МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский технический университет связи и информатики»
(МТУСИ)

Федеральное учебно-методическое объединение в сфере высшего образования по УГСНП 10.00.00 «Информационная безопасность»
(ФУМО ВО ИБ)

18-21 октября 2022 г.

II ВСЕРОССИЙСКАЯ НАУЧНАЯ ШКОЛА-СЕМИНАР

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ МЕТОДОВ И ТЕХНОЛОГИЙ ЗАЩИТЫ ИНФОРМАЦИИ

СБОРНИК ТРУДОВ

Москва – 2022

Сборник трудов II Всероссийской научной школы-семинара «Современные тенденции развития методов и технологий защиты информации». Москва, МТУСИ, 18-21 октября 2022 г. – М.: ООО «Брис-М», 2022. – 366 с.

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ:

Леохин Ю.Л., доктор технических наук, профессор, проректор по научной работе МТУСИ, председатель;

Белов Е.Б., заместитель председателя ФУМО ВО ИБ, заместитель председателя;

Лось В.П., доктор военных наук, профессор, президент МОО «Ассоциация защиты информации»;

Новиков С.Н., доктор технических наук, доцент, заведующий кафедрой «Безопасность и управление в телекоммуникациях» СибГУТИ;

Киреева Н.В., кандидат технических наук, доцент, декан факультета «Телекоммуникации и радиотехника» ПГУТИ;

Красов А.В., кандидат технических наук, доцент, заведующий кафедрой «Защищенные системы связи» СПбГУТ;

Безумнов Д.Н., начальник ОРОП МТУСИ, секретарь.

СОДЕРЖАНИЕ

РАЗДЕЛ 1. НАУЧНЫЕ ДОКЛАДЫ ГРАНТОПОЛУЧАТЕЛЕЙ 2021 ГОДА – СОИСКАТЕЛЕЙ УЧЁНОЙ СТЕПЕНИ ДОКТОРА НАУК

Баранов В.В.
ЮРГПУ(НПИ),
заведующий кафедрой
«Информационная безопасность»,
к.в.н, доцент
baranov.vv.2015@yandex.ru

МЕТОДОЛОГИЯ И АВТОМАТИЗАЦИЯ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ РАЗРАБОТКЕ И ОЦЕНКЕ ЭФФЕКТИВНОСТИ КОМПЛЕКСА МЕР ЗАЩИТЫ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация: в работе проведено обоснование необходимости создания информационной системы поддержки принятия решений (ИСППР) в области информационной безопасности (ИБ), проведен анализ существующих таких систем в области управления и методов их разработки, разработана трехуровневая модель функционирования РИС в условиях деструктивного воздействия, разработаны онтологические структурно-функциональные модели информационных модулей РИС, деструктивного воздействия и защитных мероприятий, разработана нейро-байесовская модель, позволяющая моделировать взаимосвязи событий информационной безопасности, разработан методический аппарат для проведения расчетов совместного распределения вероятностей защитных и деструктивных событий, разработаны структура, архитектура, алгоритмы и осуществлена программная реализация ИСППР, а также проведены эксперименты, подтверждающие ее работоспособность.

Ключевые слова: поддержка принятия решений, нейро-байесовская сеть, деструктивные воздействия, меры защиты информации, угрозы безопасности информации, онтологическая модель, методики, алгоритмы.

Актуальность темы исследования. Переход к цифровой экономике не возможен без решения проблемы создания современной защищенной информационной инфраструктуры государства.

Ее успешное решение связано с необходимостью разработки в условиях нечетких исходных данных эффективных систем защиты (СЗ) для распределенных информационных систем (РИС) и обеспечения их надежного функционирования в условиях деструктивных воздействий (ДВ).

Наиболее сложным аспектом в процессе решения данной проблемы является обеспечение требуемого уровня достоверности результатов моделирования действий нарушителей, выявления уязвимостей защищаемых активов, определения актуальных угроз безопасности информации (УБИ), а также при выборе комплекса мер и средств защиты информации (СЗИ).

На этапе функционирования, в условиях динамично меняющегося ДВ, система защиты требует непрерывного оперативного управления (ОУ), своевременного и обоснованного реагирования на вновь возникающие риски и УБИ.

Существующие организационно-руководящие (ОРД) и методические документы (МД) регуляторов в области ИБ предписывают решение данных задач методом экспертной оценки [1,2,3].

Такой подход определяет ту, или иную степень субъективности принимаемых решений, качество которых зависит от полноты исходных данных, сложности структуры РИС, а также уровня подготовки экспертов.

Следует отметить, что автору неизвестны системно увязанные динамические модели, методический аппарат, а также реализующие их алгоритмы и системное ПО, которые применялись бы для поддержки принятия решений (ППР) в задачах разработки и оценки эффективности защиты РИС на всех этапах их жизненного цикла.

Слабо изучены закономерности формирования типовых цепочек событий ИБ: «Тип нарушителя - Возможности нарушителя - Способ реализации УБИ»; «Техники реализации УБИ – Тип уязвимости - Актив».

Не исследовано взаимное влияние между сценариями, тактиками (техниками) реализации УБИ и структурно-функциональными характеристиками РИС [1,4,5].

Все вышесказанное определяет актуальность темы данного исследования.

Исследование находится на завершающей стадии разработки, выполнено более 80% запланированного объема.

Целью научного исследования является: создание комплекса моделей, системного методического аппарата, алгоритмов и их программной реализации, обеспечивающих автоматизацию процесса ППР при разработке, оценке эффективности мер защиты РИС, в ходе ОУ СЗИ с требуемой степенью достоверности, полноты и качества.

Для достижения поставленной цели были решены следующие задачи:

1. Проведен анализ возможных путей решения проблемы разработки моделей, методик и алгоритмов СППР в области ИБ.
2. Предложены показатели качества и критерии оценки защищенности РИС в условиях ДВ.
3. Разработана методология формирования комплекса интегрированных моделей функционирования РИС в условиях ДВ.
4. Разработана комплексная динамическая модель ОУ защищенными РИС в условиях ДВ.
5. Разработан комплекс методик и алгоритмов, реализуемых для ППР при формировании и оценке их эффективности мер по защите РИС в условиях ДВ.
6. Разработана СППР при формировании и оценке эффективности комплекса мер по защите РИС в условиях ДВ.
7. Проведены эксперименты, подтверждающие достоверность, научную ценность и практическую значимость полученных результатов исследования.

Научная новизна исследования заключается в том, что впервые на системном уровне предложена концепция и методология формирования и оценки эффективности комплекса МЗИ РИС, позволяющие реализовать процесс ППР в задачах управления событиями ИБ.

Научная значимость работы состоит в развитии теории и методологии обеспечения ИБ в части создания новых и совершенствования существующих методов, моделей и алгоритмов ППР при формировании и оценки эффективности комплекса мер по защите РИС в условиях ДВ, учитывающие взаимосвязи применяемых МЗИ от способов, техник и сценариев реализации УБИ, структуры РИС, типов уязвимостей.

Практическая значимость результатов исследования заключается в их использовании в деятельности организаций, осуществляющих проведение аттестаций РИС, что подтверждается актами о внедрении. Применение результатов исследования позволяет значительно сократить, сроки проведения работ по формированию модели УБИ, разработке и выбору МЗИ, СЗИ, режимных мероприятий, оформлению отчетных документов, повысить степень обоснованности принятых решений и достоверности результатов оценки защищенности РИС.

Прикладная направленность исследования состоит в использовании ее положений при разработке МД, выполнении НИР, а также в учебном процессе при подготовке и переподготовке специалистов по ЗИ.

Для решения поставленных задач были использованы методы системного анализа, теории принятия решений, методы онтологий, байесовских сетей, тории ближайшего соседа, теории систем управления, нечетких множеств, теории вероятности, методы получения интегральных оценок, теории дифференциального исчисления и численных методов.

Положения, выносимые на защиту.

1. Комплекс интегрированных онтологических структурно – функциональных моделей (ОС-ФМ) информационного модуля (ИМ), ДВ и защитных мероприятий. Данные модели позволяют определить структурно – функциональные взаимосвязи между объектами потенциального воздействия (концептами) на пяти уровнях ИМ РИС: аппаратном, сетевом, системном, прикладном и пользовательском, их уязвимостями, защитными мероприятиями и сценариями УБИ. Соответствует п.9,10 паспорта специальности 2.3.6.
2. Нейро-байесовская модель (НБМ) защищенных РИС впервые позволяет на системном уровне моделировать кластеры ДВ на защищенные РИС и кластеры формирования МЗИ, а также осуществлять выявление уязвимостей защищаемых активов, проводить оценку актуальности УБИ, предпочтительности сценариев и техник их реализации, выбор необходимых МЗИ и способов ОУ функционированием подсистемы защиты РИС в условиях ДВ. Соответствует п.9,10 паспорта специальности 2.3.6.
3. Комплекс методик и алгоритмов ППР при разработке мер по защите РИС в условиях ДВ. Разработанный методический подход впервые позволил определять вероятностные характеристики сценариев, тактик и техник реализации УБИ, разрабатывать способы реализации ОМ и ТМ, проводить оценку их эффективности для складывающихся условий

и способы ОУ подсистемой защиты РИС в условиях ДВ. Соответствует п.9,10 паспорта специальности 2.3.6.

4. Методика и алгоритмы разработки ПО для СППР при формировании комплекса мер по защите и ОУ РИС. Впервые применена интеграция алгоритмов, реализующих ОС-ФМ и НБМ защищенной РИС, методики расчета численных значений показателей и их оценку, а также использование необходимых баз данных. Соответствует п.2 паспорта специальности 2.3.6.
5. ПО СППР при разработке комплекса мер по защите РИС и оценки их эффективности. Впервые в области ЗИ реализована трехуровневая СППР. На когнитивном уровне осуществляется ввод ИД и формируются экспертный и инструментальный (машинный) варианты оценки событий ИБ и предлагаемых действий. На втором уровне производится их сравнение и оптимизация. На третьем уровне формируется оптимизированное решение по реагированию на складывающуюся ситуацию, осуществляется его документирование и генерируются варианты решений для ОУ защищенной РИС. Соответствует п.2, 18 паспорта специальности 2.3.6.

Достоверность и обоснованность научных положений, результатов и выводов работы обеспечивается многосторонним анализом современного состояния исследований в предметной области, системным обоснованием предложенных методов, моделей и алгоритмов, не противоречащих известным положениям других авторов, достаточной апробацией полученных результатов в научных публикациях и докладах на международных и российских научных и НПК, а также подтверждается положительным эффектом от внедрения в практику в ряде организаций, работающих в области ЗИ и осуществляющих подготовку соответствующих специалистов.

Апробация результатов работы. Результаты исследования докладывались на X Всероссийская НТК «Синтез и прикладная синергетика»; IV International Scientific Conference "MIST: Aerospace-IV 2021: Advanced Technologies in Aerospace, Mechanical and Automation Engineering" held in Krasnoyarsk, Russia, December (2021г.); Всероссийская НТК «Теория и практика обеспечения информационной безопасности» (2021г.); Всероссийская НТК «Состояние и перспективы развития современной науки по направлению «ИТ-технологий» (2022 г.); XVII Всероссийской НПК «Информационная безопасность цифровой экономики» (2022 г.) и на других форумах.

Было опубликовано и принято к публикации 8 статей в рецензируемых журналах из перечня ВАК, 3 статьи в изданиях, индексируемых Scopus, оформлено 4 свидетельства о государственной регистрации программ для ЭВМ.

Реализация результатов работы. Разработанные в научном исследовании модели, методы и алгоритмы использовались при выполнении НИР и НИОКР: НИР на специальную тему шифр «Восход-30», СПб.: ВАС инв. № 9714, 2021 г.; НИР на специальную тему шифр «Атмосфера-2050», СПб.: ВАС инв. № 9711, 2021 г.

Внедрение. Результаты работы внедрены в практическую деятельность НТЦ ФГУП «НПП "Гамма"»; ЗАО «Институт сетевых технологий»; ООО «Региональный экспертно-аттестационный центр «Эксперт» в учебный процесс Военной академии связи имени С.М. Буденного; ЮРГПУ (НПИ).

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Введение. Обоснована актуальность темы исследования, дана ее краткая характеристика, сформулированы проблема, цель и задачи исследования, определены объект и предмет исследования, приведены положения, выносимые на защиту, аргументированы научная ценность и практическая значимость, представлены данные об апробации и результатах внедрения, изложено краткое содержание разделов.

В первой главе проведен анализ научных работ по теме исследования, руководящих и методических документов регуляторов в области ИБ по вопросам моделирования защищенных РИС, моделирования УБИ, разработки ИСППР в различных областях управления.

Анализ системных взаимосвязей между регулятивными, методологическими и техническими аспектами разработки и оценки эффективности способов защиты РИС позволил выделить основные нормативные документы, определяющие виды РИС [1,2,6,7,8,9,10,11]. (Рис.1)

Анализ содержания вышеуказанных документов позволил сделать следующий вывод – все МЗИ можно разделить на однотипные модули, которые будут применены в алгоритмах моделей защищенных РИС.

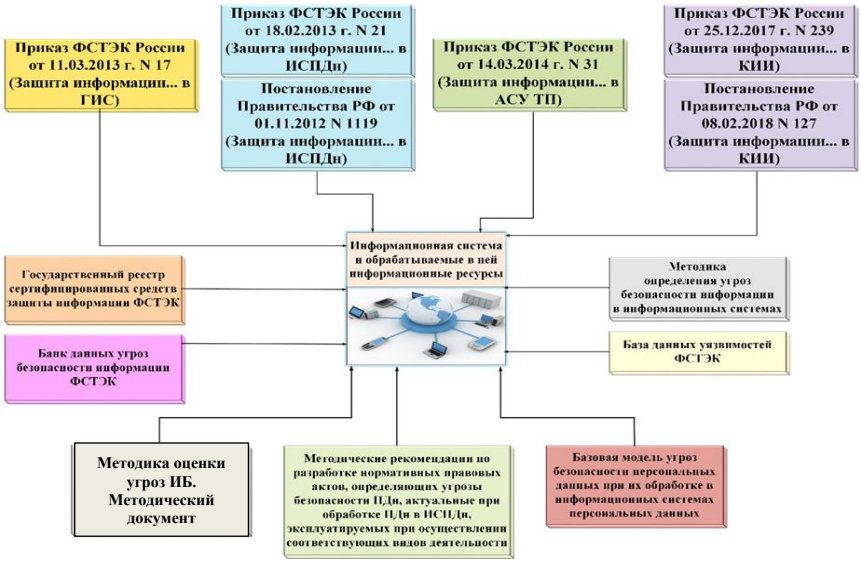


Рис. 1. Нормативно-правовое обеспечение защиты информации в РИС

Разные способы различных УБИ будут иметь уникальное сочетание тактик и техник реализации, представляющие собой сценарии. Данный аспект требует изучения, систематизации и разработки математического аппарата для применения в моделях ДВ.

Объекты воздействия УБИ определяются на аппаратном, сетевом, системном, прикладном и пользовательском уровне, однако их взаимное влияние и показатели безопасности на интегративном уровне не исследованы.

Актуализация УБИ осуществляется экспертным методом в ходе построения модели УБИ, которая включает модель нарушителя. Степень опасности угрозы определяется величиной риска ее реализации и степенью ущерба при ее реализации. Состояние реализации угрозы, приведшее к нанесению ущерба является инцидентом. Подход достаточно субъективен и требует разработки методики на основе математического аппарата [1,2,4,5].

МЗИ предназначены для перекрытия (локализации) актуальных УБИ. МЗИ подразделяются на ТМ, реализуемые СЗИ и ОМ реализуемые режимными мероприятиями на основе разработанных ОРД. Совокупность применяемых ОМ и ТМ представляют собой способ ЗИ в РИС. Частные модели способов защиты представлены в профилях защиты (ПЗ) на сайте ФСТЭК.

Проведенное исследование позволило выделить структуру существующего подхода к разработке способов защиты РИС (Рис.2).

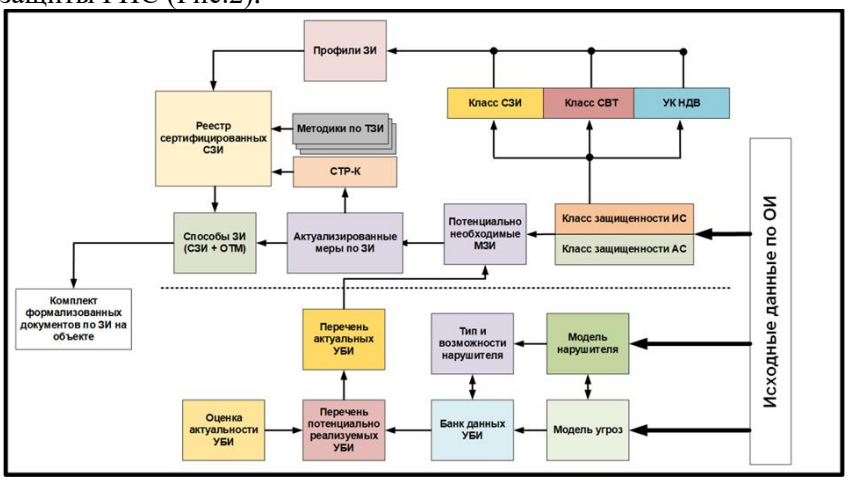


Рис. 2. Структурная схема процесса разработки способов защиты РИС

Анализ существующих комбинированных ИСППР показал, что большинство из них основаны на программных продуктах для работы с байесовскими сетями (БС) [12,13,14]. В работе был проведен анализ ряда наиболее функционально адаптированных к области ИБ программ.

BayesiaLab представляет собой комплексный инструмент для создания и использования байесовских сетей. С помощью пакета BayesiaLab можно определять, изучать, редактировать и анализировать БС модели. [15,16,17].

Программный продукт AgenaRisk сильной стороной которого является возможность работы с различными типами моделей, обучение БС, применение различных типов распределений, а также графическая визуализация при анализе рисков [18,19].

Программный продукт Hugin и его ядро - Hugin Development Environment, объединяет интерфейс для создания и модификации сетевых моделей и СППР с использованием объектно-ориентированных БС. [20,21].

Анализ возможностей указанных программных продуктов позволил выделить их сильные стороны, необходимые для выполнения задачи ППР в области ИБ. Такая ИС должна обладать рядом перечисленных ниже функций.

Функция моделирования.

Функция обработки баз данных (информационно-расчетная функция).

Функция обработки баз знаний (аналитическая функция).

Функция обеспечения коммуникативности.

Функция документирования.

В ходе анализа существующих методов моделирования были выбраны четыре, наиболее подходящих для моделирования процессов разработки и функционирования РИС в условиях ДВ. Это метод онтологий (онтологический инжиниринг) для формирования ситуационных С-ФМ [22,23,24]. Метод БС для формирования НБМ[12,13,26]. Методы ближайших соседей и нечетких множеств для обеспечения требуемой степени достоверности результатов обучения НБМ [25,27,28,29].

Рассмотренные методы, базирующиеся на известных статистических принципах и теоремах, позволяющие определить вероятностные значения событий ИБ в РИС.

Во второй главе представлены основные положения методологии и формализованное описание методов, моделей функционирования РИС в условиях ДВ и критерии оценки эффективности МЗИ, базирующиеся на материалах научных исследований [30,31,32].

Для разработки и исследования моделей, методик и алгоритмом для ИСППР были выбраны показатели качества существенных свойств защищенной РИС и критерии их оценки.

Была разработана трехуровневая комплексная модель функционирования РИС в условиях ДВ (Рис 3).

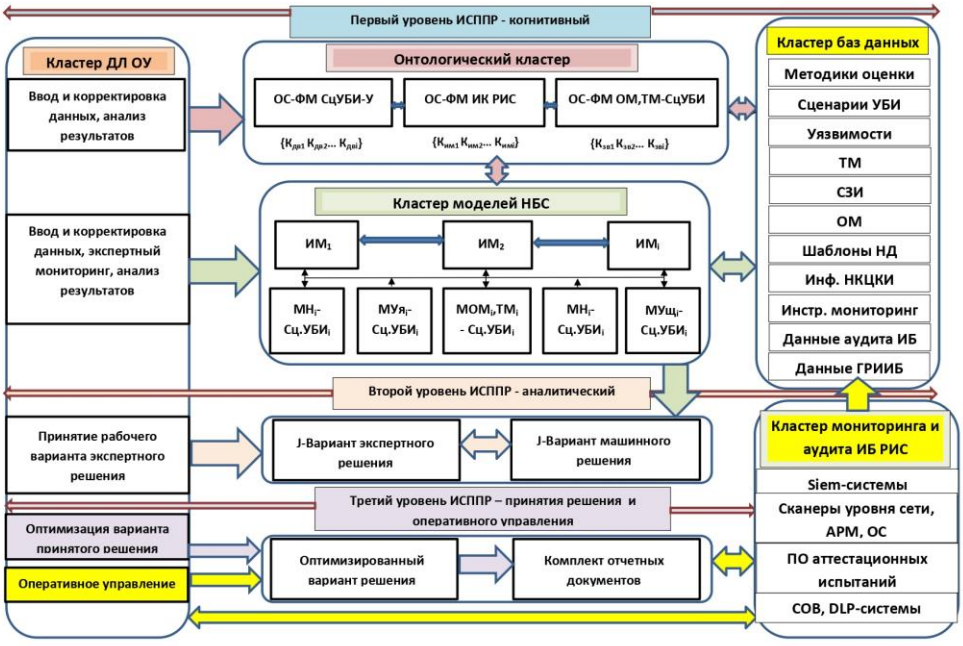


Рис. 3. Структура модели СППР.

Первый уровень ИСППР - когнитивный, объединяет в своем составе кластеры онтологических моделей, НБМ, баз данных, а также кластер управляющих воздействий ДЛ ОУ на первом уровне.

Первый кластер представлен тремя ОС-ФМ. Рассмотрим их более подробно.

ОС-ФМ ИМ РИС. Структурно РИС состоит из ИМ и подсистем (ЦОД, ЛИВС, узлов резервирования (УР) и др.). В составе модели выделены пять уровней концептов, отражающих потенциальные объекты ДВ на аппаратном, системном, прикладном, сетевом и пользователей уровнях [1]. К ним относятся: типы ОТСС, типы интерфейсов ОТСС, типы протоколов, типы ОС и прикладного

ПО, виды защищаемых активов, типы и структура линий и информационных потоков между РИС, ИМ и их внутренними элементами.

В ходе построения онтологии между концептами устанавливаются и прописываются связи, отражающие их взаимное влияние. Таким образом, моделируется текущая ситуация – совокупность всех сведений о структуре элементов РИС и их функционировании.

ОС-ФМ взаимосвязей сценариев реализации УБИ и уязвимостей (ОС-ФМ СцУБИ-У). Отражает взаимосвязи следующих концептов: множество классов нарушителей {КлН$_1$…КлН$_i$}, множество УБИ и сценарием их реализации {S$_1$…S$_i$}, множество тактик реализации УБИ {Т$_1$…Т$_i$}, множество техник реализации УБИ {t$_1$…t$_i$}, множество уязвимостей {У$_1$…У$_i$} объектов ДВ на аппаратном, системном, прикладном и сетевом и пользовательском уровне ИМ [33].

ОС-ФМ взаимосвязей защитных мероприятий, уязвимостей, способов, тактик и техник реализации УБИ (ОС-ФМ ОМ, ТМ-У-СцУБИ). Отражает взаимосвязи следующих концептов: множество способов применения ТМ {S$_{тм1}$…S$_{тмi}$} применения ОМ {S$_{тм1}$…S$_{тмi}$} направленных на закрытие уязвимостей объектов ДВ на аппаратном, системном, прикладном и сетевом и пользовательском уровне {У$_1$…У$_i$} ИМ и (или) локализацию множества способов реализации УБИ {S$_1$…S$_i$}, их тактик {Т$_1$…Т$_i$}, и техник {t$_1$…t$_i$}.

