.

6. Миняев А.А., Будько М.Ю. Метод оценки эффективности системы защиты персональных данных // Информатизация и связь, 2016, № 2. С. 85-87.

В изданиях, индексируемых Web of Science и Scopus:

7. Minyaev A. Andrey, Krasov V. Andrey, Saharov V. Dmitriy. The Method and Methodology of efficiency assessment of protection system of distributed information systems // Institute of Electrical and Electronics Engineers – 2020, pp. 291-295.

8. I.I. Livshitz, D.V. Yurkin, A.A. Minyaev. Formation of the Instantaneous Information Security Audit Concept // Communications in Computer and Information Science – 2016, Vol. 678, pp. 314-324.

Свидетельства о государственной регистрации программ для ЭВМ:

9. Свидетельство о государственной регистрации программы для ЭВМ 2020617876 Российская Федерация. Модель угроз и нарушителя / **Миняев А.А.**, Красов А.В., Пешков А.И.; заявитель и правообладатель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ) – № 2020616749; заявл. 29.06.2020; опубл. 15.07.2020.

10. Свидетельство о государственной регистрации программы для ЭВМ 2020664343 Российская Федерация. Оценка систем защиты информации / **Миняев А.А.**, Красов А.В., Пешков А.И.; Ушаков И.А.; заявитель и правообладатель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский

государственный университет телекоммуникаций им. проф. М.А. Бонч - Бруевича» (СПбГУТ) – № 2020663630; заявл. 03.11.2020; опубл. 11.11.2020.

В других изданиях:

11. Миняев А.А. Разработка системы защиты информации территориально-распределенных информационных систем // X Юбилейная Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: Сборник научных статей, СПбГУТ, 2021. С. 597-600.

12. Миняев А.А., Карельский П.В., Ковцуп М.М. Особенности развертывания Security Operations Center при организации удаленного доступа к инфраструктуре компании // X Юбилейная Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: сборник научных статей, СПбГУТ, 2021. С. 433-437.

13. Ковцур М.М., Миняев А.А., Потемкин П.А., Хамза Д.Д. Обеспечение информационной безопасности Web-приложений с использованием машинного обучения // IX Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: сборник научных статей, СПбГУТ, 2020. С. 597-601.

14. Миняев А.А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // IX Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: сборник научных статей, СПбГУТ, 2020. С. 716-719.

15. Миняев А.А., Будько М.Ю. Методика оценки эффективности системы защиты персональных данных информационной системы // Проблемы комплексного обеспечения информационной безопасности и совершенствование образовательных технологий подготовки специалистов силовых структур: Межвузовский сборник трудов VI Всероссийской научно-технической конференции (ИКВО НИУ ИТМО, 10 декабря 2015 г.), 2016. С. 43-45.

16. Minyaev A.A., Livshitz I.I., Yurkin D.V. Method of assessment of efficiency of the system of protection of personal data // Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь (DCCN-2017, Москва, 25–29 сентября 2017 г.), 2017. С. 552-555.

Подписано в печать 29.09.2021. Формат 60×84 1/16.
Печ. л. 1,0. Тираж 100 экз.

Отпечатано в СПбГУТ, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1