Данные ОС-ФМ взаимно интегрированы и предназначены для проведения ситуационного анализа и выявления параметров и существенных факторов, определяющих характеристики процесса ДВ на элементы (концепты) пяти уровней РИС, применяемых МЗИ, их взаимосвязей и степени их взаимовлияния.

Ввод исходных данных по структуре ИМ РИС осуществляется ДЛ ОУ ИБ из кластера БД.

Онтологический кластер алгоритмично связан с кластером НБМ. Основу его составляют типовые модули, отражающие вероятностные характеристики событий ИБ в процессе функционирования защищаемой РИС в условиях ДВ [30,34] (Рис.4).

Ввод ИД осуществляется по направлению ДВ и направлению МЗИ в соответствии с разработанными ОС-ФМ четырех уровней РИС.

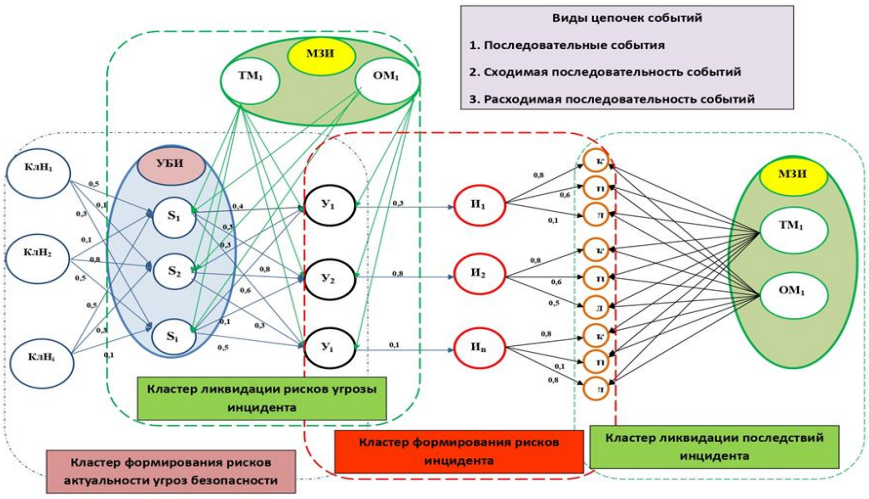


Рис. 4. Типовой модуль НБМ построения защиты РИС

Кластер рисков УБИ формируется путем моделирования характеристик потенциальных возможностей нарушителя {КлН$_1$…КлН$_i$}. Каждый из классов нарушителей способен с определенной вероятностью реализовать множество УБИ определенными способами {S$_1$…Si} [33,34]. Фрагмент матрицы потенциальных возможностей разных классов нарушителей по реализации УБИ представлен на Рис.5.

Перечень возможных способов реализации каждой УБИ {S1…Si} формируется из данных, полученных с сайта ФСТЭК, а также в ходе разработки такого перечня на объекте.

		Нарушитель внутренний			Нарушитель внешний с высоким потенциалом		
		Нарушитель внутренний с высоким потенциал	Нарушитель внутренний с средним потенциал	Нарушитель внутренний с слабым потенциалом	Нарушитель внешний с высоким потенциалом	Нарушитель внешний с средним потенциалом	Нарушитель внешний с слабым потенциалом
24	Угроза изменения режимов работы аппаратных элементов	1					
25	Угроза изменения системных и глобальных переменных		1				
26	Угроза искажения XML-схемы		1			1	
27	Угроза искажения вводимой и выводимой на периферийные устройства информации			1	1		
28	Угроза использования альтернативных путей доступа к ресурсам			1			1
29	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами			1			1
30	Угроза использования информации идентификации/аутентификации, заданной по умолчанию			1		1	
31	Угроза использования механизмов авторизации для повышения привилегий			1			1
32	Угроза использования поддельных цифровых подписей BIOS					1	
33	Угроза использования слабостей кодирования входных данных		1			1	
34	Угроза использования слабостей протоколов сетевого/локального обмена данными			1			1
35	Угроза использования слабых криптографических алгоритмов BIOS				1		
36	Угроза исследования механизмов работы программы		1			1	
37	Угроза исследования приложения через отчёты об ошибках		1			1	
38	Угроза исчерпания вычислительных ресурсов хранилища			1			

Рис. 5. Модель возможностей различных классов нарушителей по реализации УБИ (фрагмент)

Каждый способ имеет свой сценарий (тактики (T_i) и техники (t_j)) реализации через существующие уязвимости ($У_i$). Таким образом, представляется возможность составить вероятностную модель взаимных влияний УБИ, способов и сценариев их реализации. Фрагмент данной модели представлен на Рис.6 [30,35].

Определив в модели критерии актуальности УБИ, способов и сценариев их реализации мы получим соответствующую матрицу.

Наименование угроз безопасности информации	Угроза физического выведения из строя средств хранения,	Угроза форматирования носителей	Угроза «форсированного веб-браузинга»	Угроза хищения средств хранения, обработки и (или)
Описание угрозы безопасности информации	Реализация данной угрозы возможна при условии получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)	Угроза заключается в возможности утраты хранящейся на форматируемом носителе информации, зачастую без возможности её восстановления, из-за преднамеренного или случайного выполнения процедуры форматирования носителя информации.	Угроза заключается в возможности получения нарушителем доступа к защищаемой информации, выполнения привилегированных операций или осуществления иных деструктивных воздействий на некорректно защищённые компоненты веб-приложений. Данная угроза обусловлена слабостями (или отсутствием) механизма проверки корректности вводимых данных на веб-серверах. Реализация данной угрозы возможна при условии успешной реализации «ручного ввода» в адресную строку веб-браузера определённых адресов веб-страниц и осуществления принудительного перехода по древу веб-сайта к страницам, ссылки на которые явно не указаны на веб-сайте	Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации
Интерфейсы				
внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями (проводные, б/проводные, веб-интерфейсы, др.)			$У_2$ $У_3$ $У_1$ $У_4$ S_2 S_1 S_1, S_4 S_2 T_1 T_5 T_1, T_2 T_1 $t_1\ t_4\ t_5$ $t_1\ t_2\ t_3$ $t_1\ t_7$ $t_2\ t_4\ t_6$	
внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими			$У_1$ $У_3$ S_2 S_1, S_5 T_1 T_2, T_3 $t_1\ t_7$ $t_2\ t_3\ t_6$	$У_1$ $У_3$ S_2 S_1, S_5 T_1 T_2, T_3 $T_1\ t_7$ $T_2\ t_3\ t_6\ t_7$
интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.)	$У_1$ $У_3$ $У_7$ S_2 S_3, S_5 S_1, S_4 T_1 T_2, T_3 T_1, T_2 $t_1\ t_4$ $t_3\ t_5$ $t_4\ t_5$	$У_1$ $У_3$ S_2 S_3, S_5 T_1 T_2, T_3 $t_1\ t_6$ $t_4\ t_5$		$У_1$ $У_3$ S_2 S_3, S_3 T_1 T_2, T_4 $t_1\ t_4$ $t_3\ t_5$

Рис. 6. НБМ взаимосвязей уязвимостей, способов и сценариев реализации УБИ (фрагмент).

Процесс формирования БД МЗИ для перекрытия УБИ представлен на Рис.7 в виде модели.

Кластер ликвидации рисков УБИ формируется путем ввода характеристик МЗИ, определенных в [1,2,3,4] и состоящих из ТМ и ОМ по локализации способов реализации УБИ и (или) ликвидации уязвимостей.

После актуализации УБИ на выходе модели останутся только актуальные УБИ, способы и сценарии их реализации, а также необходимые для их закрытия СЗИ и ОРД.

Таким образом, создается машинный вариант принятия решения по актуализации УБИ, способам реализации ОМ и ТМ, который на **аналитическом уровне** (второй уровень ИСППР) сравнивается с вариантом решения, разработанного экспертным способом.

Рис.7 Модель формирования базы данных МЗИ, перекрывающих УБИ

Машинный и экспертный варианты принятия решения сравниваются на предмет полноты, качества и адекватности.

После сравнения, анализа и оценки производится оптимизация варианта принятия решений (третий уровень ИСППР). На этом же уровне формируется комплект отчетных документов и осуществляется моделирование системы ОУ защищенной РИС в условиях ДВ.

Мониторинг и аудит ИБ РИС в ходе ОУ осуществляется инструментальным методом. Вариант модели ОУ защищенной РИС представлен на Рис.8.

Полученные данные используются для наращивания или изменения структуры СЗ при применении новых УБИ, способов их реализации, или новых уязвимостей. Результаты инструментального контроля защищенности оцениваются ДЛ ОУ и вносятся в ИД моделей когнитивного уровня.

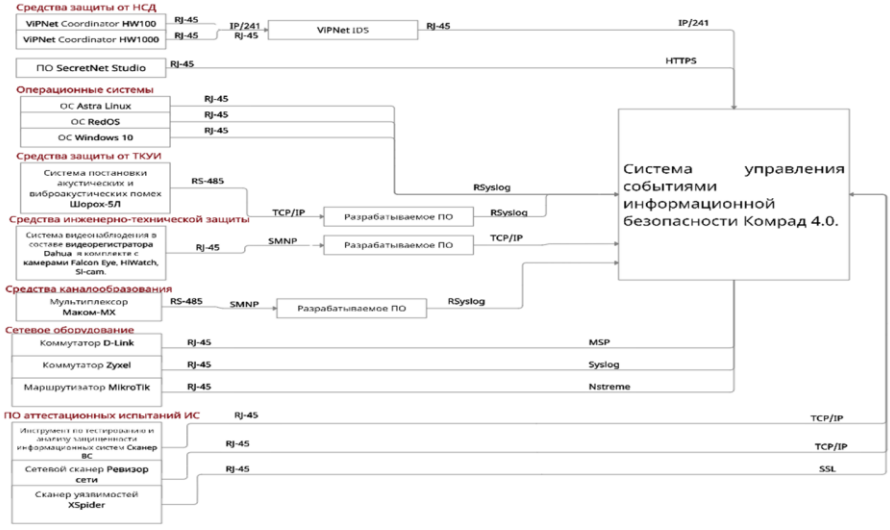


Рис. 8. Модель ОУ событиями ИБ (вариант)

В типовом модуле НБМ за моделирование процесса ОУ событиями ИБ отвечает кластер формирования рисков инцидента. Он моделируется с учетом вероятности нанесения ущерба конфиденциальности (К), целостности (Ц) и доступности (Д) защищаемым информационным ресурсам с определенной степенью вероятности.

Кластер ликвидации последствий инцидента моделируется аналогично кластеру ликвидации рисков УБИ, с составлением соответствующей модели.

В третьем разделе исследования разработаны комплексная методика и алгоритмы автоматизации ППР при разработке мер по защите РИС в условиях ДВ.

Методика и алгоритмы определения актуальности сценариев и тактик УБИ.

Данная методика даёт возможность проведения универсальной оценки для событий ИБ по количественным значениям подмножества переменных показателей МЗИ и ДВ нарушителей, которая минимизирует вероятность ошибочного решения [30,36].

Рассмотрим **алгоритм** ее применения для ранее разработанной ОС-ФМ РИС.

Каждая РИС состоит из ИМ различного назначения и структуры. Обозначим их через множество $\{G_{1\ldots}G_i\}$. В каждом ИМ для определения объектов ДВ выделены пять уровней его структуры. Представим это в виде следующего кортежа:

$$G_i \in \{A_i, F_i, P_i, L_i, H_i\}, \quad (1)$$

где A_i - аппаратный, F_i-системный, P_i-прикладной, L_i- сетевой, H_i-пользовательский уровни i-го ИМ.

Концепты каждого уровня ИМ имеют определенный набор уязвимостей $\{У_1 \ldots У_i\}$. Уязвимости определяются в ходе проведения мероприятий тестирования.

Для каждого ИМ введем понятие вектора его суммарных уязвимостей на каждом из уровней:

$$G_i \in \left\{ \sum_1^n Y_{Ai}, \sum_1^n Y_{Fi}, \sum_1^n Y_{Pi}, \sum_1^n Y_{Li}, \sum_1^n Y_{Hi} \right\} \quad (2)$$

Для обеспечения привязки данного вектора к онтологической модели, составим следующие матрицы для уязвимостей концептов каждого уровня G_i. В столбцах матрицы отображаются концепты $\{K_{1Ai} \ldots K_{mAi}\}$ соответствующего уровня, а в строках обнаруженные уязвимости каждого из них:

$$G_{iA_i} = \begin{matrix} K_{1Ai}Y_1 & K_{1Ai}Y_2 & .... & K_{1Ai}Y_n \\ K_{2Ai}Y_1 & K_{2Ai}Y_2 & .... & K_{2Ai}Y_n \\ K_{3Ai}Y_1 & K_{3Ai}Y_2 & .... & K_{3Ai}Y_n \\ K_{mAi}Y_1 & K_{mAi}Y_2 & .... & K_{mAi}Y_n \end{matrix} \quad (3а)$$

$$G_{iL_i} = \begin{matrix} K_{1Li}Y_1 & K_{1Li}Y_2 & .... & K_{1Li}Y_n \\ K_{2Li}Y_1 & K_{2Li}Y_2 & .... & K_{2Li}Y_n \\ K_{3Li}Y_1 & K_{3Li}Y_2 & .... & K_{3Li}Y_n \\ K_{mLi}Y_1 & K_{mLi}Y_2 & .... & K_{mLi}Y_n \end{matrix} \quad (3б)$$

$$G_{iF_i} = \begin{matrix} K_{1Fi}Y_1 & K_{1Fi}Y_2 & .... & K_{1Fi}Y_n \\ K_{2Fi}Y_1 & K_{2Fi}Y_2 & .... & K_{2Fi}Y_n \\ K_{3Fi}Y_1 & K_{3Fi}Y_2 & .... & K_{3Fi}Y_n \\ K_{mFi}Y_1 & K_{mFi}Y_2 & .... & K_{mFi}Y_n \end{matrix} \quad (3в)$$

$$G_{iH_i} = \begin{matrix} K_{1Hi}Y_1 & K_{1Hi}Y_2 & .... & K_{1Hi}Y_n \\ K_{2Hi}Y_1 & K_{2Hi}Y_2 & .... & K_{2Hi}Y_n \\ K_{3Hi}Y_1 & K_{3Hi}Y_2 & .... & K_{3Hi}Y_n \\ K_{mHi}Y_1 & K_{mHi}Y_2 & .... & K_{mHi}Y_n \end{matrix} \quad (3г)$$

$$G_{iP_i} = \begin{matrix} K_{1Pi}Y_1 & K_{1Pi}Y_2 & .... & K_{1Pi}Y_n \\ K_{2Pi}Y_1 & K_{2Pi}Y_2 & .... & K_{2Pi}Y_n \\ K_{3Pi}Y_1 & K_{3Pi}Y_2 & .... & K_{3Pi}Y_n \\ K_{mPi}Y_1 & K_{mPi}Y_2 & .... & K_{mPi}Y_n \end{matrix} \quad (3д)$$

Вводим матрицу векторов критической значимости концептов каждого уровня для живучести ИМ:

$$W_{G_i} = \begin{matrix} w_{1K_{Ai}} & w_{2K_{Ai}} & w_{3K_{Ai}} & \ldots & w_{mK_{Ai}} \\ w_{1K_{Fi}} & w_{2K_{Fi}} & w_{3K_{Fi}} & \ldots & w_{mK_{Fi}} \\ w_{1K_{Pi}} & w_{2K_{Pi}} & w_{3K_{Pi}} & \ldots & w_{mK_{Pi}} \\ w_{1K_{Li}} & w_{2K_{Li}} & w_{3K_{Li}} & \ldots & w_{mK_{Li}} \\ w_{1K_{Hi}} & w_{2K_{Hi}} & w_{3K_{Hi}} & \ldots & w_{mK_{Hi}} \end{matrix} \quad (4)$$

где w - вес (значимость) i-го концепта для всего ИМ в целом.

Введем правило: «Если уязвимость в ходе тестирования вскрыта, то она должна быть защищена применением ТМ и (или) ОМ».

Для этого необходимо проделать следующие мероприятия.

1. Актуализировать с помощью кластера НБМ вероятностные показатели способов и сценариев реализации УБИ.
2. Актуализировать перечень доступных для ДВ уязвимостей концептов (3а-3д) и их критическую значимость (4). Данные связи прописаны в базах данных.
3. Составить матрицу распределения СЗИ и проводимых режимных мероприятий. Данные связи прописаны в базах данных.
4. Ввести данные по проведенным МЗИ в кластер НБМ.
5. Вывести отчет и убедиться, что все уязвимости закрыты и (или) сценарии реализации УБИ локализованы.

Однако, опыт подсказывает, что абсолютно защищенных РИС нет.

Поэтому для определения потенциальной возможности ДВ на концепты в ходе функционирования ИМ, необходимо провести следующие действия [36,37]:

1. Для каждого ИМ ввести понятие вектора вероятностей обнаружения его уязвимостей компьютерной разведкой противника:

$$G_i \in \{p_{y1}, p_{y2}, \ldots . p_{yn}\} \quad (5)$$

2. Составить матрицы вероятностей вскрытия уязвимостей ($P_{вск.Уi}$) и вскрытия элементов СЗ ($P_{вск.СЗi}$)
3. Составить матрицы вероятностей выживания i-го ИМ ($P_{выж.ИМi}$) при физическом и(или) программном воздействии.
4. Составить матрицы вероятностей выживания СЗ ($P_{выж.СЗi}$) при физическом и(или) программном воздействии.
5. Составить матрицы вероятностей сохранения работоспособности при воздействии преднамеренных, и (или) непреднамеренных радиоэлектронных помех на СЗ ($P_{сп.сзi}$) и ИМ ($P_{сп.ЭИМi}$).
6. Составить матрицы вероятностей исправного функционирования СЗИ ($P_{над.\ сзиi}$) и элементов ИМ ($P_{над.\ ЭМИi}$) в ходе эксплуатации в условиях критического изменения параметров, в т.ч. и при ошибочных действиях персонала.

Расчет вероятностных характеристик п.п. 3,4,5,6 должен производиться с учетом весов критичности концептов на всех его уровнях ИМ [38].

Рассмотрим методику расчета указанных выше вероятностных характеристик ДВ с помощью НБМ.

Математическая основа для этого является теорема Байеса, суть которой описывает следующая формула:

$$P(A|B)\,P(B) = P(B|A)\,P(A) \quad (6)$$

В типовом модуле модели (Рис.4) взаимное влияние ДВ и МЗИ представлены в виде цепочек последовательных событий, сходимой и расходимой последовательностей событий.

События в последовательных цепочках могут быть однородные (деструктивные или защитные) и разнородные (деструктивные и защитные) (Рис 9).

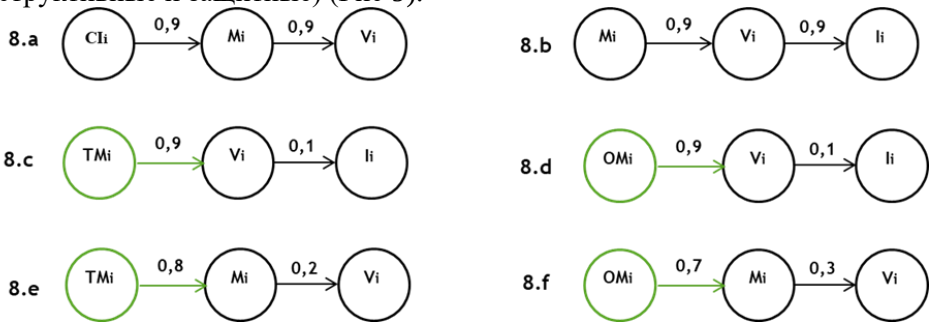


Рис.9 Типы последовательных цепочек событий: 8 a,b – цепочки однородных событий, 8 c,d,e,f – разнородные последовательности событий

Расчет совместного распределения вероятностей для последовательных как однородных, так и разнородных событий осуществляется по приведенным ниже формулам.

Для варианта 8.a - цепочки однородных (деструктивных) событий:

$$P(КлН_i, У_i \mid S_i) = \frac{P(КлН_i, S_i, У_i)}{P(S_i)} = \frac{P(КлН_i)(S_i|КлН_i)P(У_i|S_i)}{P(S_i)} = P(КлН_i \mid S_i)P(У_i \mid S_i) \quad (7)$$

Аналогичным образом составляются формулы и устанавливаются вероятностные зависимости событий ИБ для других типов цепочек последовательных событий.

В модели также выявлено взаимное влияние ДВ и МЗИ в виде цепочек сходимых событий (Рис.9).

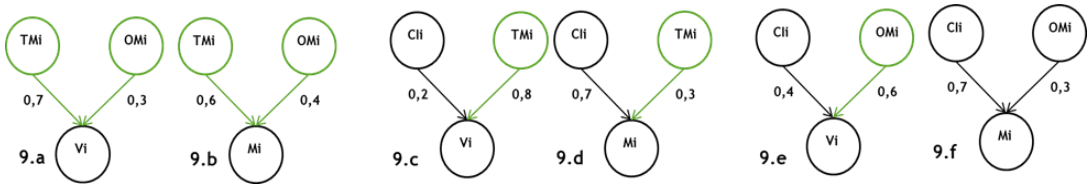


Рис.10. Типы цепочек сходимых событий.

Совместное распределение вероятностей для варианта 9.а сходимой последовательности событий ИБ рассчитывается по следующей формуле:

$$P(TM_i, OM_i, Y_i) = \sum_{y_i} P(TM_i)P(OM_i)P(Y_i \mid OM_i, TM_i) = P(OM_i \mid Y_i)P(TM_i \mid Y_i) \quad (8)$$

Аналогичным образом составляются формулы и устанавливаются вероятностные зависимости событий ИБ для других типов цепочек расходимых событий.

Взаимное влияние ДВ и МЗИ в виде цепочек расходимых событий представлено на Рис.11.

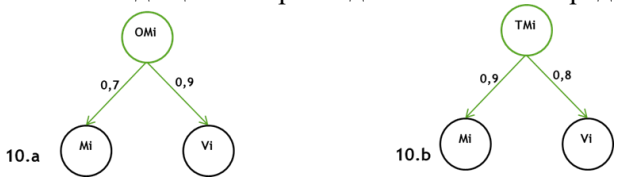


Рис.11 Типы цепочек расходимых событий.

Совместное распределение вероятностей для расходимой последовательности событий ИБ рассчитывается по следующей формуле:

$$P(S_i, Y_i \mid TM_i) = \frac{P(TM_i, S_i, Y_i)}{P(TM_i)} = P(S_i \mid TM_i)P(Y_i \mid TM_i) \quad (9)$$

Данный подход позволяет рассчитать зависимость априорной вероятности событий от вероятности событий, которые могут произойти, т.е. определить вероятностную зависимость ДВ от защитных мер и наоборот.

Схема элементов взаимодействия элементов типового модуля приведена на Рис.12

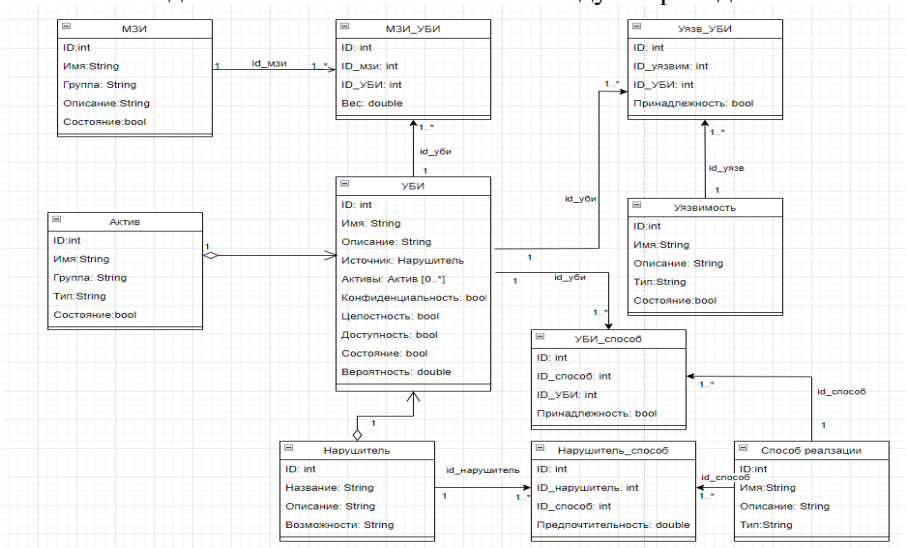


Рис. 12. Схема взаимосвязи БД компонентов НБМ

Программные алгоритмы реализации указанных выше методик представлены на Рис. 13-16.

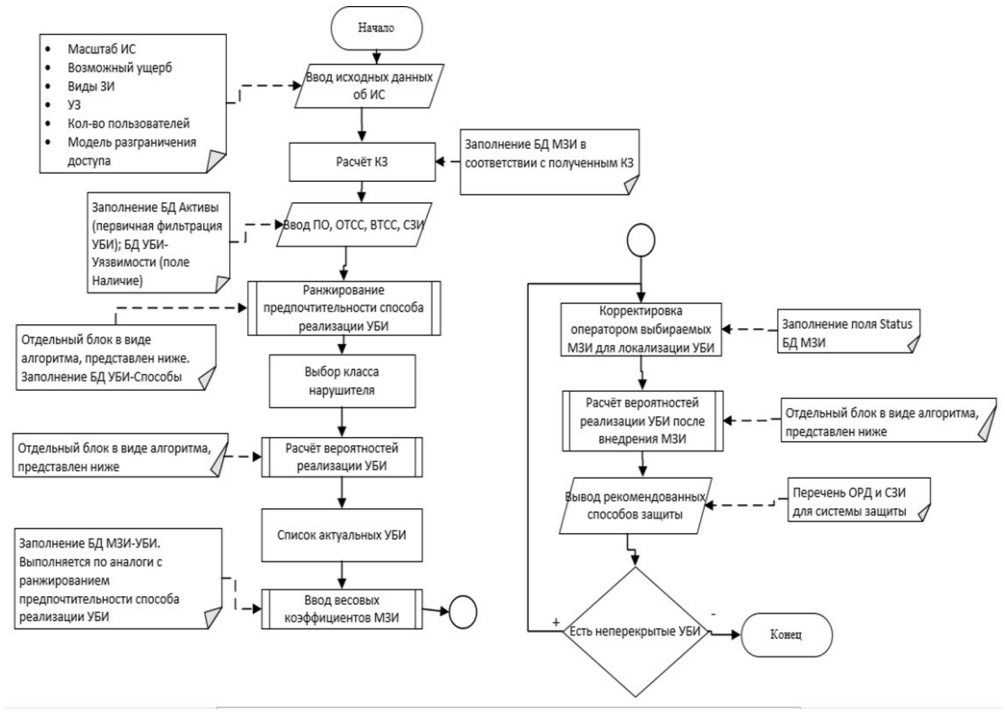


Рис. 13. Алгоритм работы ПО

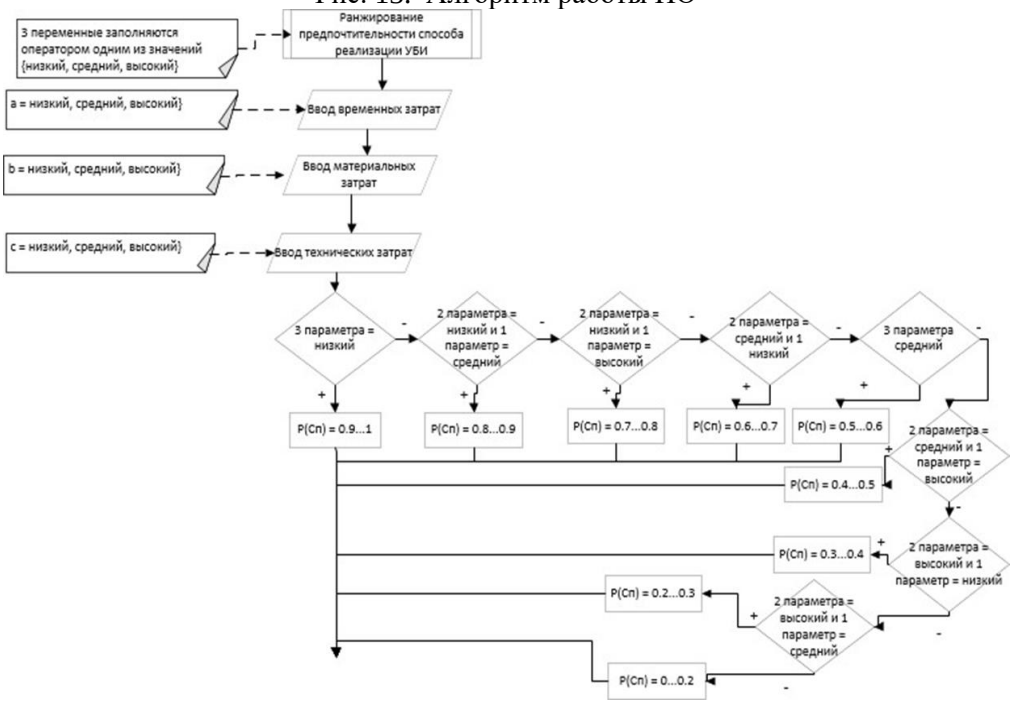


Рис. 14. Алгоритм Задание вероятности предпочтительности способа реализации УБИ

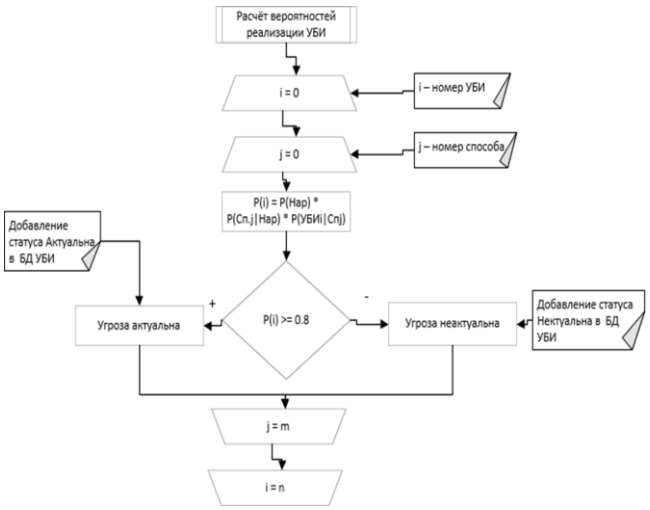


Рис. 15. Алгоритм расчёта вероятности реализации УБИ

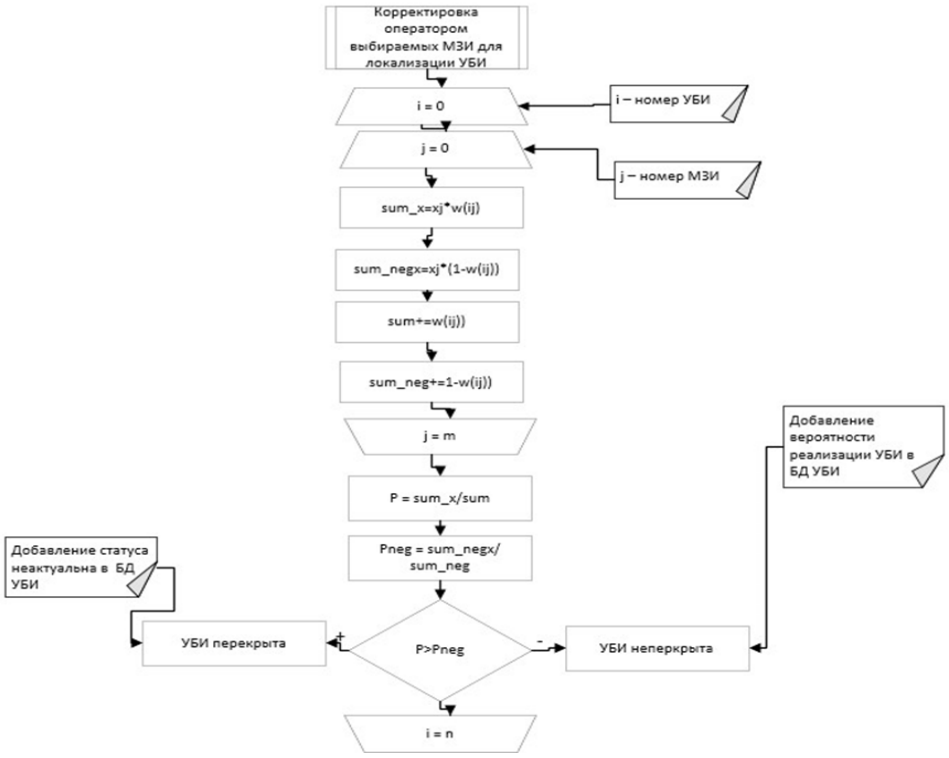


Рис. 16. Алгоритм расчёта вероятности реализации УБИ после выбора оператором СЗИ

В четвертом разделе исследования разработана ИСППР при разработке комплекса мер по защите РИС, оценки их эффективности и ОУ [39,40].

Были сформированы необходимые базы данных.

Все таблицы в приложении созданы с помощью СУБД SQLLite и библиотеки Hibernate. В ПО реализован ручной ввод названия класса-сущности в класс-сборщик сессии Hibrenate.

Процесс разработки ПО далее представлен в виде скриншотов

	ID	Name	Group_MZI	Description	State
1	1	ИАФ.1	ИАФ	Идентификация и аутентификация пользоват…	0
2	2	ИАФ.2	ИАФ	Идентификация и аутентификация устройств…	0
3	3	ИАФ.3	ИАФ	Управление идентификаторами, в том числе…	0
4	4	ИАФ.4	ИАФ	Управление средствами аутентификации, в …	0
5	5	ИАФ.5	ИАФ	Защита обратной связи при вводе аутентиф…	0

```java
@Entity
@Table(name = "MZI", schema = "main", catalog = "")
public class MziEntity {
    @Id
    @Column(name = "ID", nullable = false)
    private int id;
    @Basic
    @Column(name = "Name", nullable = true, length = -1)
    private String name;
    @Basic
    @Column(name = "Group_MZI", nullable = true, length = -1)
    private String groupMzi;
    @Basic
    @Column(name = "Description", nullable = true, length = -1)
    private String description;
    @Basic
    @Column(name = "State", nullable = true)
    private Integer state;
```

Рис. 17. Маппинг класса программы через Hibernate

```java
private HibernateSessionFactoryUtil() {}
public static SessionFactory getSessionFactory()
{
    if (sessionFactory == null) {
        try {
            Configuration configuration = new Configuration().configure();
            configuration.addAnnotatedClass(MziEntity.class);
            configuration.addAnnotatedClass(UbiEntity.class);
            configuration.addAnnotatedClass(VulnerabilitiesEntity.class);
            configuration.addAnnotatedClass(MziUbiEntity.class);
            configuration.addAnnotatedClass(AssetEntity.class);
            configuration.addAnnotatedClass(MziNewEntity.class);
            configuration.addAnnotatedClass(MeansThreatsEntity.class);
            configuration.addAnnotatedClass(UbiMeansEntity.class);
            configuration.addAnnotatedClass(UbiVulnAssetEntity.class);

            StandardServiceRegistryBuilder builder = new StandardServiceRegistryBuilder().applySettings
                    (configuration.getProperties());
            sessionFactory = configuration.buildSessionFactory(builder.build());

        } catch (Exception e) {
            System.out.println("Исключение!" + e);
        }
    }
    return sessionFactory;
}
```

Рис. 18. Метод, возвращающий сессию Hibernate со всеми включёнными аннотированными классами.

```java
//Расчёт для ПДн
{
    Criteria cr1 = session.createCriteria(DataPdnEntity.class);
    List<DataPdnEntity> data_pdn = cr1.list();
    List<String> UZ_for_all_pdn = new ArrayList<>();
    for (int i = 0; i < data_pdn.size(); i++) {
        if (data_pdn.get(i).getClassPdn() == null) {
            data_pdn.get(i).setClassPdn();
            Transaction tx1 = session.beginTransaction();
            session.update(data_pdn.get(i));
            tx1.commit();
            //session.flush();
        }
        UZ_for_all_pdn.add(data_pdn.get(i).getClassPdn());
    }
    String final_UZ_for_pdn = (UZ_for_all_pdn.contains("1У3")) ? "1У3" : (UZ_for_all_pd
    textField_ClassPDn.setText(final_UZ_for_pdn);
}
/
//Расчёт общего класса защищённости
String class_Pdn_sootvetstvie = (textField_ClassPDn.getText() == "1У3") ? "К1"
        : (textField_ClassPDn.getText() == "2У3") ? "К2" : "К3";
String class_sluzh = textField_ClassSluzh.getText();
String class_commerce = textField_ClassCommerce.getText();
String total_class = (class_Pdn_sootvetstvie.equals("К1") ||
        class_sluzh.equals("К1") || class_commerce.equals("К1")) ? "К1" :
        (class_Pdn_sootvetstvie.equals("К2") || class_sluzh.equals("К2") ||
                class_commerce.equals("К2")) ? "К2" : "К3";
```

Рис. 19. Расчёт общего класса защищённости информационной системы

```
while(iter_asset.hasNext())
{
    AssetEntity asset = new AssetEntity();
    asset.setId(Long.toString(iter_asset.nextIndex()));
    String description = (((String)iter_infoAsset.next()).trim());
    String name = (((String)iter_asset.next()).trim());
    asset.setName((name));
    asset.setManufacturer(iter_infoAsset.next());
    asset.setGroupAsset(iter_infoAsset.next());
    //проверка на содержание ключевых слов в имени актива и/или в его содержании/описании
    java.util.regex.Matcher matcher_microprog = Pattern.compile("[мМ]икро?прог.*обеспеч.*").matcher(description);
    java.util.regex.Matcher matcher_DB= Pattern.compile("систем.управ.*баз.*дан*").matcher(description);
    java.util.regex.Matcher matcher_browser = Pattern.compile("[бб]раузер").matcher(description);
    java.util.regex.Matcher matcher_antivirus= Pattern.compile("антивирус").matcher(description);
    java.util.regex.Matcher matcher_textEditor= Pattern.compile("текст.*редактор").matcher(description);
    java.util.regex.Matcher matcher_crypto= Pattern.compile("криптограф").matcher(description);
    java.util.regex.Matcher matcher_progPack= Pattern.compile("[пП]акет прогр").matcher(description);
    java.util.regex.Matcher matcher_SCADA= Pattern.compile("SCADA").matcher(description);
    java.util.regex.Matcher matcher_systemMonitoring = Pattern.compile("[Сс]ист.*монитор.*").matcher(description
    java.util.regex.Matcher matcher_systemResources = Pattern.compile("SAP").matcher(description);
    java.util.regex.Matcher matcher_communication= Pattern.compile("[сервер|систем].* обмена сообщен.*").matcher
    java.util.regex.Matcher matcher_messagesServer= Pattern.compile("почтов.*сервер.*").matcher(description);
    java.util.regex.Matcher matcher_Cloud = Pattern.compile("обла[кч].*").matcher(description);

    if (matcher_antivirus.find() || name.contains("Защитник") || name.contains("Defender") || name.contains("Ка
    {
        asset.setType("Антивирус");
    }
    else if (matcher_microprog.find() || name.contains("Микропрограммное обеспечение") || name.contains("Huawei"
    {
```

Рис.20. Классификация ПО

	ID	Exist 1	Name	Type	Group_asset
1	55	1	QEMU	ПО виртуализации	ПО виртуализации/ПО виртуального програ
2	117	1	SendMail SMTP Server	Почтовый сервер	Сетевое программное средство
3	156	1	Red Hat Enterprise Linux	Операционная система	Операционная система
4	986	1	Cisco Catalyst 3750V2-24TS Switch	Коммутатор	ПО сетевого программно-аппаратного сред
5	1455	1	Kaspersky Internet Security for …	Антивирус	Программное средство защиты
6	2965	1	Adobe Acrobat Reader 2017	Офисная программа	Прикладное ПО информационных систем
7	3094	1	MySQL	СУБД	СУБД
8	4376	1	FusionSphere OpenStack	<null>	ПО программно-аппаратного средства
9	7514	1	SSD DC P4511 Series	Микропрограммное обеспечен…	Микропрограммный код
10	8028	1	PicoTCP	<null>	Сетевое средство
11	9270	1	FortiAnalyzer	<null>	ПО программно-аппаратных средств защиты

Рис. 21. Выбор наличия активов

	ID	Probability_choice	ID_Technics	Description_Tecnics	ID_Mean
1	1	0.15688329935073853	T1	Сбор информации о системах и сетях. Тактическая…	T1.1
2	2	0.04047620669007301	T1	Сбор информации о системах и сетях. Тактическая…	T1.2
3	3	0.4463852643966675	T1	Сбор информации о системах и сетях. Тактическая…	T1.3
4	4	0.062444835901260376	T1	Сбор информации о системах и сетях. Тактическая…	T1.4
5	5	0.416946142911911	T1	Сбор информации о системах и сетях. Тактическая…	T1.5
6	6	0.339969664812088	T1	Сбор информации о системах и сетях. Тактическая…	T1.6
7	7	0.20364363491535187	T1	Сбор информации о системах и сетях. Тактическая…	T1.7
8	8	0.6523627638816833	T1	Сбор информации о системах и сетях. Тактическая…	T1.8
9	9	0.08458428084850311	T1	Сбор информации о системах и сетях. Тактическая…	T1.9
10	10	0.12436790019273758	T1	Сбор информации о системах и сетях. Тактическая…	T1.10
11	11	0.6198339462280273	T1	Сбор информации о системах и сетях. Тактическая…	T1.11
12	12	0.4495171010494232	T1	Сбор информации о системах и сетях. Тактическая…	T1.12

Рис. 22. Ранжирование предпочтительности выбора способа

```
public static void isActualUbi(int ubi_means_size, List <MeansEntity> means, double P_intruder)
{

    int count_ubi = ubi_means_size/means.size();
    //лимит = показывает какой порог должно перешагнуто значение, чтобы угроза считалась актуальной
    double limit_isActual = 0.5;
    //показывает сколько записей будут рассмотрены с максимальными вероятностями => будет рассматриваться топ-5
    int max_records_forInvestigations = 5;

    //i - номер рассматриваемой УБИ
    for (int i = 0; i < count_ubi; i++)
    {
        Session session = HibernateSessionFactoryUtil.getSessionFactory().openSession();
        double max_probability_record[] = new double[max_records_forInvestigations];
        Criteria cr = session.createCriteria(UbiMeansEntity.class);
        cr.add(Restrictions.eq( propertyName: "idUbi",String.valueOf(i+1)));
        List <UbiMeansEntity>ubi_means_with_i_ubi = cr.list();
        session.close();

        for (int j = 0; j < ubi_means_with_i_ubi.size(); j++)
        {
            //рассчитываем вероятность только для тех уби, которые могут быть реализованы способом j
            if(ubi_means_with_i_ubi.get(j).getState()!=0)
            {
                session = HibernateSessionFactoryUtil.getSessionFactory().openSession();
                Criteria cr1 = session.createCriteria(MeansEntity.class);
                cr1.add(Restrictions.eq( propertyName: "idMean",ubi_means_with_i_ubi.get(j).getIdMean()));
                List <MeansEntity>means_j = cr1.list();
                session.close();
```

Рис.23. Расчёт актуальности УБИ

```
String message = "";
for (int i = 0; i < ubi.size(); i++)
{
    boolean isActual = false;
    //Если вероятность не равна нулю => УБИ актуальна
    if (ubi.get(i).getProbability() != null)
    {
        isActual = true;
        message += "Для перекрытия УБИ" + i + " нужны следующие МЗИ: ";
        session = HibernateSessionFactoryUtil.getSessionFactory().openSession();
        Criteria cr1 = session.createCriteria(MziUbiEntity.class);
        cr1.add(Restrictions.eq( propertyName: "idUbi",i));
        List <MziUbiEntity>mzi_for_ubi_i = cr1.list();
        session.close();
        for(int j = 0; j < mzi_for_ubi_i.size(); j++)
        {
            if (mzi_for_ubi_i.get(j).getWeight()!=0)
            {

                session = HibernateSessionFactoryUtil.getSessionFactory().openSession();
                Criteria cr2 = session.createCriteria(MziEntity.class);
                cr2.add(Restrictions.eq( propertyName: "id",mzi_for_ubi_i.get(j).getIdMzi()));
                List <MziEntity>mzi_for_ubi_i_id = cr2.list();
                session.close();
                message += mzi_for_ubi_i_id.get(0).getName() + " , ";
            }
        }
    }
    if(isActual) {
        message += "\n";
```

Рис.24. Выявление необходимых МЗИ

```
Criteria cr = session.createCriteria(SziEntity.class);
cr.add(Restrictions.eq( propertyName: "state",  value: 1));
List<SziEntity> szi = cr.list();
session.close();

session = HibernateSessionFactoryUtil.getSessionFactory().openSession();
cr = session.createCriteria(MziSziEntity.class);
List<MziSziEntity> mzi_szi = cr.list();
session.close();

for(int i = 0; i < mzi_szi.size(); i++)
{
    for (int j = 0; j < szi.size(); j++)
    {
        if (mzi_szi.get(i).getSziInfoteks().contains(szi.get(j).getName()) ||
                mzi_szi.get(i).getSziCodeBezopasnosti().contains(szi.get(j).getName()) ||
                mzi_szi.get(i).getSziOthers().contains(szi.get(j).getName()))
        {
            String mzi_id = mzi_szi.get(i).getIdMzi();
            session = HibernateSessionFactoryUtil.getSessionFactory().openSession();
            cr = session.createCriteria(MziEntity.class);
            cr.add(Restrictions.eq( propertyName: "name", mzi_id));
            List<MziEntity> mzi = cr.list();
            if(mzi.size()!=0)
            {
                if (mzi.get(0).getState() != 1) {
                    Transaction tx1 = session.beginTransaction();
                    mzi.get(0).setState(1);
                    session.update(mzi.get(0));
                    tx1.commit();
```

Рис.25. Выбор требуемых СЗИ для актуальных МЗИ

```
Session session = HibernateSessionFactoryUtil.getSessionFactory().o
Transaction tx1 = session.beginTransaction();
int count_ubi = mzi_ubi_size / mzi.size();
//i - номер рассматриваемой УБИ
for (int i = 0; i < count_ubi; i++)
{
    Criteria cr = session.createCriteria(MziUbiEntity.class);
    cr.add(Restrictions.eq( propertyName: "idUbi", value: i + 1));
    List<MziUbiEntity> mzi_ubi_with_i_ubi = cr.list();
        P_e_Hp(mzi_ubi_with_i_ubi,mzi);
        wholeProb(mzi_ubi_with_i_ubi,mzi);
        if(probability_Hp_e > probability_Hc_e)
        {

            cr = session.createCriteria(UbiEntity.class);
            cr.add(Restrictions.eq( propertyName: "id",  value: i + 1));
            List<UbiEntity> ubi_i_closed_with_mzi = cr.list();

            ubi_i_closed_with_mzi.get(0).setState("Перекрыта МЗИ");
            ubi_i_closed_with_mzi.get(0).setProbability(0.0F);
            session.update(ubi_i_closed_with_mzi.get(0));
        }
}
tx1.commit();
session.close();
```

Рис.26. Выявление неперекрытых УБИ

```
public static void P_e_Hp(List<MziUbiEntity> mzi_ubi, List<MziEntity> mzi)
{
    probability_e_Hp = 0;
    probability_e_Hc = 0;
    double sum_x = 0;
    double negativ_sum_x = 0;
    for(int i = 0; i < mzi_ubi.size(); i++)
    {
        probability_e_Hp +=  mzi.get(i).getState() * mzi_ubi.get(i).getWeight();
        probability_e_Hc += mzi.get(i).getState() * (1-mzi_ubi.get(i).getWeight());
        sum_x += mzi_ubi.get(i).getWeight();
        negativ_sum_x += (1 - mzi_ubi.get(i).getWeight());
    }
    probability_e_Hp /= sum_x;
    probability_e_Hc /= negativ_sum_x;
}

public static void wholeProb(List<MziUbiEntity> mzi_ubi, List<MziEntity> mzi)
{
    double probability_Hp = 0.7;
    double probability_Hc = 0.3;
    probability_Hp_e = (probability_Hp * probability_e_Hp) / ((probability_Hp * probability_e_Hp)
            + (probability_Hc * probability_e_Hc));
    probability_Hc_e = (probability_Hc * probability_e_Hc) / ((probability_Hp * probability_e_Hp)
            + (probability_Hc * probability_e_Hc));
}
```

Рис.27. Расчёт вероятностей гипотез

Таким образом, процесс разработки ПО для ИСППР завершен. Оформлены документы для государственной регистрации ПО.

В пятом разделе исследования приведены численные эксперименты и примеры применения ИСППР при разработке и оценке эффективности РИС.

Пример ее работоспособности представлен в виде скриншотов

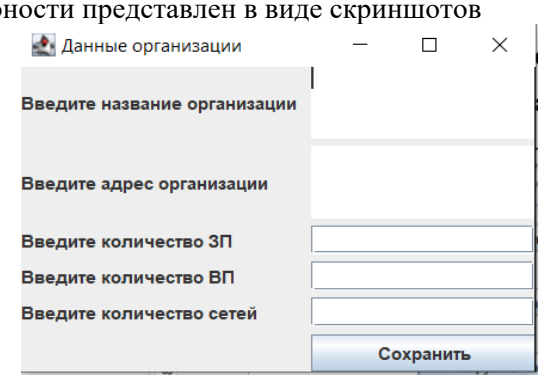


Рис.28. Окно ввода исходных данных

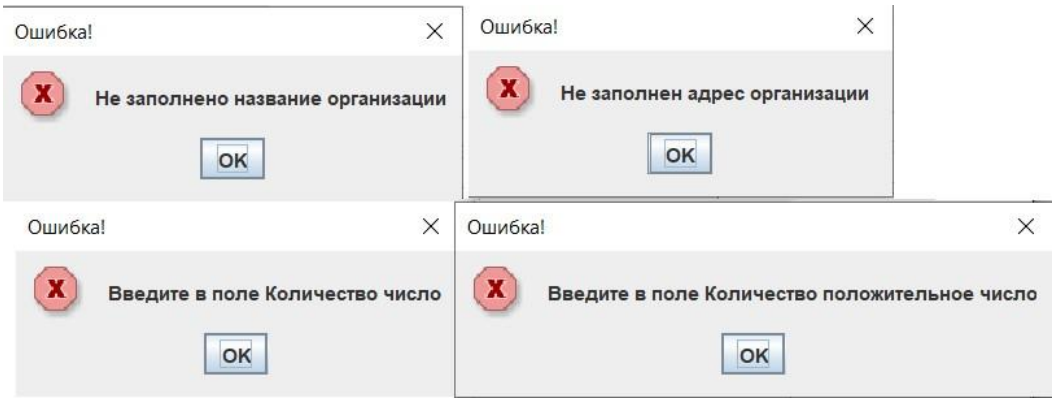


Рис.29. Примеры ошибок неправильного ввода данных

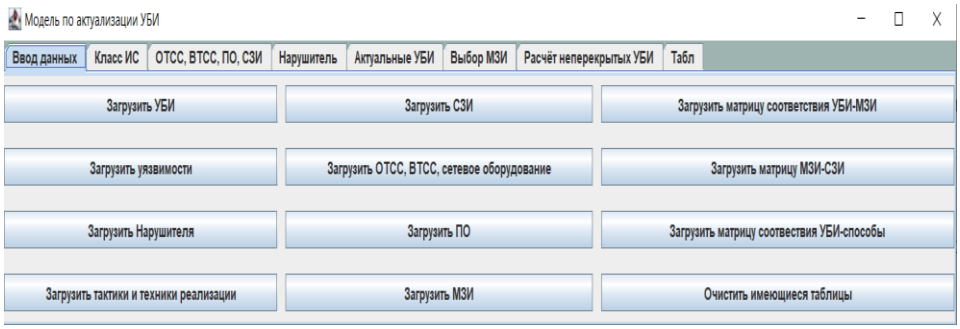


Рис. 30. Модуль для ввода данных и проведения расчётов

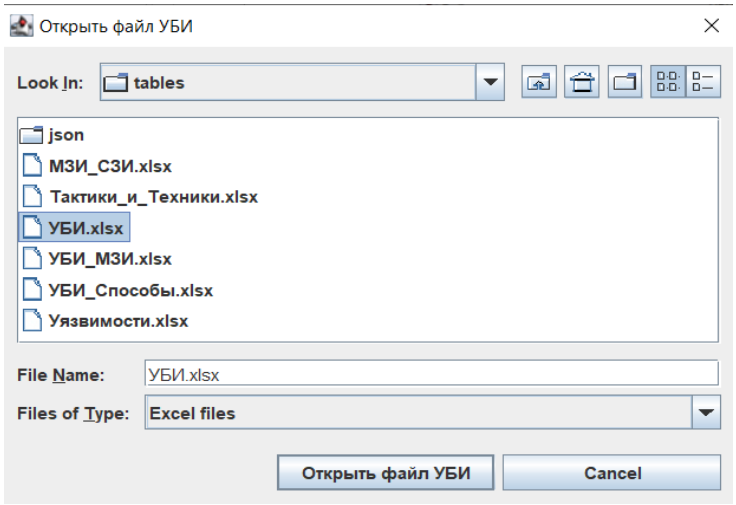


Рис. 31. Выбор таблицы УБИ путём нажатия на кнопки «Загрузить УБИ»

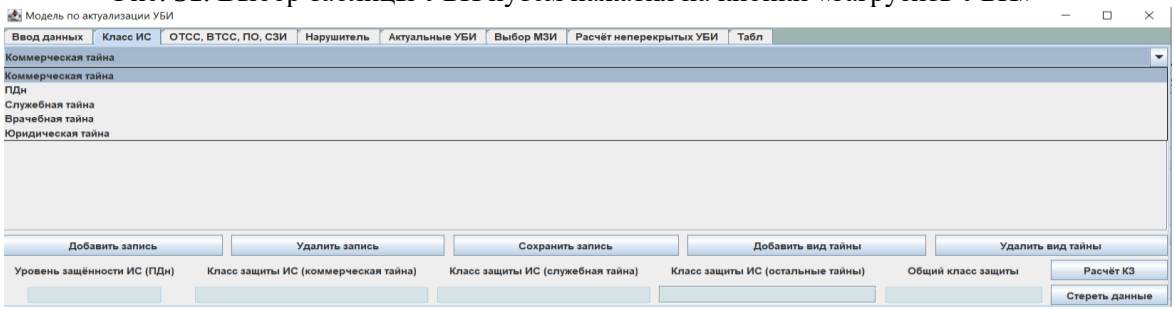


Рис. 32. Выбор вида защищаемой информации

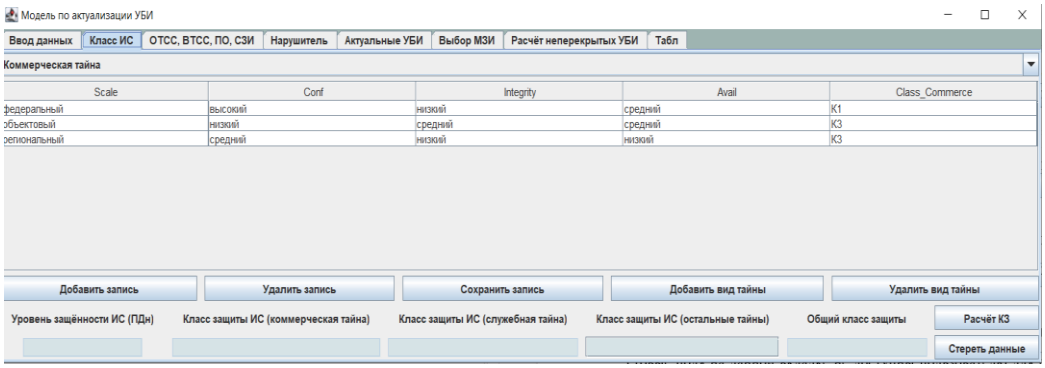


Рис. 33. Ввод данных о защищаемой информации

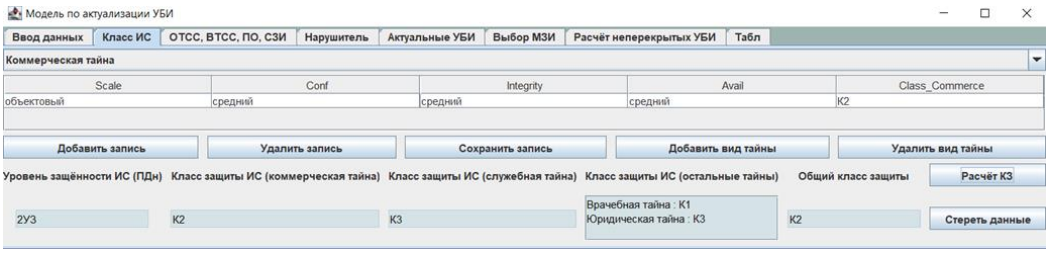


Рис.34. Расчёт класса защищенности для ГИС

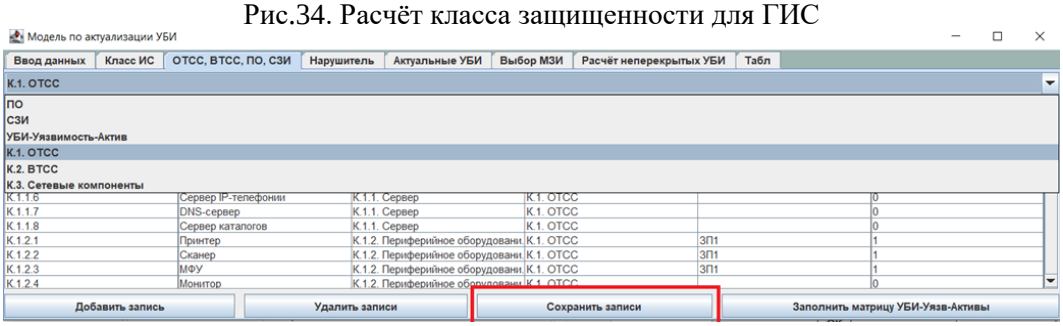


Рис.35. Выбор вводимых данных и занесение их в БД

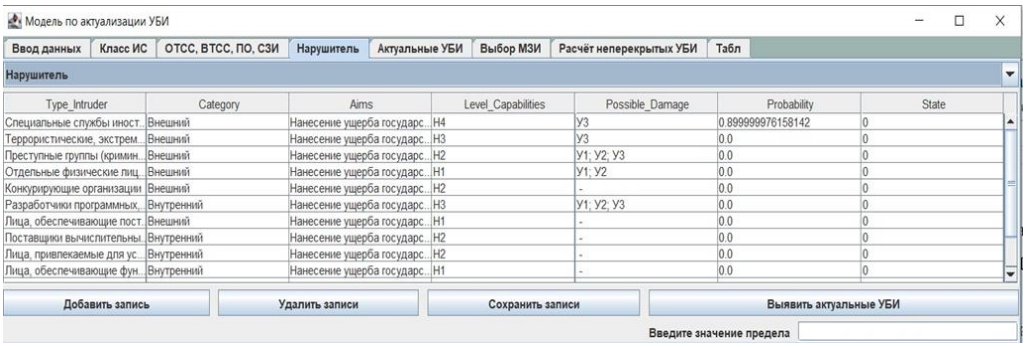


Рис. 36. Вкладка «Нарушитель»

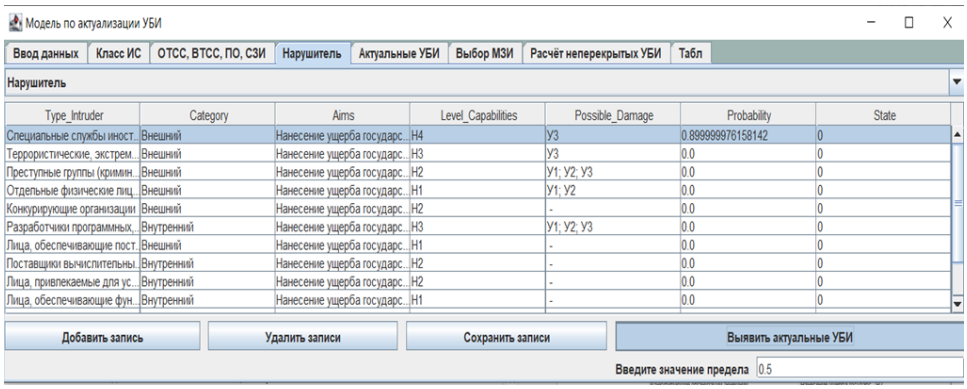


Рис. 37. Выбор нарушителя

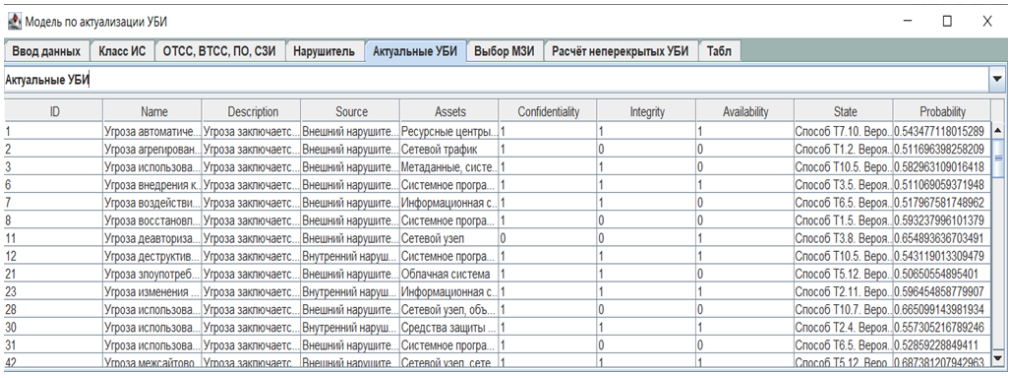


Рис. 38. Перечень актуальных УБИ

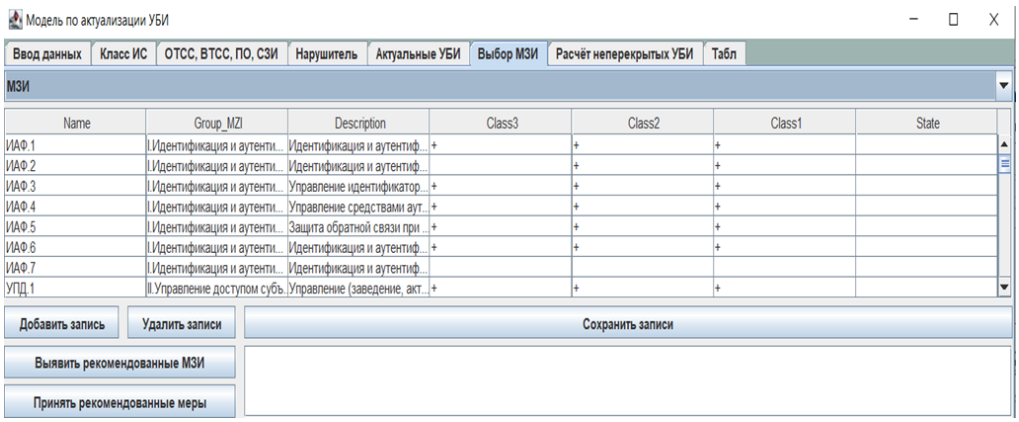


Рис. 39. Вкладка выбор МЗИ

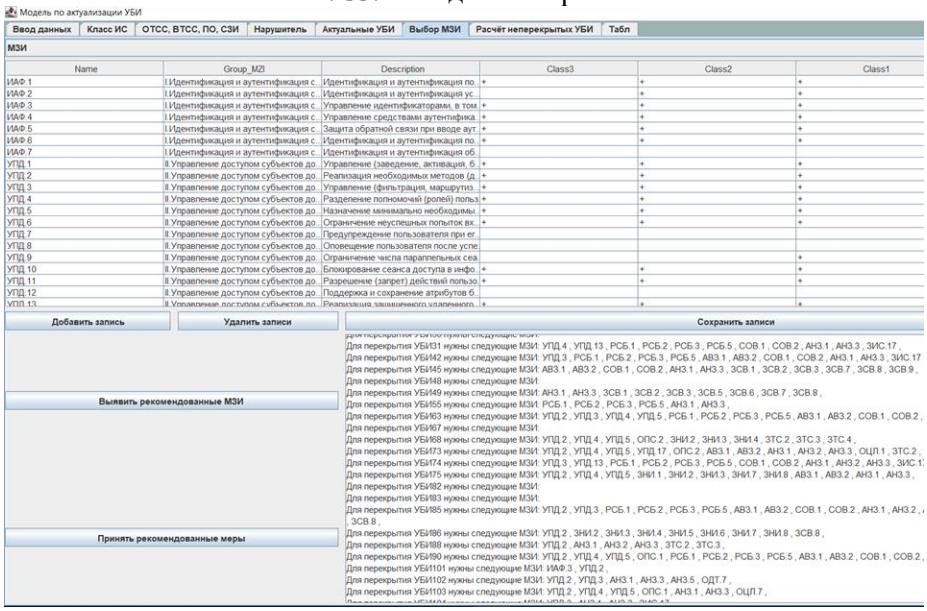


Рис. 40. Выявленные необходимые МЗИ

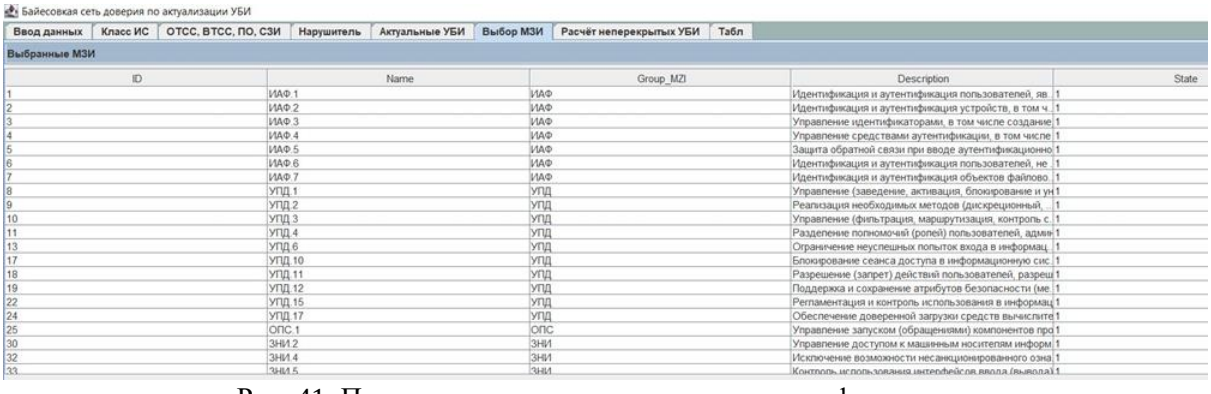


Рис. 41. Перечень применяемых мер защиты информации

Рис. 42. В РИС присутствуют не перекрытые УБИ

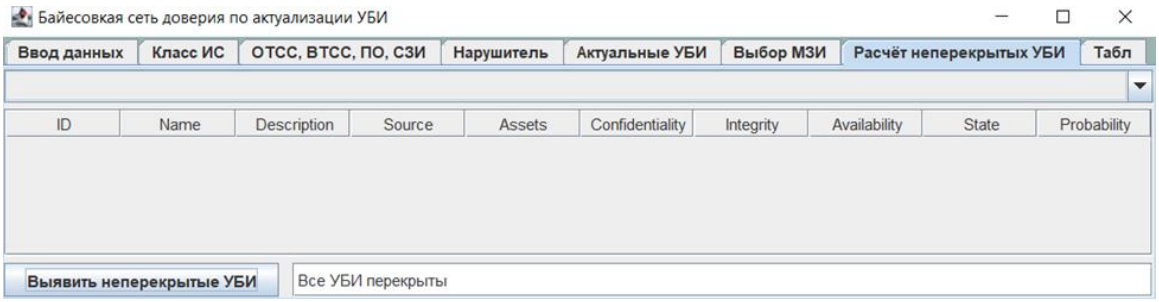


Рис. 44. В ИС все УБИ перекрыты

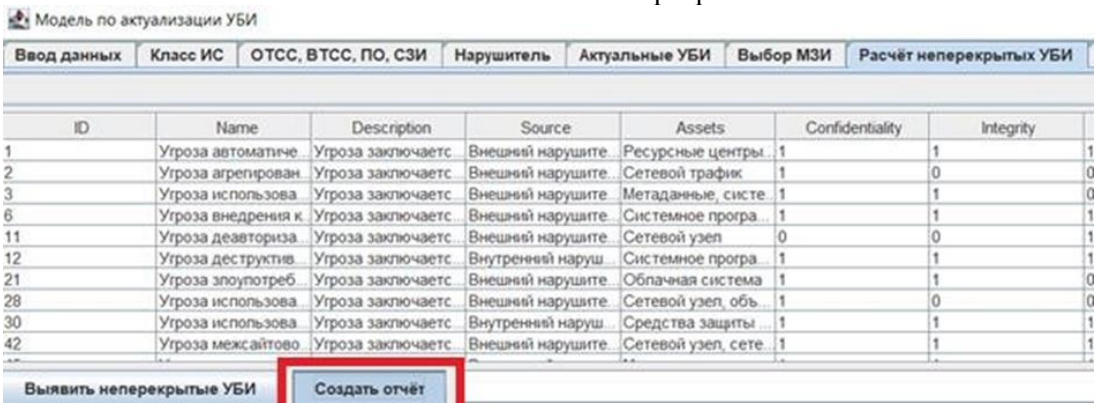


Рис. 45. Кнопка «Создать отчёт»

Таким образом, задача промежуточного этапа исследования выполнена в полном объеме.

Заключение. В данный момент осуществляется разработка алгоритмов ПО, реализующего ОС-ФМ.

Направлениями дальнейших исследований в данной области могут быть следующие:

1. Повышение быстродействия расчетной системы. Для повышения быстроты расчётов произвести распределение каждой задачи по процессам и запараллеливание вычислений.
2. Создания более детальной классификации уязвимостей, УБИ, способов их реализации и активов для повышения точности созданных связей элементов модели.
3. Разработка интерактивного графического интерфейса, представляющего собой БСД с выводом промежуточных вероятностей.
4. Реализация возможности периодического обновления БД путём загрузки документа в формате excel по указанной ссылке. Данное действие обеспечит повышение автоматизации действий оператора.

ПОДТВЕРЖДЕНИЯ

Работа выполнена при финансовой поддержке гранта MTUSI, предоставленного Министерством финансов Российской Федерации из федерального бюджета в 2021 году (научный проект № 35/21-d) в рамках федерального проекта "Информационная безопасность" национальной программы "Цифровая экономика Российской Федерации".

СПИСОК ЛИТЕРАТУРЫ

1. Методический документ. Утвержденная ФСТЭК России 5 февраля 2021 года "Методика оценки угроз информационной безопасности" [Электронный ресурс]. - URL-АДРЕС: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g (дата обращения 20.12.2021).

2. Базовая модель угроз безопасности 2008 "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России" [Электронный ресурс]. - URL-АДРЕС: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (дата обращения 20.12.2021).

3. Джиарратано, Д. Экспертные системы: принципы разработки и программирования/ Д. Джиарратано, Г. Райли // Изд. 4-е, перевод с английского. - Издательство Уильямса. - ISBN: 978-5-8459-1156-8, 2007. - С. 115-201.

4. Буйневич, М.В. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации / М.В. Буйневич, В.В. Покусов, К.Е. Израилов // Информатизация и связь. – 2021. – № 4. – С. 66–73.

5. Еремеев, М.А. Продукционное представление знаний для моделирования источников атак в сети / М.А. Еремеев, А.Г. Ломако, В.М. Моргунов, Н.В. Свергун // CDE'17: The 2017 Symposium on Cybersecurity of the Digital Economy. – Иннополис: Издательский Дом "Афина" (Санкт-Петербург), 19-20 сентября, 2017. – С. 167–180.

6. Приказ ФСТЭК России "Об утверждении требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" от 12.02.2013 № 17 [Электронный ресурс]. - URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения 20.12.2021).

7. Приказ ФСТЭК России "Об утверждении состава и содержания организационных и технических мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" от 18.02.2013 № 21 [Электронный ресурс]. - URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения 20.12.2021).

8. Приказ ФСТЭК России "Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей среды" от 14.03.2014 № 31 [Электронный ресурс]. - URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения 20.12.2021).

9. Приказ ФСТЭК России от 25.12.2017 № 239 "Об утверждении требований к обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" (с изменениями и дополнениями. 26 декабря 2019 г., № 60) [Электронный ресурс]. - URL-АДРЕС: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения 20.12.2021).

10. Постановление Правительства Российской Федерации от 08.02.2018 № 127 "Об утверждении Правил категоризации объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений" [Электронный ресурс ресурс]. - URL-АДРЕС: http://government.ru/docs/6339 / (дата обращения 20.12.2021).

11. Постановление Правительства Российской Федерации от 01.10.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" [Электронный ресурс]. - URL-АДРЕС: https://www.garant.ru/products/ipo/prime / doc/72166260 / (дата обращения 20.12.2021).

12. Перл, Д. Байесовские сети. - М.: Лаборатория когнитивных систем Калифорнийского университета, Лос-Анджелес, 2000. - 102 с.

13. Джаксен, Ф. Байесовские сети и графики принятия решений. - М.: Sprinnger, 2001. – с. 54-120.

14. Литвиненко, Н.Г. Агенариск. Работа с байесовскими сетями / Н.Г. Литвиненко, А.Г. Литвиненко, О.Ж. Мамырбаев, А.С. Шаяхметова. - Алматы: Институт информационных и вычислительных технологий, 2019. - 233 с.

15. Конради, С. Байесовские сети и Байесовская лаборатория, Практическое введение для исследователей./ С.Конради, Л.Джуфф, - https://www.researchgate.net / публикация/282362899 - Байесовские сети Bayesialab - Практическое введение для исследователей.

16. Руководство пользователя BAYESIALAB - https://library .bayesia.com/display / BlabC/BayesiAlab+Руководство пользователя+.

17. Конради, С. Введение в байесовские сети и Байесовскую лабораторию/ С. Конради, Л.Джуфф - https://library.bayesia.com/download/attachments/10092794/ BayesianNetworks Введение v16.pdf.

18. Расширенное моделирование с использованием AgenaRisk. - https://www.agenarisk.com .

19. Байесовская сетевая технология Agena. - https://www.agenarisk.com . Начало работы с AgenaRisk. - https://www.agenarisk.com .

20. Эксперт Хугин, Построение байесовской сети./ Эксперт Хугин - https://www.hugin.com/wp-content/uploads/2016/05/Building-a-BN-Tutorial.pdf .

21. Эксперт Хугин, Технический Документ./ Эксперт Хугин - http://download.hugin.com / webdocs/технический документ/huginexpert-технический документ.pdf.

22. Гаврилова, Т.А. Инженерия знаний. Модели и методы. / Т.А. Гаврилова, Д.В. Кудрявцев, Д.И. Муромцев. — СПб.: Издательство «Лань», 2016. — 324 с.

23. Копайгородский, А.Н. Применение онтологий в семантических информационных системах / А.Н. Копайгородский // Онтология проектирования. – № 4 (14). – 2014. – С.78-89.

24. Ворожцова, Т.Н. Онтология как основа для разработки интеллектуальной системы обеспечения кибербезопасности / Т.Н. Ворожцова // Онтология проектирования. – № 4 (14). – 2014. – С.69-77.

25. Сатыбалдина, Д.Ж. Оценка рисков информационной безопасности на основе нечеткой логики / Д.Ж. Сатыбалдина, А.А. Шарипбаев // Знания – онтологии – теории: сборник трудов II Всероссийской конференции с международным участием – Новосибирск, 2009. – С. 216-220.

26. Фентон, Н. Оценка рисков и анализ решений с использованием байесовских сетей./ Н. Фентон, М. Нил, - Королева Мария, Лондонский университет и Agena Ltd. CRC press. - ISBN: 9781439809105, ISBN 10: 1439809100.

27. Громов, Ю.Ю. Применение теории нечетких множеств в решении задачи оценки рисков сетевых информационных систем / Ю.Ю. Громов, О.Г. Иванова, С.В. Проскуряков, М. Аль-Балуши // Современные информационные технологии. – 2013. – № 17. – С. 82-91.

28. Басакер, Р. Конечные графы и сети/ Р. Басакер, Т. Саати - М.: Наука, 1974. - с. 205-278.

29. Гавришев, А.А. Анализ программ моделирования нечетких систем/ А.А. Гавришев// Дистанционное и виртуальное обучение. - 2017. - № 6. - с. 76-83.

30. Баранов, В.В. Анализ модели информационной поддержки процессов и систем при реализации многоагентного интеллектуального взаимодействия / В.В. Баранов, Е.А. Максимова и О.С. Лаута// Устройства и системы. Управление, контроль, диагностика. 2019. № 4. С. 32-41.

31. Баранов, В.В. Автоматизация разработки методов защиты объектов информатизации/ В.В. Баранов, А.В. Секретарев, А.Р. Игнатьева // Социотехнические и гуманитарные аспекты информационной безопасности. Материалы Всероссийской научно-практической конференции. 2019. С. 21-30.

32. Баранов, В.В. Прогнозирование разрушительных вредных воздействий на объекты критической информационной инфраструктуры./ В.В. Баранов, Е.А. Максимова // Коммуникации в компьютерных и информационных науках, 2021, 1395 CCIS, стр. 88-99.

33. Егошин, Н.С. Формирование модели нарушителя / Н.С. Егошин, А.А. Конев, А.А. Шелупанов // Безопасность информационных технологий. – 2017. – Т. 24. – №4. – С. 19–26. – DOI: 10.26583/bit.2017.4.02

34. Егошин, Н.С. Модель угроз безопасности информации и ее носителей / А.К. Новохрестов, А.А. Конев, А.А. Шелупанов, Н.С. Егошин // Вестник Иркутского государственного технического университета. – 2017. – Т. 21. – №12(131). – С. 93–104. – DOI: 10.21285/1814-3520-2017-12-93-104

35. Агеев, С.А. Оценка рисков сетевой компьютерной безопасности на основе нечеткого логического вывода / С.А. Агеев, И.Б. Саенко // ИБРР-2017: X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России». – Санкт-Петербург: СПб.: СПОИСУ, 1-3 ноября, 2017. – Том 3. – С. 28–30

36. Шангытбаева, Г.А. Анализ методов повышения эффективности выявления распределенных сетевых атак / Г.А. Шангытбаева, А.А. Жумагулова, Ж. Жумагалиева // Вестник Казахской академии транспорта и коммуникаций им. М. Тынышпаева. – 2015. – № 2-3 (93). – С. 108-114.

37. Чечулин, А.А. Методика построения графов атак для систем анализа событий безопасности / А.А. Чечулин // Инновации в науке. – 2013. – № 16-1. – С. 156-160.

38. Баранов, В.В. Методика количественной оценки угроз безопасности информации в защищенных информационных системах/ В.В. Баранов, А.Н. Шилина // Информационные системы и технологии. 2022. № 2 (130). С. 92-99.

39. Свидетельство о государственной регистрации программы для ЭВМ № 2022616409 «Автоматизированная система разработки модели угроз безопасности информации в организации» (АСРМ УБИ).

40. Свидетельство о государственной регистрации программы для ЭВМ № 2022665542 «Информационная система поддержки принятия решений при разработке системы защиты информации» (ИС ППР РСЗИ).

Губарева О.Ю.
ФГБОУ ВО ПГУТИ, начальник УНИД, к.т.н.,
o.gubareva@psuti.ru

ПРИНЦИПЫ И РЕШЕНИЯ ПО СОВЕРШЕНСТВОВАНИЮ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ С КОМПАКТНЫМИ ПЛОТНЫМИ ОПТОВОЛОКОННЫМИ СЕТЯМИ ДАННЫХ

Аннотация: в работе рассматриваются алгоритмы определения местоположения источника звука (злоумышленника) с применением системы распределенных акустических сенсоров в двумерном и трехмерном пространстве, в частности, простой алгоритм триангуляции и алгоритм триангуляции со смещением источника звука. Предложенные в работе алгоритмы могут быть использованы для построения вспомогательных систем безопасности для предотвращения хищения информации и/или ценного имущества. Также в работе было проведено моделирование влияния источника гармонического акустического воздействия на систему распределенных акустических сенсоров, по результатам которого расстояние от оптического волокна до места расположения источника гармонического акустического воздействия (нарушителя) могло быть определено с погрешностью до 10-15% и менее.

Ключевые слова: акусто-оптоволоконный канал, оптическое волокно, утечка информации, технология «волокно к рабочему месту», распределенный оптоволоконный акустический сенсор, компактные оптоволоконные сети данных, система физической защиты.

Актуальность темы исследования

Ранее в научных работах для всех известных решений оптическое волокно (ОВ) рассматривалось как разнесенный акустический сенсор, но никогда в качестве разнесенного акустического сенсора не рассматривалась система ОВ, разнесенных в 3D-пространстве.

Развитие цифровой экономики, которая базируется на развитии информационных сетей, послужило толчком к созданию системы разнесенных в пространстве ОВ, проложенных на объекте. Данные системы дают новые возможности как злоумышленникам, так и появляются новые возможности с точки зрения защиты информации. В частности, становится возможным не только съем аудиоинформации, но и определение местоположения источника звука с заданной точностью и последующей идентификацией источника звука. К примеру, злоумышленник, наблюдая за 3D-моделью системы разнесенных в пространстве ОВ может определить, какие именно сотрудники работают в каких помещениях, отследить распорядок их дня и т.д. С точки зрения безопасности объекта системы видеонаблюдения можно дополнять системами аудиоконтроля и создавать полные 3D-модели пространства, ввиду чего целесообразным является разработка моделей распределенных волоконно-оптических акустических сенсоров, разнесенных в 3D-пространстве.

Степень разработанности темы исследований

Современная криминогенная ситуация в мире в целом и в Российской Федерации в частности свидетельствует о высокой необходимости обеспечения безопасности промышленных объектов. Урон от успешных действий злоумышленников все чаще оказывается слишком серьезным для различных объектов. Наличие широкого спектра угроз предполагает осуществление адекватных мероприятий по противодействию им и обеспечению безопасности на всех уровнях объекта. Традиционные системы видеонаблюдения легко обмануть, зная место расположения камер на объекте, многие из которых в целях экономии ресурсов настроены на включение и запись по движению. Существующие радиоволновые датчики, вибрационные датчики и сейсмические датчики не применяются внутри помещений и не подходят для определения местоположения злоумышленника внутри крупных офисных зданий [1].

До недавнего времени для решения задач определения точного местоположения наиболее широко были распространены распределенные беспроводные сенсоры (wireless sensor networks – WSN) [2-8]. Однако WSN не обладают достаточной точностью определения местоположения сенсора, что в свою очередь влияет на погрешность локализации источника звука [7,8].

Для решения проблемы определения с заданной точностью местоположения злоумышленника на охраняемом объекте предложено использовать имеющиеся на объекте волоконно-оптические линии связи (ВОЛС) с установленными на них распределенными акустическими сенсорами – DAS (Distributed Acoustic Sensors) [9-13], один из методов реализации предложен Губаревой О.Ю. и Бурдиным В.А. в патенте RU2671855. Системы TDOA (Time Difference of Arrival), построенные на

основе DAS, имеют размах по расстоянию между сенсорами менее 1 м и чувствительность до 90 дБ [14-16]. Стоит учесть, что помимо искомого источника акустического воздействия на сенсор воздействуют множество других факторов, в том числе источники посторонних шумов, флуктуации среды, в которой находится ОВ, микро-, макро-изгибы, а также сжатие и растяжение самого ОВ [17]. Также стоит сказать о возможности реализации злоумышленником акусто-оптоволоконного канала утечки акустической и, в частности, речевой информации (РИ).

Гришачев В.В., Халяпин Д.Б. и Шевченко Н.А. в патентах RU2416166, RU2416167 предлагают способы защиты ОВ активным локализованным акустическим зашумлением. Недостаток методики заключается в том, что злоумышленник может отфильтровать локальное воздействие на ОВ с помощью известных способов спектрального анализа [18-21].

В патентах US5381492 (Дж.Б. Дули, Дж.Д. Махс, В.Т. Кеннет) и US20120224182 (Э. Тапанес) описаны способы, фиксирующие наличие оптического излучения в ОВ. Однако они не позволяют выделить сигналы, передаваемые при несанкционированном подключении к ОВ. Гришачевым В.В. в патенте RU2428798 описаны способы обнаружения акусто-оптоволоконного канала утечки конфиденциальной РИ в волоконно-оптическом канале, базирующиеся на DAS и фазочувствительных импульсных оптических рефлектометрах [22, 23]. Основным недостатком методик является отсутствие возможности определения наличия последовательности нештатных импульсов в ОВ – одного из основных признаков наличия канала утечки.

На сегодняшний день практически все здания имеют сеть ВОЛС. Свободные ОВ могут быть успешно использованы в качестве DAS для определения местоположения источника звука, и, в том числе, злоумышленника. По полученным данным предлагается выстроить цифровую 3D-карту объекта с наложением на систему видеонаблюдения для формирования адекватных моделей угроз, с использованием существующих на объекте средств выявления, идентификации и классификации угроз нарушения информационной безопасности для объектов различного вида и класса, а также для дополнения технологии идентификации пользователей на объекте.

Целью работы является разработка принципов и решений по созданию новых и усовершенствовании существующих средств защиты информации на объектах с компактными плотными оптоволоконными сетями данных.

Для достижения поставленной цели в работе решаются следующие задачи:

— разработка моделей угроз хищения аудиоинформации распределенными волоконно-оптическими акустическими сенсорами, разнесенными в 3D-пространстве;

— разработка алгоритмов идентификации и определения местоположения пользователя/персонала или иного лица в 3D-пространстве на основе применения системы распределенных и разнесенных оптоволоконных акустических сенсоров;

— разработка средств защиты информации на объектах с компактными плотными оптоволоконными сетями данных;

— экспериментальная проверка предлагаемых решений.

Объектом исследования являются компактные плотные оптоволоконные сети данных при наличии или отсутствии акустических воздействий.

Предметом исследования являются совокупность методов и средств определения местоположения пользователя/персонала или иного лица в 3D-пространстве на основе применения системы распределенных и разнесенных оптоволоконных акустических сенсоров.

Методы исследования. Поставленные в работе задачи решались методами математического моделирования, системного анализа, теории оптических волноводов, цифровой обработки сигналов, вычислительной математики, защиты информации, экспертного оценивания, проведением экспериментальных исследований на физических моделях.

Достоверность изложенных положений работы обосновывается корректным выбором исходных данных, строгим использованием математического аппарата, системным подходом к решению поставленных задач, обоснованием выбранных методов и алгоритмов идентификации и определения местоположения пользователя/персонала или иного лица в 3D-пространстве на основе применения системы распределенных и разнесенных оптоволоконных акустических сенсоров, результатами натурных экспериментов на ВОЛС предложенных алгоритмов, анализом работ существующих зарубежных и отечественных практик решения аналогичных задач, апробацией результатов работы на международных и российских конференциях, а также подтверждением о внедрении предложенных методов и алгоритмов в организациях и предприятиях.

Положения, выносимые на защиту:

1. Модель угроз хищения аудиоинформации распределенными волоконно-оптическими акустическими сенсорами, разнесенными в 3D-пространстве.

2. Алгоритмы идентификации и определения местоположения злоумышленника/пользователя/персонала или иного лица в 3D-пространстве на основе применения системы распределенных и разнесенных оптоволоконных акустических сенсоров.

Научная новизна данного исследования заключается в:

1. Разработаны модели угроз хищения аудиоинформации распределенными волоконно-оптическими акустическими сенсорами, разнесенными в 3D-пространстве;

2. Разработаны принципы и решения по созданию новых и усовершенствовании существующих средств защиты информации на объектах с компактными плотными оптоволоконными сетями данных.

Теоретическая значимость данного исследования заключается в разработке новых и методов, алгоритмов и технологий идентификации и определения местоположения злоумышленника/пользователя/персонала или иного лица в 3D-пространстве на основе применения системы распределенных и разнесенных оптоволоконных акустических сенсоров. Полученные результаты могут быть использованы для развития теоретической базы угроз ИБ связанных акустооптоволоконным каналом утечки информации.

Практическая значимость работы заключается в заключается в обеспечении защиты информации на объектах с плотной оптоволоконной кабельной сетью, а так же предложен алгоритм идентификации и определения местоположения пользователя/персонала или иного лица в 3D-пространстве на основе применения системы распределенных и разнесенных оптоволоконных акустических сенсоров, на основе которого планируется разработать цифровую 3D-карту объекта с наложением на систему видеонаблюдения для формирования адекватных моделей угроз, с использованием существующих на объекте средств выявления, идентификации и классификации угроз нарушения информационной безопасности для объектов различного вида и класса, а также для дополнения технологии идентификации пользователей на объекте. Разработанные алгоритмы повышают надежность, функционирования системы защиты информации на объектах с компактными плотными оптоволоконными сетями данных, путем снижения количества реализованных инцидентов нарушения ИБ.

Реализация и внедрение работы. Разработанные алгоритмы и системы на их основе внедрены в ООО «А4 Сенсорс» и ООО «НПК», а так же используются при проведении лабораторных работ по дисциплине «Средства физической защиты объектов» для подготовки специалистов по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» и бакалавриата по направлению подготовки 10.03.01 «Информационная безопасность» в ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики».

Апробация работы. Результаты работы докладывались на российских и международных научно-технических конференциях и форумах: XXVI – XXIX Российская научная конференция профессорско-преподавательского состава, научных сотрудников и аспирантов (ПГУТИ, Самара, 2019-2022 гг.); XI, XII международная конференция «Фундаментальные проблемы оптики» (ИТМО, Санкт-Петербург, 2019-2020 гг.); X Всероссийская научно-практическая конференция «Проблемы передачи информации в инфокоммуникационных системах» (ВолГУ, Волгоград, 2019 г.); II – IV Научный форум «Телекоммуникации: теория и технологии», XVII – XIX международная научно-техническая конференция «Оптические технологии в телекоммуникациях», (КНИТУ-КАИ, Казань, ПГУТИ, Самара, 2019-2021 гг.); VI, VIII Международная конференция и молодежная школа «Информационные технологии и нанотехнологии» (Самарский университет, Самара, 2020, 2022 гг.); 19th, 21nd International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networks and Systems, совместно с 12th, 14th Conference on Internet of Things and Smart Spaces (Springer, Санкт-Петербург, 2019, 2021 гг.); Всероссийская научно-теоретическая конференция «Теория и практика обеспечения информационной безопасности» (МТУСИ, Москва, 2021 г.); 23rd International Conference of Young Professionals in Electron Devices and Materials (IEEE, Эрлагол, 2022 г.); International Conference on Electronics, Engineering Physics and Earth Science (CIEES, Варна, 2022); Международный семинар по волоконным лазерам (НЦВО РАН, Новосибирск, 2022 г.).

Результаты исследования были представлены на следующих научных конкурсах: конкурс на назначение денежных выплат молодым ученым и конструкторам, работающим в Самарской области (Министерство образования и науки Самарской области, г. Самара, 2021 г.) – выплаты на 2021 г., Всероссийский конкурс научных проектов аспирантов, соискателей и молодых ученых на проведение

научных исследований и разработок в области информационной безопасности для задач цифровой экономики «Гранты ИБ МТУСИ» (МТУСИ, Москва, 2021 г.) – грант на 2021-2022 гг.

1. Анализ угроз хищения аудиоинформации на компактных плотных оптоволоконных сетях данных

Результаты оценки угроз хищения аудиоинформации необходимы для выбора и обоснования требуемых мер при построении систем защиты информации на компактных плотных оптоволоконных сетях данных. В свою очередь определение перечня угроз и построение модели нарушителя являются обязательным этапом проектирования системы защиты. Ввиду чего в работе были сформулированы ключевые понятия для экспертной системы оценки угроз. Приведена схема работы экспертной системы оценки угроз хищения аудиоинформации безопасности информации для компактных плотных оптоволоконных сетей данных. Проанализирована международная практика управления рисками ИБ на основе общепринятых стандартов.

2. Обзор средств защиты от хищения аудиоинформации с помощью оптоволоконных сенсоров

Были определены ключевые аспекты инфраструктуры компактных плотных оптоволоконных сетей данных и средства их защиты. Рассмотрены основные способы маскировки звуковых сигналов: применения технических средств защиты речевой информации, применение звукопоглощающих материалов и конструкций, звукоизоляция помещений.

3. Разработка моделей угроз хищения аудиоинформации распределенными волоконно-оптическими акустическими сенсорами, разнесенными в 3D-пространстве

При решении практических задач защиты информации большое значение имеет количественная оценка ее уязвимости. В работе приведены результаты анализа моделей и методов моделирования угроз хищения аудиоинформации распределенными волоконно-оптическими акустическими сенсорами, моделей атак и угроз, методов и методик оценки эффективности средств защиты информации, а также результаты анализа международных стандартов и нормативных правовых актов регуляторов в области обеспечения ИБ.

4. Разработка алгоритмов идентификации и определения местоположения пользователя/персонала или иного лица в 3D-пространстве на основе применения системы распределенных и разнесенных оптоволоконных акустических сенсоров

Рассматриваемые в работе алгоритмы определения местоположения источника звука (злоумышленника) основываются на использовании DAS. Подобные сенсоры акустического мониторинга в своем составе имеют фазочувствительный оптический рефлектометр (PH-OTDR), работающий во временной области, к которому подключено ОВ, служащее сенсором. DAS отличаются высокой чувствительностью и удовлетворительным разрешением. Распределенное акустическое зондирование — это технология, в которой используется явление, заключающееся в том, что амплитуда и фаза рэлеевского обратного рассеяния света в ОВ очень чувствительны к внешним акустическим сигналам и механическим вибрациям; внешние динамические возмущения могут быть определены количественно и локализованы в зависимости от расстояния по всему ОВ с помощью соответствующих алгоритмов обработки [24, 25]. Благодаря непрерывной оптимизации производительности современные системы DAS способны количественно определять и локализовать возмущения с пространственным разрешением сантиметрового порядка и частотным разрешением от 20 Гц до 2 кГц на расстоянии до 70 км [26-28].

4.1. Алгоритм распределенной локализации акустического источника, основанный на методе ASP

Для локализации источника звука с помощью метода обработки сигналов массива (Array Signal Processing - ASP) применяется пространственная корреляция. DAS преобразует ОВ в распределенный массив акустических сенсоров. В случае с ASP нельзя пренебрегать разницей между эквивалентным массивом сенсоров и массивом точечных измерений, а именно чувствительными элементами, расстоянием между элементами массива, апертурой массива и т.д. При построении модели массива необходимо учесть следующее: канал обнаружения DAS отличается от точечных сенсоров, искомый сигнал представляет собой интеграл акустических сигналов в пространственном диапазоне вдоль чувствительного волокна и получается из пространственной разности фаз между двумя положениями [28-30]. В свою очередь дифференциальная длина волокна определяется как $\Delta x = x_{i,1} - x_{i,0}$, что является калибровочной длиной, а соответствующий пространственный масштаб называется апертурой элемента массива. Далее определяется расстояние между элементами массива, для точечных измерений расстояние между элементами массива — это расстояние между двумя соседними точечными датчиками, но при этом нельзя пренебрегать апертурой элемента массива. Интервалом

между элементами массива является расстояние между начальными положениями двух соседних измерительных каналов, $d_i = x_{i,0} - x_{i-1,0}$, а апертура массива определяется как расстояние от начала первого элемента до конца последнего элемента, $L = x_{N,1} - x_{1,0}$, где N — количество элементов массива. Модель такого распределенного массива показана на рис. 1.

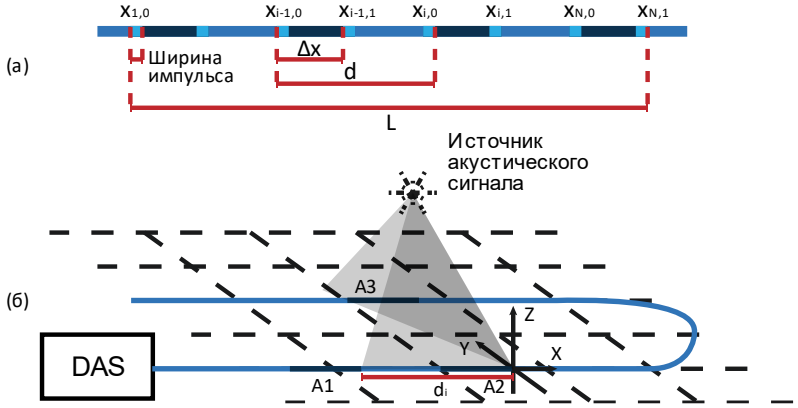


Рис. 1. Модель распределенного массива сенсоров (а) и эквивалентный массив сенсоров (б)

Для конечной обработки используется оценка пространственного спектра и рассчитывается функция пространственного спектра P_{MUSIC} (метод классической множественной классификации сигналов – multiple signal classification – MUSIC) [29].

4.2. Определение местоположения злоумышленника с помощью DAS на основе алгоритма простой триангуляции

4.2.1. Определение местоположения источника акустического воздействия на плоскости с заданной точностью

Во втором рассматриваемом способе определение местоположения источника акустического воздействия (злоумышленника), основано на применении алгоритма простой триангуляции (Algorithm of simple triangulation – AST), предполагается, что акустическое воздействие оказывается на множество точек сенсора [30]. Далее по аналогии с предыдущим алгоритмом определяются отдельные элементарные участки $x_i.x_{i+1}$ и т.д., длина которых равна калибровочной длине DAS, а ОВ представляется в виде набора элементарных участков. На рис. 2 представлено воздействие на элементарные участки ОВ источником звука, где r_0 – кратчайшие расстояние от источника звука до ОВ, при условии, что звуковая волна падает перпендикулярно на ОВ.

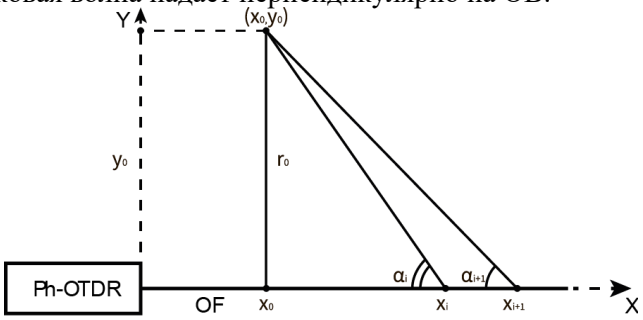


Рис. 2. Оценка расстояния от ОВ до источника акустического воздействия

Из рис.2 следует, что α_i – угол падения луча акустического воздействия на i-й элементарный участок ОВ, тогда его значение можно определить как:

$$\alpha_i = \arccos\left(\frac{\varphi_{i+1} - \varphi_i}{k \cdot \Delta x}\right), \qquad (1.1)$$

где φ – фаза, получаемая при анализе характеристики обратного рассеяния ОВ, k – волновое число, Δx – калибровочная длина, λ – длина акустической волны, c – скорость звука в воздухе, f – частота звука.

Зная, как рассчитываются волновое число и скорость звука в воздухе определим кратчайшее расстояние до источника звука:

$$x_{0i} = \frac{x_i \cdot tg\alpha_i - x_{i+1} \cdot tg\alpha_{i+1}}{tg\alpha_i - tg\alpha_{i+1}}, \tag{2.1}$$

$$r_{0i} = x_{0i} \cdot tg\alpha_i, \tag{3.1}$$

Применяя метод Равиля Нигматуллина [31], сделаем сортировку значений по убыванию с заданным ограничением, и получим, что $\langle x_{0i} \rangle \to \vec{x}_0$.

В случае для двух ОВ на плоскости кратчайшее расстояние будет лежать на оси ординат, поэтому допускаем что $r_0 \approx y_0$, тогда $\langle y_{0i} \rangle \to \vec{y}_0$.

4.2.2. Определение местоположения источника акустического воздействия в 3-D пространстве с заданной точностью

Для более точной картины местоположения злоумышленника в пространстве необходимо использовать три ОВ, разнесенных в пространстве (ОВ1, ОВ2, ОВ3), используемых в качестве акустических сенсоров, последовательно подключенных к фазочувствительному импульсному оптическому рефлектометру и источник звука – злоумышленник, который оказывает звуковые колебания на ОВ (Рис. 3).

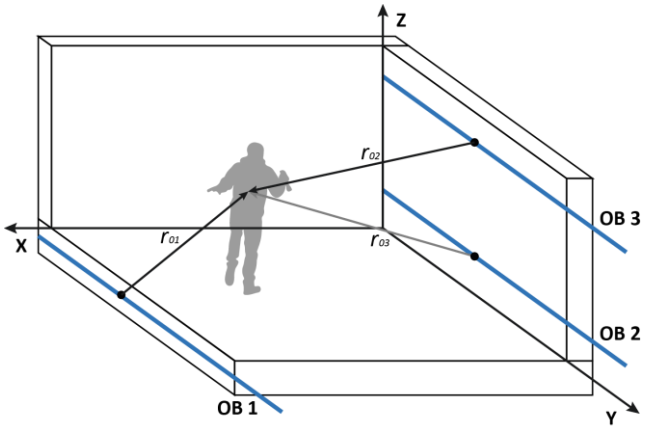


Рис. 3. Определение местоположения злоумышленника в 3-D пространстве

Для трехмерного пространства кратчайшее расстояние от ОВ до источника звука будет определяться по формуле

$$r_0 = \sqrt{z_0^2 + y_0^2 + x_0^2}, \tag{4.1}$$

где z_0 – кратчайшее расстояние до источника звука в плоскости *Z*, y_0 – кратчайшее расстояние до источника звука в плоскости *Y*, x_0 – кратчайшее расстояние до источника звука в плоскости *X*.

Для каждого из трех ОВ определим соответствующие значения x_{01}, x_{02}, x_{03}. Тогда на плоскости источник звука будет находится как пересечение трех окружностей, радиусы которых равны r_{01}, r_{02}, r_{03} соответственно (Рис.4). Далее разложим источник звука на спектральные характеристики и зададим обязательные условия $\Delta\varphi = \varphi_{i+1} - \varphi_i < 2\pi$, $k\Delta x < 2\pi$, все вычисления осуществляются только на низких частотах отсекая паразитные шумы и помехи.

Рис. 4. Определение координат источника звука

Для типичных DAS калибровочная длина лежит в пределах 1.0–10 м [25, 26]. Отклик *i*-го участка DAS запишется как [31, 32]:

$$s_i(t) = \int_{x_{i,0}}^{x_{i,1}} \eta(x) \cdot \varepsilon(x,t) dx, \tag{5.1}$$

где $\varepsilon(x,t)$ – деформация ОВ; $\eta(x)$ – коэффициент отклика, зависящий от условий прокладки кабеля, конструкции кабеля, положения ОВ в кабеле т.п.

Коэффициент $\eta(x)$ в общем случае изменяется вдоль оптоволоконного кабеля (ОК). Однако в первом приближении в пределах строительной длины ОК его можно полагать постоянным.

Если ограничиться анализом для дальней зоны, полагая, что условия для такого допущения выполняются, то акустическое поле точечного источника, воздействующее на ОВ кабеля, описывается как [32]:

$$P(t,x) = \frac{P_0}{r} \exp\left[j(\omega t - kr) \right], \quad r = \sqrt{(z-z_0)^2 + (y-y_0)^2 + (x-x_0)^2} \tag{6.1}$$

где x_0, y_0, z_0 – координаты источника акустических сигналов, x, y, z – координаты некоторой точки ОВ, ω – круговая частота, t – время; k – волновое число, P_0 – амплитуда акустического сигнала на выходе источника.

С учетом (5.1)-(6.1) регистрируемый DAS сигнал с ОВ на элементарном участке кабеля описывается как

$$P_C(t, x_i) = P_0 \cdot \exp(j\omega t) \int_{x_{i,0}}^{x_{i,1}} \frac{\eta(x)}{r} \exp(-jkr) dx. \tag{7.1}$$

4.3. Алгоритм определения местоположения злоумышленника с применением системы TDOAs, построенные на основе DAS

Данный алгоритм основан на использовании систем определения разности времени прибытия акустических сигналов, построенных на основе DAS. Локализация источника звука осуществляется путем объединения измерений, поступающих из разных узлов. С геометрической точки зрения, учитывая оценку разности времени прибытия (Time difference of arrival – TDOA), источник обязан лежать на ветви гиперболы (гиперболоида в 3D), фокусы которой находятся в точках $m_i^{(m)}$ и $m_j^{(m)}$, а вершины $c\hat{\tau}_{ij}^{(m)}$ расположены далеко друг от друга. Если источник и сенсоры являются копланарными, то местоположение источника может быть идеально получено путем нахождения пересечения двух или более гипербол (Рис. 5).

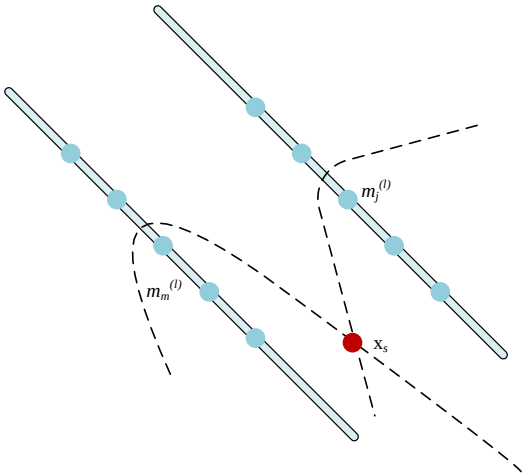


Рис. 5. Определение местоположения источника звука на пересечении гипербол, полученных из TDOAs

5. Экспериментальная проверка предлагаемых решений

Для проведения испытаний было оборудовано помещение, приближенное к реальным условиям эксплуатации. Размерность помещения составляла 5×5×2 м. В помещении присутствовали участки с мебелью вдоль ОВ и участки без неё, таким образом можно оценить влияние паразитных объектов на распространение звука в рамках помещения и на точность определения координат источника звука. В рамках тестирования испытания проводились для двух конфигураций расположения ОК. В первом случае использовался один ОК, расположенный в конфигурации (Рис. 6), где была возможность снимать характеристики распределения амплитуды и фазы звукового сигнала, воздействующего на ОВ, в трех плоскостях со смещенным центром координат, а также проводить сравнение реакции на источник акустического сигнала двух параллельных участков волокна.

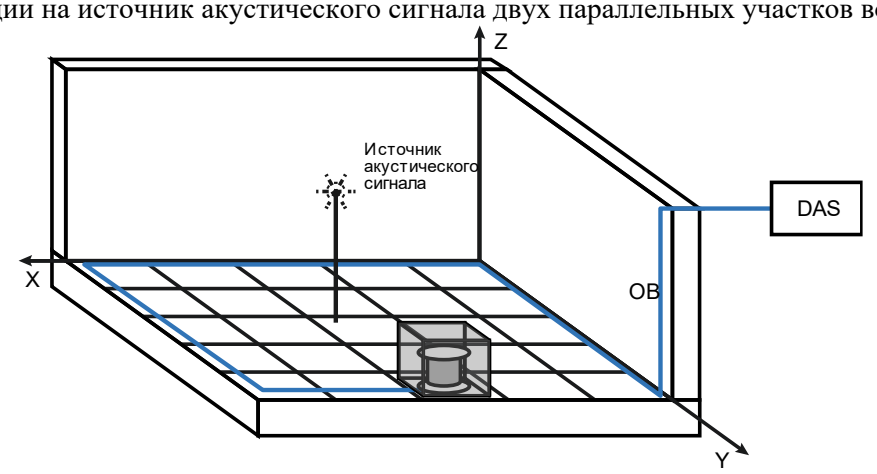


Рис. 6. Конфигурация для тестирования с одним ОК, расположенным в трех плоскостях

Как можно заметить на рис. 6, оси *X* и *Y* имеют общий центр координат, в то время как ось *Z* смещена на 5 метров. Один конец ОВ подключается к DAS, второй конец ОВ находится на буферной катушке, зафиксированной в пространстве и изолированной от различных звуковых влияний. Поскольку принцип работы DAS основан на сравнении показателей характеристик обратного рассеяния между сенсорами ОВ на расстоянии, равном калибровочной длине, изолированная часть ОВ не вносила дополнительных погрешностей при анализе поведения амплитуды и фазы акустического сигнала. Характеристики распределения амплитуды и фазы на трех участках ОВ снимались единовременно, с учетом их взаимного влияния друг на друга. Источник акустического воздействия был настроен на частоту 400 Гц. Калибровочная длина бралась в двух вариантах: 20 и 5 м.

Во второй конфигурации использовались три ОВ, расположенных в трех плоскостях с общим центром координат (Рис. 7).

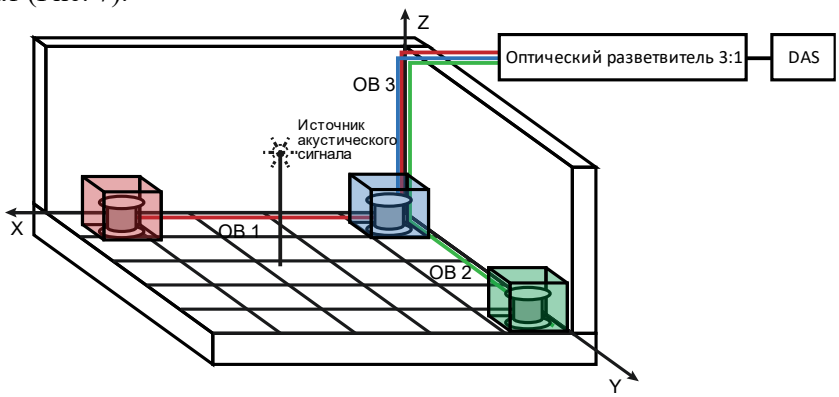
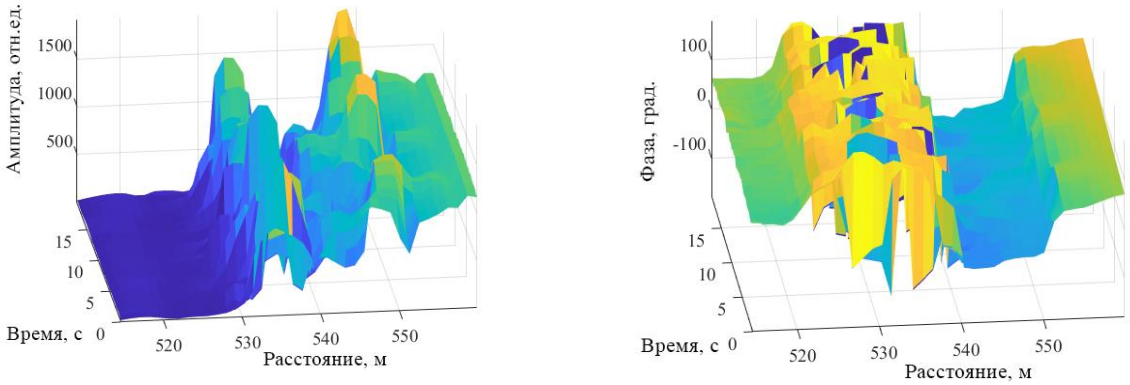


Рис. 7. Конфигурация для тестирования с тремя ОК, расположенными в трех плоскостях

Как можно видеть из рис. 7, каждое из трех ОВ с одного конца подключено к оптическому разветвителю 3:1, а с другого конца имеет буферную катушку, изолированную от акустического воздействия. ОВ из оптического разветвителя подключается к DAS. Запись характеристик трех ОВ производится последовательно, затем их показатели учитываются в объединенной форме.

На рис. 8 приведены результаты вычислений распределений амплитуды и фазы отношения $P(t,x)P_0$ вдоль ОВ при условии, что ОК проложен прямолинейно. При этом полагали, что источник акустического сигнала находится в воздухе, частота акустического сигнала 400 Гц и скорость распространения звука в воздухе 331 м/с.



а) б)

Рис. 8. Распределение амплитуды (а) и фазы (б) вдоль ОВ для конфигурации с одним ОК

Согласно полученным результатам, как наиболее оптимальный для дальнейших исследований был выбран метод определения местонахождения нарушителя с помощью DAS на основе AST для 3D-пространства. На рис. 9 приведен график зависимости погрешности от расстояния до источника звука (уровень ОСШ – 10 дБ).

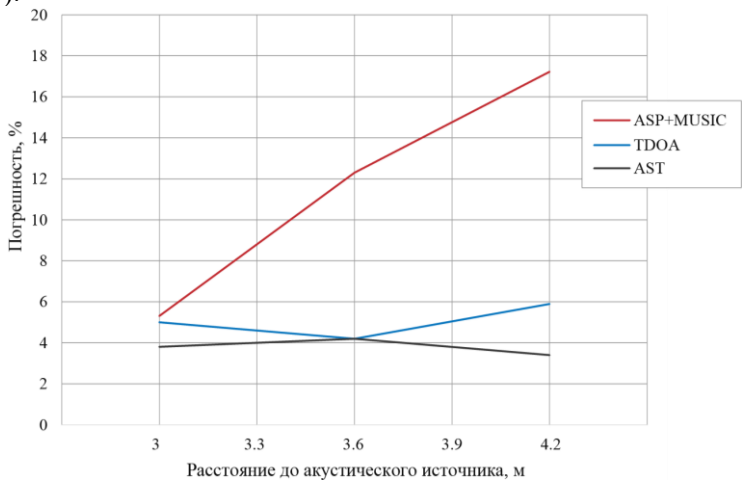


Рис. 9. График зависимости погрешности от расстояния до источника звука

Несмотря на примерно равные уровни погрешности методов TDOA и AST, метод AST является наиболее предпочтительным из-за более объемных и трудоемких вычислений для TDOA. В свою очередь метод ASP показывает низкую погрешность при намотке ОВ на структуру резонатора, что позволяет уменьшить калибровочную длину DAS, но такие конфигурации не встречаются в реальных условиях эксплуатации ВОЛС. Большой интерес для дальнейших исследований представляют конфигурации со всенаправленным источником акустического сигнала, а также конфигурации с более высокими акустическими частотами. С одной стороны, низкочастотный сигнал оказывает большее влияние на DAS. С другой стороны, он оказывает ощутимое воздействие на все окружающие предметы и конструкции, что приводит к увеличению доли паразитных влияний на различные сенсорные точки.

После выбора метода AST в качестве основного была рассмотрена возможность использования уже существующих на объектах городской застройки линий связи, основанных на таких технологиях передачи информации как «волокно до офиса» и «волокно до рабочего места» применительно к задачам физической защиты объектов. Для этого на территории ПГУТИ был подготовлен опытный полигон, на котором были проложены ОК различных конструкций, в том числе и в конфигурациях, показанных на рис. 6 и 7. Испытания проводились раздельно в условиях как отсутствия, так и наличия естественных преград. В рамках испытаний на полигоне рассмотрены аспекты применения распределенных акустических сенсоров на основе PH-OTDR для локализации источников акустического воздействия в момент реального времени, то есть для определения местоположения злоумышленника на охраняемом объекте. Была проведена оценка чувствительности оптических трактов различной конфигурации к акустическим воздействиям, соответствующим речевым сигналам предполагаемого злоумышленника. Были рассмотрены оптические тракты на основе ОВ в ОК сухой конструкции и ОВ в оптическом модуле с гидрофобным заполнением, определена зависимость влияния наличия гидрофоба в кабеле на акустические характеристики распределенного акустического сенсора. Для определения местоположения злоумышленника с заданной точностью были определены

пороговые значения чувствительности DAS. Был проведен анализ спектральной чувствительности исследуемых образцов ОВ. Измерения проводились с применением источника вибро-акустического сигнала в режиме плавного сдвига основной рабочей частоты в диапазоне 100-300 Гц при различных фиксированных уровнях мощности акустического сигнала. Проведена оценка влияния условий прохождения трассы прокладки ОК и взаимодействия ОК с окружающими объектами. Проведен анализ результатов, полученных в ходе тестовых испытаний на опытном полигоне. В результате испытаний установлена возможность локализации источника акустического сигнала акустооптическими методами, в частности методом AST. На рис. 10 показаны абсолютные погрешности оценок координат источника звука вдоль оси ОВ на частоте 200 Гц.

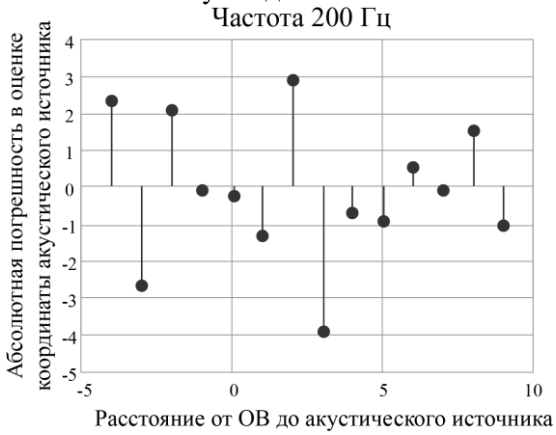


Рис. 10. Погрешность оценок координат источника звука вдоль оси ОВ

Полученные результаты позволяют использовать методику алгоритма простой триангуляции для локализации источника звука в трехмерном пространстве в реальном времени с помощью DAS на базе уже существующих на объектах городской застройки линий связи, основанных на таких технологиях передачи информации как «волокно до офиса» и «волокно до рабочего места».

6. Разработка средств защиты информации на объектах с компактными плотными оптоволоконными сетями данных

На основе полученных теоретических и экспериментальных исследований был предложен алгоритм нахождения злоумышленника на объектах с компактными плотными оптоволоконными сетями данных с заданной точностью, на основе которого планируется разработка ПО, позволяющего визуализировать местоположение источника акустических колебаний на 3-D плане охраняемого объекта, с последующей реализацией функционала по интеграции уже имеющихся на защищаемом объекте видеокамер, для реализации визуального ведения злоумышленника после определения его нахождения на объекте.

Перспективы дальнейшей разработки темы. С целью развития темы исследования в дальнейшем на её основе планируется создание системы физической защиты объектов исключающей хищение информации при помощи разнесенных в пространстве волоконно-оптических сетей, а также провести анализ эффективности локализации источника акустического сигнала (злоумышленника) на внешней территории объектов, с использованием ВОЛС, проложенных под землей.

СПИСОК ЛИТЕРАТУРЫ

1. Магауенов, Р.Г. Системы охранной сигнализации. Основы теории и принципы построения / Р.Г. Магауенов – М.: Горячая линия - Телеком, 2004. – 367.
2. Segura-Garcia, J. Low-cost alternatives for urban noisenuisance monitoring using wireless sensor networks / J. Segura-Garcia, S. Felici-Castell, J.J. Perez-Solano, M. Cobos, J.M. Navarro // IEEE Sensors Journal. – 2015. – 15. – 2. – 836-844.
3. Bertrand, A. Applications and trends in wireless acousticsensor networks: a signal processing perspective / A. Bertrand // Proc. IEEE Symposium on Communications and Vehicular Technology in the Benelux. – 2011. – 1-6.
4. Cheng, L. A survey of localization in wireless sensor network / L. Cheng, C. Wu, Y. Zhang, H. Wu, M. Li, C. Maple // International Journal of Distributed Sensor Networks. – 2012. – 2012. – 12.
5. Liu, H. Survey of wireless indoor positioning techniques and systems. / H. Liu, H. Darabi, P. Banerjee, J. Liu // IEEE Transactions on Systems, Man and Cybernetics. – 2007. – 37(6). – 1067-1080.
6. Wang, H. Wireless sensor networks for acoustic monitoring: Ph.D. dissertation. / H. Wang // University of California, Los Angeles (UCLA). Los Angeles, Calif, 2006.

7. Priyantha, N. The cricket location- support system / N. Priyantha, A. Chakraborty, H. Balakrishnan // Proc. 6th Annual International Conference on Mobile Computing and Networking. – 2000. – 32-43.
8. Raykar, V.C. Position calibration of microphones and loudspeakers in distributed computing platforms / V.C. Raykar, I.V. Kozintsev, R. Lienhart // Proc. IEEE Transactions on Speech and Audio. – 2005. – 13(1). – 70-83.
9. Bucaro J.A. Optical fiber acoustic sensor / J.A. Bucaro, H.D. Dardy, E.F. Carome // Applied Optics. – 1997. – 16(7). – 1761-1762.
10. Kim B.Y. Use of highly elliptical core fibers for two-mode fiber devices / B.Y. Kim, J.N. Blake, S.Y. Huang, H.J. Shaw // Optics Letters. – 1987. – 12(9). – 729-731.
11. Wang, Y. A comprehensive study of optical fiber acoustic sensing / Y. Wang, H. Yuan, X. Liu, Q. Bai, H. Zhang, Y. Gao, B. Jin // IEEE Access. – 2019. – 7. – 85821-85837.
12. Wild, G. Hinckley S. Acousto-Ultrasonic Optical Fiber Sensors: Overview and State-of-the-Art / G. Wild, S. Hinckley // IEEE Sensors Journal. – 2008. – 8(7). – 1184-1193.
13. Бурдин, В.А. Методы локализации источников звука в акустооптических сенсорных сетях / В.А. Бурдин, О.Ю. Губарева // Фундаментальные проблемы оптики. – 2020. – 199.
14. Трещиков, В. Dunay software and hardware complex [Электронный ресурс] / В. Трещиков // Компания Т8. – 2019. – Режим доступа: https://t8.ru/wp-content/uploads/2019/01/Dunay-2019-eng.pdf.
15. Грознов, Д.И. «Дунай» — система мониторинга активности в охранной зоне трубопровода / Д.И. Грознов, А.В. Леонов, О.Е. Наний, Е.Т. Нестеров, В.Н. Трещиков // Экспозиция Нефть Газ. – 2014. – 4(36). – 51-53.
16. Распределенный датчик акустических и вибрационных воздействий: пат. 2532562 Рос. Федерация N 2013132950/28; заявл. 17.07.13; опубл. 10.11.14, Бюл. N 31.
17. Blake, J.N. Analysis of intermodal coupling in a two-mode fiber with periodic microbends / J.N. Blake, B.Y. Kim, H.E. Engan, H.J Shaw // Optics Letters. – 1987. – 12(4). – 281-283.
18. Communicating or reproducing an audible sound: пат. 2009010392 США N 11/918,434; заявл. 12.04.06; опубл. 23.04.09.
19. Communicating or reproducing an audible sound: пат. 8000609 США N 11/918,434; заявл. 12.04.06; опубл. 23.04.09.
20. Teixeira, J.G.V. Advanced Fiber-Optic Acoustic Sensors / J.G.V. Teixeira, I.T. Leite, S. Silva, O. Frazao // Photonic Sensors. – 2014. – 4(3). – 198-208.
21. Pohl, A.A.P. Advances and new applications using the acousto-optic effect in optical fibers / A.A.P. Pohl, R.A. Oliveira, R.E. Da Silva, C.A.F. Marques, P. de T. Neves, K.Cook, J. Canning, R.N. Nogueira // Photonic Sensors. – 2013. – 3(1). – 1-25.
22. Горшков, Б.Г., Парамонов В.М., Курков А.С., Кулаков А.Т., Зазирный М.В. Распределенный датчик внешнего воздействия на основе фазочувствительного волоконного рефлектометра / Б.Г. Горшков, В.М. Парамонов, А.С. Курков, А.Т. Кулаков, М.В. Зазирный // Квантовая электроника. – 2006. – 36(10). – 963-965.
23. Нестеров, Е.Т. Волоконно-оптическая система мониторинга протяжённых объектов (нефтепроводов) на основе когерентного рефлектометра / Е.Т. Нестеров, К.В. Марченко, В.Н. Трещиков, А.В. Леонов // T-Comm. – 2014. – 1. – 25-28.
24. Masoudi, A. A distributed optical fibre dynamic strain sensor based on phase-OTDR / A. Masoudi, M. Belal, T. P. Newson // Meas. Sci. Technol. – 2013. – 24. – 085204.
25. Pan, Z. Phase-sensitive OTDR system based on digital coherent detection / Z. Pan, K. Liang, Q. Ye, H. Cai, R. Qu, and Z. Fang // Proc. SPIE. – 2011. – 8311. – 83110S.
26. Wang, S. Distributed fiber-optic vibration sensing based on phase extraction from time-gated digital OFDR / S. Wang, X. Fan, Q. Liu, Z. He // Opt. Express. – 2015. – 23. – 33301.
27. Chen, D. Distributed Fiber-Optic Acoustic Sensor With Enhanced Response Bandwidth and High Signal-to-Noise Ratio / D. Chen, Q. Liu, X. Fan, Z. He // J. Lightwave Technol. – 2017. – 35. – 2037.
28. Mompó, J.J. Sidelobe apodization in optical pulse compression reflectometry for fiber optic distributed acoustic sensing / J.J. Mompó, S. Martín-López, M. González-Herráez, A. Loayssa // Opt. Lett. – 2018. – 43. – 1499.
29. Jiajing, L. Distributed acoustic sensing for 2D and 3D acoustic source localization / L. Jiajing, W. Zhaoyong, L. Bin, W. Xiao, L. Luchuan, Y. Qing, Q. Ronghui, C. Haiwen // Opt. Lett. – 2019. – 44(7). – 1690.
30. Gubareva, O.Yu. Potential capabilities of optical distributed acoustic sensors to determine the location of an intruder / O.Yu. Gubareva // Proc. SPIE. – 2011. – 11793. – 153-163.

31. Nigmatullin, R.R. The general theory of the Quasi-reproducible experiments: How to describe the measured data of complex systems? / R.R. Nigmatullin, G. Maione, P. Lino, F. Saponaro, W. Zhang // Communications in Nonlinear Science and Numerical Simulationю – 2017. – 42. – 324-341.
32. Huang, Y.A., Audio Signal Processing for Nextgeneration Multimedia Communication Systems / Y.A. Huang, J. Benesty // Boston, MA.: Springer Science & Business Media, 2007. – 370.

Попков Г.В.
СибГУТИ, Зав. кафедрой ЗИСС, к.т.н., доцент
glebpopkov@inbox.ru

МЕТОДОЛОГИЯ ПРОЕКТИРОВАНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СВЯЗИ

В работе рассматривается методология проектирования обеспечения информационной безопасности мультисервисных сетей связи (МСС), условиями для проектирования такого рода сетей являются требования на обеспечение информационной безопасности сети в части доступности, целостности, конфиденциальности пользовательской и служебной информации, циркулирующей в мультисервисной сети связи. Для формирования целей и задач проектирования требуется создание адекватной гиперсетевой модели сети МСС, актуальной модели угроз, методики проектирования средств защиты информации для проектируемой защищённой сети связи. Разработанная методология предлагает использовать методы, алгоритмы, инструментарий, учитывающие временно – вероятностные характеристики, а также иные данные необходимые для эффективного выбора средств защиты сетей МСС. Предложенные укрупнённые алгоритмы принятия решений позволят проектировать защищённую сеть связи в условиях, приближенных к реальным условиям работы.

Ключевые слова: мультисервисные сети связи, информационная безопасность, сетевая безопасность, целостность, доступность информации.

Актуальность данной темы исследования обусловлена проблематикой, связанной с обеспечением информационной безопасности (ИБ), проектированием, строительством, эксплуатацией защищённых мультисервисных сетей связи (МСС), устойчивых к внешним деструктивным воздействиям (ВДВ).
Такие сети должны обладать высокой степенью надёжности, живучести, гарантированно обеспечивать заданную вероятность доступности, целостности, конфиденциальности, циркулирующей в них пользовательской и служебной информации. Это проблема является актуальной как для транспортных сетей большой протяжённости, так и для сетей абонентского доступа развёртываемых в населённых пунктах.
В данном случае под ВДВ подразумеваются, любые воздействия преднамеренного или непреднамеренного характера, естественного либо искусственного происхождения, влияющие на структуру сети связи либо информацию, циркулирующую в ней, ведущие к уничтожению, модификации информации, либо иным последствиям, приводящим к выходу из штатного режима работы элементов сети связи, систем управления, программного обеспечения вплоть до их полного выведения из строя (уничтожения).
Важными факторами, оказывающими значительное влияние на устойчивость сети связи, являются, ошибки при принятии решений в проектировании, управлении, текущей эксплуатации, модернизации, масштабировании сетей МСС, проектантами, инсталляторами, непосредственно операторами (провайдерами) сетей связи.
Для детерминированных сетей связи, важны возможности систем управления сетью связи, поддерживать работоспособность сети МСС в заданных пределах на определённый отрезок времени воздействия ВДВ с определёнными ограничениями.
Очевидно, что при различных вариантах событий могут использоваться различные средства и способы достижения цели ВДВ нарушителем. В случае возникновения стихийных природных воздействий, должны учитываться такие факторы как мощность, масштаб вероятного воздействия, климатические условия, особенности местности, на которой расположены элементы сетей МСС.

Учитывая повышающиеся требования со стороны конечного пользователя телекоммуникационных услуг (сервисов), так и со стороны операторов связи, к предоставлению качества услуг на сетях МСС, необходимо эффективно проектировать, строить, эксплуатировать устойчивые сети связи к любым ВДВ.

Одним из важных направлений в проектировании защищённых систем связи, а также информационных систем в широком смысле являются законодательно определённые структуры с повышенными требованиями к безопасности, это объекты КИИ (критические информационные инфраструктуры).

Криптографические методы защиты информации в данной работе не рассматривались.
По мнению автора, задача разработки методики проектирования и обеспечения информационной безопасности сетей МСС, представляет собой многокритериальную трудноразрешимую проблему и

характеризующуюся пространственной и алгоритмической сложностью. Это в свою очередь требует внедрения современных математических методов и алгоритмов, позволяющих более эффективно проектировать обеспечение информационной безопасности для сетей МСС. Создание эффективной методологии проектирования защищённых сетей МСС, позволит решать эти задачи более эффективно по выбранным критериям с лучшим экономическим эффектом.

Применение корректных математических постановок задач, а также адекватных математических моделей, основанных на теории гиперсетей, теории массового обслуживания, алгоритмического подхода в задачах поиска решений, позволит при проектировании устойчивой сети связи, рассматривать сеть МСС как сложный, гетерогенный, многофункциональный объект, функционирующий в условиях ВДВ.

Научная проблема, решению которой посвящена диссертация - создание методологии проектирования обеспечения информационной безопасности мультисервисных сетей связи.

Актуальность рассмотренной проблематики подтверждается тем фактом, что она затрагивает технологии, которые имеют важное социально – экономическое значение и важное значение для обороноспособности страны и безопасности государства (т. называемые критические технологии) – распоряжение Правительства РФ от 14 июля 2012 г. № 1273-р (19 пункт: “Технологии поиска, сбора, хранения, обработки, предоставления, распространения и защиты информации”)

Цель работы - создание методологии, инструментария для решения задач обеспечения информационной безопасности, проектирования, планирования, синтеза устойчивых сетей МСС с учётом влияния ВДВ.

В соответствии с поставленной целью необходимо решить следующие задачи:

1. Провести анализ существующих подходов для решения задач обеспечения информационной безопасности для сетей МСС.
2. Провести анализ частных моделей нарушителя, угроз, уязвимостей для сетей МСС.
3. Исследовать факторы временно - вероятностных характеристик, влияющих на обеспечение целостности и доступности ресурсов сети связи на определённом уровне сети МСС.
4. Провести имитационное моделирования работы СЗИ (системы СППР) в условиях ВДВ с использованием нейросетевого подхода на реальных сетях связи.
5. Разработать иерархическую нестационарную гиперсетевую математическую модель для проектирования сетей МСС в условиях ВДВ.
6. Разработать частные модели нарушителя, модели угроз, для МСС с учётом ограничений.
7. Разработать методику проектирования сети МСС устойчивой к ВДВ на основе принятой нестационарной гиперсетевой модели.
8. Разработать методы, алгоритмы, инструментарий повышения структурной надёжности, живучести сетей МСС в условиях ВДВ.
9. Разработать циркулярную сеть связи для сервиса коротких сообщений в сети МСС в случае чрезвычайных ситуаций (ГО ЧС), с использованием межсетевых шлюзов.

Объектом исследования являются методы эффективного обеспечения информационной безопасности, проектирования и построения сетей МСС устойчивых к внешним деструктивным воздействиям.

Предметом исследования является совокупность методов, алгоритмов, решений для обеспечения информационной безопасности сетей МСС с учётом внешних деструктивных воздействий.

Научная новизна

1. Разработанные имитационные модели атак ВДВ на сети МСС в отличии от известных, более полно отражают механизмы реализации атак типа “отказ в обслуживании”, что повышает адекватность модели (пункты 1, 3, 6 области исследований специальности 2.3.6).
2. Впервые предложенная иерархическая 8-ми уровневая нестационарная гиперсетевая модель (*G-Net*) сети МСС, позволяет решать задачи обеспечения информационной безопасности, проектирования сетей с ограничениями, обеспечивающая уменьшение время восстановления tвосст. элементов сети МСС в условиях ВДВ (пункты 9, 11 области исследований специальности 2.3.6).
3. Предложена методика, инструментарий проектирования (поиска оптимальных решений) устойчивой МСС к ВДВ с использованием сценарной модели угроз, позволяет эффективно выбирать актуальные средства СЗИ, СКЗИ на проектируемой сети МСС (пункты 9, 10 области исследований специальности 2.3.6).

4. Предложенная новая классификация угроз (атак) на сети МСС, отличающаяся многоуровневым распределением по видам и типу воздействия, базируется на предложенной модели *G-Net* сети МСС (пункт 1 области исследований специальности 2.3.6).

5. Разработанная частная модель угроз позволяет наиболее полно описывать инциденты информационной безопасности и связанные с ними риски на сетях МСС (пункт 1, 9, 11 области исследований специальности 2.3.6).

6. Впервые разработаны математические модели, алгоритмы построения сети циркулярной связи для сервиса коротких сообщений в сети МСС в случае ГО и ЧС, позволяющие организовать сервис передачи коротких сообщений между системами связи общего пользования (пункты 9, 10, 11 области исследований специальности 2.3.6).

7. Предложенная математическая модель топоосновы для решения задач проектирования сети МСС, позволяет наиболее полно задавать пространственные характеристики проектируемой МСС в реальных условиях городской застройки. (пункты 1, 9 области исследований специальности 2.3.6).

8. Исследованы и предложены методы, алгоритмы повышения структурной надёжности, живучести сети МСС для различных уровней гиперсетевой модели G-Net (пункты 6, 9 области исследований специальности 2.3.6).

Теоретическая значимость работы

1. Проведён анализ подходов обеспечения информационной безопасности сетей МСС с учётом ВДВ, определены недостатки существующих подходов, намечены пути решения задач, связанных с проектированием защищённых сетей МСС.

2. Определены факторы, достоинства и недостатки существующих подходов, влияющие на обеспечение информационной безопасности МСС, определены недостатки существующих методов создания, моделей нарушителя, угроз, уязвимости, влияющие на проектирование защищённых МСС.

3. Проведена модернизация существующих гиперсетевых математических моделей сетей МСС, основанная на декомпозиции элементов сети МСС с учётом внешних деструктивных воздействий.

4. Новые положения, заключаются в разработке новых методов исследований, моделирования, многокритериального проектирования сетей МСС в условиях ВДВ учитывают (распределённую архитектуру построения, циркуляцию разнородного трафика, ограниченность сетевых ресурсов, поддержания QoS) с учётом систем мониторинга и управления.

5. Предложены эвристические алгоритмы поиска мест расположения межсетевых узлов, для обеспечения сервиса коротких сообщений в сети МСС в условиях ГО и ЧС.

6. Разработаны методики, алгоритмы, повышения структурной надёжности, живучести сети МСС на различных уровнях гиперсетевой *G-Net* модели.

Практическая значимость работы

Предложенная методология позволит рассчитывать характеристики сети МСС в условиях ВДВ при различных наборах исходных данных, топологии сети, известных атак с учётом “профиля атаки”, сценарной модели угроз, задающего временно – вероятностные характеристики существующих и потенциальных угроз для обеспечения информационной безопасности МСС. Это позволит увеличить возможное количество вариантов и позволит выбирать из них наиболее оптимальный на основе строгого анализа, обеспечивать высокий уровень информационной безопасности сети МСС в условиях ВДВ, повысить качество проектируемых защищённых МСС, уменьшить время принятия решений при реальном проектировании, планировании, за счёт применения комплексных решений.

Методология и методы диссертационного исследования

Методической основой для решения поставленных задач являются: теория графов и гиперсетей, теория массового обслуживания, теория множеств, алгоритмический подход.

Положения, выносимые на защиту

1. Предложенные методы, математические модели, алгоритмы, инструментарий для решения задач по проектированию защищённых сетей МСС, позволяют более полно решать частные задачи, связанные с обеспечением, вероятности целостности, доступности, конфиденциальности пользовательской, служебной информации, циркулирующей в сети МСС.

2. Разработана актуальная модель угроз, для сетей МСС.

3. Результаты проведённого имитационного моделирования работы системы IDS/IPS позволяют более эффективно оценивать воздействия ВДВ на приложения, работающие в реальном времени в сети МСС.

4. Применённая нейросетевая технология позволяет более эффективно применять (использовать) обучаемую систему IPS/IDS (систему СППР) работающую в реальных условиях воздействия ВДВ.

5. Разработанная комплексная математическая гиперсетевая восьмиуровневая модель, позволяет более эффективно проектировать защищённые сети МСС.

6. Предложенные методы и алгоритмы позволяют повысить структурную надёжность, живучесть сетей МСС в условиях ВДВ.

7. Впервые предложенная математическая модель топоосновы для реализации задач, связанных с проектированием, планированием сетей МСС в условиях ВДВ, позволит эффективно учитывать градостроительные и иные факторы, в процессе реального проектирования.

Первая глава посвящена анализу современного состояния обеспечения информационной безопасности мультисервисных сетей связи (МСС), приведено описание существующих и перспективных методов проектирования защищённых сетей МСС, в условиях ВДВ.

В последние годы, проводя анализ существующей ситуации на сетях МСС всё более актуальными становятся вопросы, связанные с поддержанием уровня информационной безопасности услуг и сервисов, реализуемых сетями МСС на должном уровне.

Это касается операторов связи большой протяжённости (сетей МСС), работающих на региональном уровне, это касается операторов связи, действующих на сетях доступа в населённых пунктах. В последние годы начались радикальные изменения концептуальных положений, определяющих основные направления дальнейшего развития телекоммуникационных систем, следовательно, требования, предъявляемые к качеству предоставляемых услуг, возросли.

Это касается стратегических решений, технических решений, применяемых на сетях МСС. Вопрос разработки методологии обеспечения информационной безопасности сетей МСС устойчивых к разрушающим деструктивным воздействиям становится всё более актуальным в связи с тяжелой международной обстановкой, связанной с фактическим ведением кибервойн между странами.

Анализ основных подходов по обеспечению доступности, целостности, пользовательской, служебной информации в сети МСС показал необходимость оптимального проектирования защищённых сетей МСС, в частности сетей МСС подверженных воздействиям ВДВ.

Приведём несколько аргументов подтверждающих доводы, сделанные ранее:

1. Для обеспечения конфиденциальности, целостности, доступности информации на сети МСС необходимо осуществить полный цикл создания защищённой сети МСС с учётом жизненного цикла сети, стандартов серии X.800, модели OSI, эффективных математических гиперсетевых моделей, адекватно задающих сеть связи.

2. Применение известных подходов к обеспечению защиты информации в МСС ограничено. Это связано с ограничениями, накладываемыми на скорость обработки информации для приложений, сервисов сети МСС, работающих в реальном времени.

Исходя из вышеперечисленных проблем, предлагается, методология, обеспечения информационной безопасности сети МСС включающей в себя, планирование, проектирование, строительство защищённых сетей МСС.

Развёртывание защищённых сетей МСС должно осуществляться системно, планомерно.

Предлагается рассмотреть восемь уровней такого рода сети:

1) Уровень пользователей/абонентов услуг сети МСС;
2) Уровень, определяющий места размещения активного сетевого оборудования, сетевых элементов *NE*;
3) Уровень среды распространения сигнала (СРС), сети МСС;
4) Уровень каналов кабельной канализации, воздушных линий связи (линейные сооружения);
5) Уровень кросс - коннекта, агрегации трафика;
6) Уровень трасс транспортных магистралей сетей связи и их взаимосвязь с другими инженерными сооружениями;
7) Уровень ситуационных трасс для возможной реализации кабельных линий по территории города;
8) Уровень карты-схемы территории, охватываемой проектируемой сетью МСС.

В дальнейшем все уровни в данной работе будут рассматриваться как ресурсы защищённой сети МСС.

В главе так же дана классификация ВДВ актуальных для сетей МСС на различных уровнях модели $G-Net$, приведён анализ актуальных систем мониторинга эффективных для сетей МСС в условиях РДВ.

Во второй главе приведена перспективная математическая нестационарная гиперсетевая модель сети МСС $G-Net$, рисунок 1, модель позволяет задавать структуру сети МСС позволяющую обеспечивать информационную безопасность, проектировать защищённые сети МСС в условиях РДВ.

Предлагается определить восемь уровней такого рода модели сети МСС:

1. Уровень пользователей/абонентов услуг сети МСС (уровень $L1$).

На этом уровне предполагается определить структуру и состав пользователей предполагаемых услуг связи. Для оценки размерности сети МСС, требуется примерно определить потребность в услугах сети МСС в части, телефонной сети общего пользования, услуг сети передачи данных, услуг мобильной сети связи, услуг кабельного телевидения. Способ определения услуг по категориям абонентов, социологическое исследование, статистический анализ, имитационное моделирование социальных процессов.

2. Уровень каналов связи (уровень $L2$).

На этом уровне решаются задачи определения мест расположения сетевых элементов NE (сетевого оборудования), согласно выбранным системам связи, данный уровень базируется на уровне G_{L3} модели $G-Net$ (уровень среды распространения сигнала) и уровне GL_8 проектируемой сети МСС и соответствующих матриц тяготений между NE, учитывая тип трафика между проектируемыми узлами.

Способ определения размещения оборудования - статистический анализ, статистическое моделирование, методы экспертных оценок, задачи перспективного планирования, методы покрывающих множеств, задача Вебера, кластерный анализ.

3. Уровень среды распространения сигнала (СРС), сети МСС (уровень $L3$).

Данный уровень модели определяет состав линий связи, проектируемой МСС, рассматривается принципиальная возможность использования беспроводных или проводных систем связи (использование радиоканала, оптического кабеля, медного симметричного/коаксиального кабеля и т.п.), с учётом уровня G_{L7} (ситуационных трасс), а также топографического плана местности (уровень G_{L8}).

На уровне также перечисляются характеристики и системы взаимодействия между различными СРС, стыки между различными системами связи (проводными, беспроводными).

4. Уровень каналов (труб) кабельной канализации, воздушных линий связи (линейные сооружения), граф G_{L4}.

Данный уровень задаёт структуру линейных сооружений. Фактически, этот уровень обеспечивает реализацию кабельных систем в выделенном пространстве. Уровень G_{L4} задает структуру топологии труб кабельной канализации, с целью упаковки в них кабельных линий сети МСС. На этом же уровне определяются трассы воздушных линий связи (ВЛС), систем радиодоступа.

Как правило, структура и состав кабельной канализации, подвески кабеля на опорах ВЛС, стволов радиорелейных систем связи (РРЛ), определяются градостроительными факторами, наличием существующих систем кабельной канализации или коллекторных систем, а также возможностью их расширения и\или замены.

5. Уровень траншей, коллекторов или воздушных линий связи, трасс АЛЛС.

Данный уровень G_{L5} является определяющим для организации кросс – коннекта между узлами уровня G_{L2}. Учитывая применение тех или иных систем связи, на данном уровне учитываются количество и тип портов для организации пользовательского и служебного трафика на модели сети МСС между сетевыми элементами NE. Здесь реализуются решения о применении различных технологий систем передачи данных, а также учитывается тип пользовательского и служебного трафика, циркулирующий в сети МСС.

6. Уровень трасс транспортных магистралей сетей связи.

На этом уровне реализуются трассы прокладки кабельной канализации, иных линейных сооружений сети МСС с учетом других инженерных сооружений и возможных коллизий, возникающих в процессе строительства, так, например, по некоторым участкам могут быть реализованы несколько трасс кабельной канализации или сеть опор ВЛС

7. Уровень ситуационных трасс для возможной реализации кабельных линий по территории города (граф G_{L7}).

Этот уровень охватывает все возможные трассы пригодные для построения линейных сооружений сетей связи на заданной территории.

Как правило, данный уровень определяется в основном экспертным способом, так как зависит от массы не формализуемых факторов и подготавливается проектировщиком путем согласования структуры ситуационных трасс со многими службами города.

8. Уровень карты-схемы территории, охватываемой проектируемой сетью МСС (граф G_{L8}).

Данный уровень является базовым для любых задач, связанных с проектированием, строительством, предоставлением телекоммуникационных услуг потребителям. Обычно этот уровень задан и существует в виде генеральных схем территорий.

Таким образом, каждому уровню можно поставить в соответствие некоторый граф или гиперграф (специальным образом определенную вторичную сеть нестационарной гиперсети) так чтобы, формально можно было бы описать соответствующий уровень гиперсети представляющий первичную сеть, сети связи.

Дадим формальное определение нестационарной гиперсети. Пусть задано множество графов (гиперграфов) $G_0 = (X^0, V), G_1 = (X^1, U^1), \dots, G_0 = (X^k, U^k)$ и корневое дерево $T_0 = (Z, R)$, где $Z = z_0, z_1, \dots, z_k, R = r_1, \dots, r_k$ определяющее вложение графов G_j в $G_i (i < j)$ аналогично вложениям определяемым в гиперсетях [4] за тем лишь исключением, что вершины x_k^i и x_l^j графов G_i и G_j не тождественны, а инцидентные. Если в граф G_j отображено несколько графов $\{G_i\}$, то те вершины этих графов отображенные в вершину (узел) у графа G_j будут инцидентны узлу у и слабо инцидентны между собой. Т. е. вершины из разных графов вторичных сетей, являясь, по сути, прообразами различных по сути элементов из моделируемых систем, будут по сути различными по типу элементами и в нестационарной гиперсети.

Следовательно, они будут слабо инцидентными в узлах первичной (транспортной) сети G_o или в вершинах сети в которую они отображаются. В дальнейшем граф G_j, который отображается в граф G_i будем называть вторичной сетью (сетью абонентского доступа), а G_i-первичной (транспортной) сетью. Очевидно, что одной и той же вершине x_k^i могут быть инцидентны несколько вершин $X_k^j = \{x_{k1}^{j1}, x_{k2}^{j2}, \dots, x_{kl}^{jl}\}$ из графов $\{G_{js}\}, s = 1, \dots, l$. На множестве вершин X_k^j можно определить граф $L^j = (X_k^j, E)$.

Вершины x_{kj}^{ji} и x_{ks}^{js} квазисмежные в L^j, если соответствующие графы G_{j_i} и G_{j_s} в вершине x_k^i имеют некоторую системообразующую связь $l(x^{ji}, x^{js})$. В противном случае эти вершины только слабо инцидентны. Также как в гиперсетях ребру $u_l^j \in G_j$ в графе G_i сопоставляется цепь или некоторая связная часть между соответствующими вершинами из G_i.

На рисунке 1 приведен пример такой гиперсети. Здесь необходимо отметить, что системообразующие связи типа $\{l(x, y)\}$, вообще говоря, могут иметь разную природу и, как правило, существенно зависят от времени. В некоторых случаях, например, в системе транспортных сетей разного типа (канализация, кабель, проводник и т. п.), такими связями в транспортных узлах будут колодцы, кроссы или кабельные муфты. В этом случае, имеет смысл рассматривать объединение всех вторичных (систем связи) сетей. Однако иногда имеет смысл рассматривать сумму всех графов гиперсети H, включая и первичную сеть PS, т.е. $G = Go + G1 + \dots + Gn + \{Lj\}$.

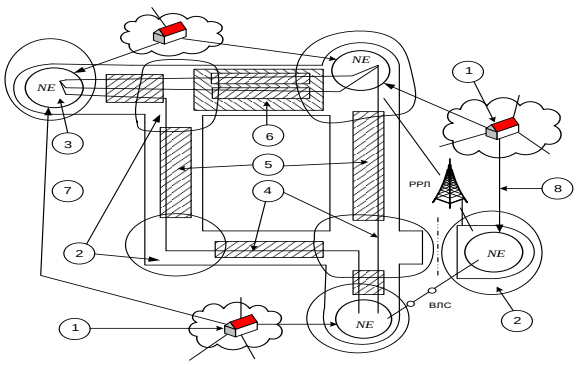


Рисунок 1 - Восьмиуровневая гиперсетевая структурная модель *G-Net* сети МСС

Так же определено понятие синтез – модели включающая в себя модель жизненного цикла сети МСС, на примере каскадной модели, стандарта безопасности МСЭ-Т Х.805, модели *G-Net*.

В главе предложен профиль атаки, рисунок 2, согласно синтезированной модели МСС:
Профиль атаки является одним из базовых элементов, определяющих ход проектирования защищённой сети МСС устойчивой к различным РДВ, используя профиль, который является вариабельным, проектировщик может получать различные варианты проектируемой сети МСС в зависимости от внешних условий и ограничений, накладываемых через параметры синтез – модели.

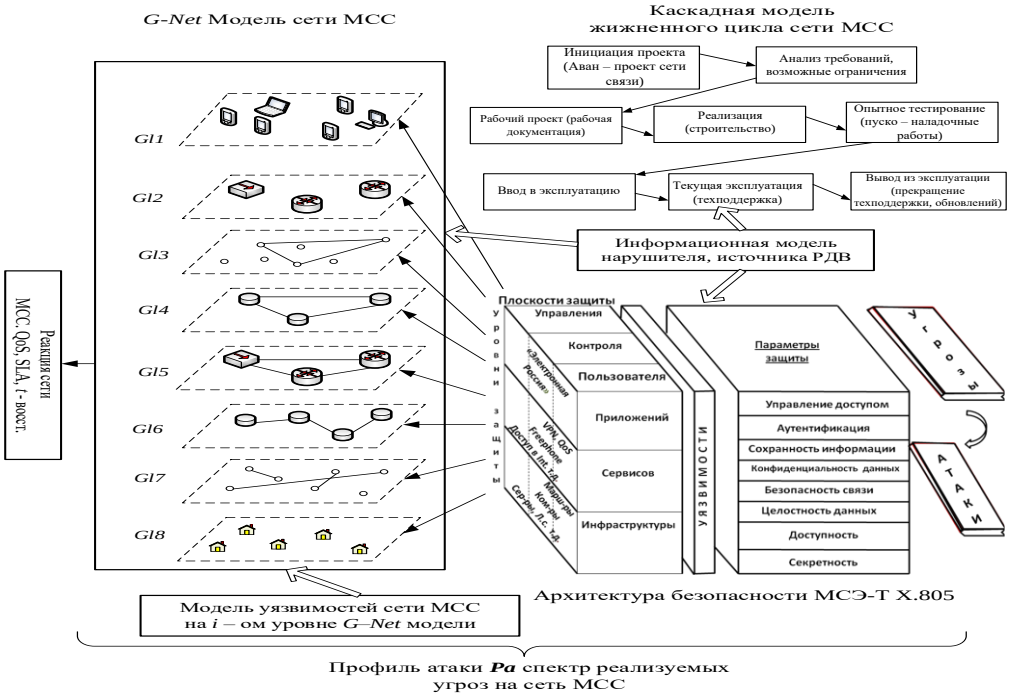


Рисунок 2 - Профиль атаки на уровни сети МСС

1.1.

Далее предложены укрупнённые алгоритмы методики проектирования защищённых МСС, а также алгоритм определения и выбора средств СЗИ, СКЗИ от профиля атаки и систем связи, проектируемых МСС в защищённом исполнении. В главе предложена актуальная модель угроз рисунок 3.

Очевидно, что для формирования профиля атаки требуется сделать систему условий для приведённой логической структуры сценарной модели угроз на сети МСС.

Сценарий модели угроз на сеть МСС согласно приведённой логической содержит 10 элементов, рисунок 3.

$$NPA_{ожс} \ni \{H_{Ext,Int}, S_A, A_i, K_S, Wi_A, I_a, V_i, P_I, R_{NPA_i}\}$$

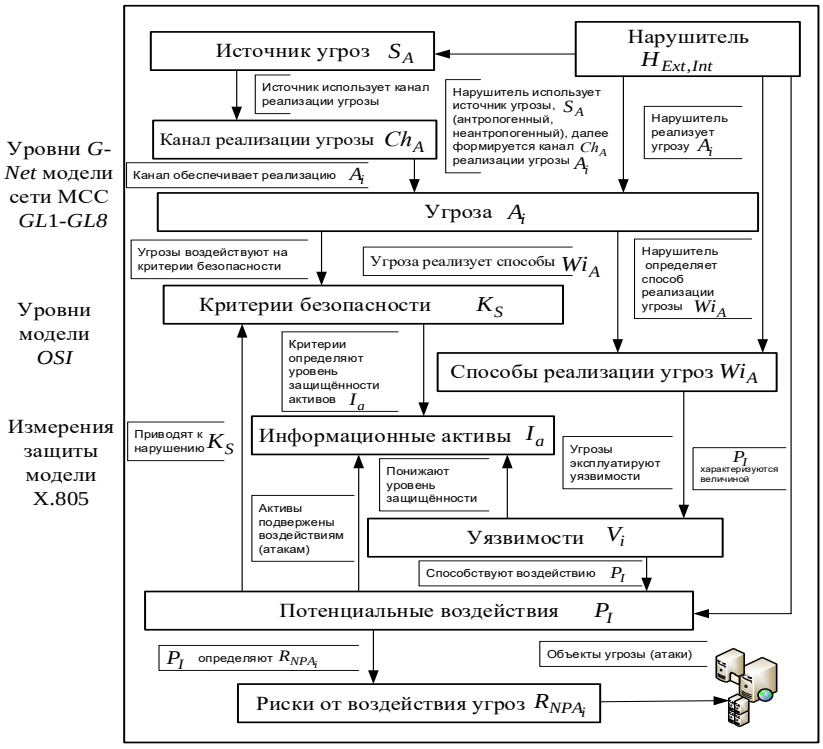


Рисунок 3. Логическая структура модели угроз информационной безопасности сети МСС

Формирование модели угроз для сетей МСС.

- Шаг 1 описание информационной системы (объекта информатизации).
- Шаг 2 описание угроз информационной безопасности.
- Шаг 3 определение актуальных уязвимостей (методы, программно – аппаратные средства).
- Шаг 4 модель нарушителя.
- Шаг 5 ранжирование потенциальных угроз согласно уровням модели OSI, модели *G-Net*, X.805, (методы, подходы, инструментарий).
- Шаг 6 способы реализации угроз.
- Шаг 7 последствия (риски) нарушения измерений ИБ.

Сценарий для сети МСС представлен ниже:

Sc *G-Net*

$$NPA_i Nl_i \ni \begin{Bmatrix} H_{Ext,int1i}^{jl1}, H_{Ext,int2i}^{jl1}, S_{Ai}^{jl1}, Ch_{Ai}^{jl1}, A_i^{jl1}, K_{Si}^{jl1}, Wi_{Ai}^{jl1}, Ia_i^{jl1}, V_i^{jl1}, Pi_i^{jl1}, R_{NPAi}^{jl1} \\ H_{Ext,int1i}^{jl2}, H_{Ext,int2i}^{jl2}, S_{Ai}^{jl2}, Ch_{Ai}^{jl2}, A_i^{jl2}, K_{Si}^{jl2}, Wi_{Ai}^{jl2}, Ia_i^{jl2}, V_i^{jl1}, Pi_i^{jl2}, R_{NPAi}^{jl2} \\ H_{Ext,int1i}^{jl3}, H_{Ext,int2i}^{jl3}, S_{Ai}^{jl3}, Ch_{Ai}^{jl3}, A_i^{jl3}, K_{Si}^{jl3}, Wi_{Ai}^{jl3}, Ia_i^{jl3}, V_i^{jl3}, Pi_i^{jl3}, R_{NPAi}^{jl3} \\ H_{Ext,int1i}^{jl4}, H_{Ext,int2i}^{jl4}, S_{Ai}^{jl4}, Ch_{Ai}^{jl4}, A_i^{jl4}, K_{Si}^{jl4}, Wi_{Ai}^{jl4}, Ia_i^{jl4}, V_i^{jl4}, Pi_i^{jl4}, R_{NPAi}^{jl4} \\ H_{Ext,int1i}^{jl5}, H_{Ext,int2i}^{jl5}, S_{Ai}^{jl5}, Ch_{Ai}^{jl5}, A_i^{jl5}, K_{Si}^{jl5}, Wi_{Ai}^{jl5}, Ia_i^{jl5}, V_i^{jl5}, Pi_i^{jl5}, R_{NPAi}^{jl5} \\ H_{Ext,int1i}^{jl6}, H_{Ext,int2i}^{jl6}, S_{Ai}^{jl6}, Ch_{Ai}^{jl6}, A_i^{jl6}, K_{Si}^{jl6}, Wi_{Ai}^{jl6}, Ia_i^{jl6}, V_i^{jl6}, Pi_i^{jl6}, R_{NPAi}^{jl6} \\ H_{Ext,int1i}^{jl7}, H_{Ext,int2i}^{jl7}, S_{Ai}^{jl7}, Ch_{Ai}^{jl7}, A_i^{jl7}, K_{Si}^{jl7}, Wi_{Ai}^{jl7}, Ia_i^{jl7}, V_i^{jl7}, Pi_i^{jl7}, R_{NPAi}^{jl7} \\ H_{Ext,int1i}^{jl8}, H_{Ext,int2i}^{jl8}, S_{Ai}^{jl8}, Ch_{Ai}^{jl8}, A_i^{jl8}, K_{Si}^{jl8}, Wi_{Ai}^{jl8}, Ia_i^{jl8}, V_i^{jl8}, Pi_i^{jl8}, R_{NPAi}^{jl8} \end{Bmatrix}$$

$$H_{Ext,Int}Nl_i \ni \begin{Bmatrix} Q_1Nl_1 \ni \{M_i^{jl1}, T_i^{jl1}, L_i^{jl1}, S_i^{jl1}, P_i^{jl1}, K_i^{jl1}, E_i^{jl1}\} \\ Q_2Nl_2 \ni \{M_i^{jl2}, T_i^{jl2}, L_i^{jl2}, S_i^{jl2}, P_i^{jl2}, K_i^{jl2}, E_i^{jl2}\} \\ Q_3Nl_3 \ni \{M_i^{jl3}, T_i^{jl3}, L_i^{jl3}, S_i^{jl3}, P_i^{jl3}, K_i^{jl3}, E_i^{jl3}\} \\ Q_4Nl_4 \ni \{M_i^{jl4}, T_i^{jl4}, L_i^{jl4}, S_i^{jl4}, P_i^{jl4}, K_i^{jl4}, E_i^{jl4}\} \\ Q_5Nl_5 \ni \{M_i^{jl5}, T_i^{jl5}, L_i^{jl5}, S_i^{jl5}, P_i^{jl5}, K_i^{jl5}, E_i^{jl5}\} \\ Q_6Nl_6 \ni \{M_i^{jl6}, T_i^{jl6}, L_i^{jl6}, S_i^{jl6}, P_i^{jl6}, K_i^{jl6}, E_i^{jl6}\} \\ Q_7Nl_7 \ni \{M_i^{jl7}, T_i^{jl7}, L_i^{jl7}, S_i^{jl7}, P_i^{jl7}, K_i^{jl7}, E_i^{jl7}\} \\ Q_8Nl_8 \ni \{\{M_i^{jl8}, T_i^{jl8}, L_i^{jl8}, S_i^{jl8}, P_i^{jl8}, K_i^{jl8}, E_i^{jl8}\} \end{Bmatrix}$$

Сценарий для модели OSI задаётся как;

$$\mathrm{Sc}OSI \left\{ \begin{array}{l} NPA_iOSIl_i \ni \begin{Bmatrix} H_{Ext,int\,1i}^{jl1}, H_{Ext,int\,2i}^{jl1}, S_{Ai}^{jl1}, Ch_{Ai}^{jl1}, A_i^{jl1}, K_{Si}^{jl1}, Wi_{Ai}^{jl1}, Ia_i^{jl1}, V_i^{jl1}, Pi_i^{jl1}, R_{NPAi}^{jl1} \\ H_{Ext,int\,1i}^{jl2}, H_{Ext,int\,2i}^{jl2}, S_{Ai}^{jl2}, Ch_{Ai}^{jl2}, A_i^{jl2}, K_{Si}^{jl2}, Wi_{Ai}^{jl2}, Ia_i^{jl2}, V_i^{jl1}, Pi_i^{jl2}, R_{NPAi}^{jl2} \\ H_{Ext,int\,1i}^{jl3}, H_{Ext,int\,2i}^{jl3}, S_{Ai}^{jl3}, Ch_{Ai}^{jl3}, A_i^{jl3}, K_{Si}^{jl3}, Wi_{Ai}^{jl3}, Ia_i^{jl3}, V_i^{jl3}, Pi_i^{jl3}, R_{NPAi}^{jl3} \\ H_{Ext,int\,1i}^{jl4}, H_{Ext,int\,2i}^{jl4}, S_{Ai}^{jl4}, Ch_{Ai}^{jl4}, A_i^{jl4}, K_{Si}^{jl4}, Wi_{Ai}^{jl4}, Ia_i^{jl4}, V_i^{jl4}, Pi_i^{jl4}, R_{NPAi}^{jl4} \\ H_{Ext,int\,1i}^{jl5}, H_{Ext,int\,2i}^{jl5}, S_{Ai}^{jl5}, Ch_{Ai}^{jl5}, A_i^{jl5}, K_{Si}^{jl5}, Wi_{Ai}^{jl5}, Ia_i^{jl5}, V_i^{jl5}, Pi_i^{jl5}, R_{NPAi}^{jl5} \\ H_{Ext,int\,1i}^{jl6}, H_{Ext,int\,2i}^{jl6}, S_{Ai}^{jl6}, Ch_{Ai}^{jl6}, A_i^{jl6}, K_{Si}^{jl6}, Wi_{Ai}^{jl6}, Ia_i^{jl6}, V_i^{jl6}, Pi_i^{jl6}, R_{NPAi}^{jl6} \\ H_{Ext,int\,1i}^{jl7}, H_{Ext,int\,2i}^{jl7}, S_{Ai}^{jl7}, Ch_{Ai}^{jl7}, A_i^{jl7}, K_{Si}^{jl7}, Wi_{Ai}^{jl7}, Ia_i^{jl7}, V_i^{jl7}, Pi_i^{jl7}, R_{NPAi}^{jl7} \end{Bmatrix} \\ H_{Ext,Int}OSIl_i \ni \begin{Bmatrix} Q_1OSIl_1 \ni \{M_i^{jl1}, T_i^{jl1}, L_i^{jl1}, S_i^{jl1}, P_i^{jl1}, K_i^{jl1}, E_i^{jl1}\} \\ Q_2OSIl_2 \ni \{M_i^{jl2}, T_i^{jl2}, L_i^{jl2}, S_i^{jl2}, P_i^{jl2}, K_i^{jl2}, E_i^{jl2}\} \\ Q_3OSIl_3 \ni \{M_i^{jl3}, T_i^{jl3}, L_i^{jl3}, S_i^{jl3}, P_i^{jl3}, K_i^{jl3}, E_i^{jl3}\} \\ Q_4OSIl_4 \ni \{M_i^{jl4}, T_i^{jl4}, L_i^{jl4}, S_i^{jl4}, P_i^{jl4}, K_i^{jl4}, E_i^{jl4}\} \\ Q_5OSIl_5 \ni \{M_i^{jl5}, T_i^{jl5}, L_i^{jl5}, S_i^{jl5}, P_i^{jl5}, K_i^{jl5}, E_i^{jl5}\} \\ Q_6OSIl_6 \ni \{M_i^{jl6}, T_i^{jl6}, L_i^{jl6}, S_i^{jl6}, P_i^{jl6}, K_i^{jl6}, E_i^{jl6}\} \\ Q_7OSIl_7 \ni \{M_i^{jl7}, T_i^{jl7}, L_i^{jl7}, S_i^{jl7}, P_i^{jl7}, K_i^{jl7}, E_i^{jl7}\} \end{Bmatrix} \end{array} \right.$$

В третьей главе рассматриваются основные процедуры, связанные с задачами, алгоритмами оптимизации защищённых сетей МСС и реализацией эффективного проектного решения и обеспечения информационной безопасности в части доступности и целостности информации для сетей МСС с учётом современных систем связи и основных существующих и перспективных сервисов, предоставляемых сетью МСС. В главе рассмотрены и даны решения задач оптимизации защищённых МСС.

Далее рассмотрим и отнесём решаемые задачи к уровням модели $G - Net$, сети МСС.

Важные задачи оптимизации для проектирования защищённых МСС в условиях ВДВ можно разбить на четыре класса:

Класс SC, задачи поиска кратчайших цепей между выделенными вершинами (полюсами) в гиперсетях и графах.

В данный класс входят задачи поиска кратчайших цепей с учётом возможных ограничений и начальных условий.

Одной из важных в этом классе является задача SC1 – поиска кратчайших цепей между парой выделенных вершин или между одной вершиной и остальными вершинами графа (задача поиска минимального растущего дерева), выполняется на уровнях $G_{L2}, G_{L4}, G_{L6}, G_{l7}$ модели $G - Net$.

Вторая задача SC2 – поиск кратчайшего пути на поверхности между двумя точками, причём на поверхности помещаются препятствия в виде полигонов (градостроительные факторы, топооснова), уровни $G_{L3}, G_{L6}, G_{l7}. G_{L8}$ модели $G - Net$.

Наиболее сложной из выше представленных, является задача SC3 – поиска системы кратчайших цепей в гиперсети с учётом стоимости (капиталовложений), рёбер и ветвей гиперсети проектируемой МСС, уровни G_{L4}, G_{L6}, G_{l7} модели $G - Net$.

На рисунке 4 приведено соответствие уровней модели $G - Net$ классам решаемых задач.

Очевидно, что эффективность предложенных решений существенно зависит от точности решения задач оптимизации на гиперсетевых моделях.

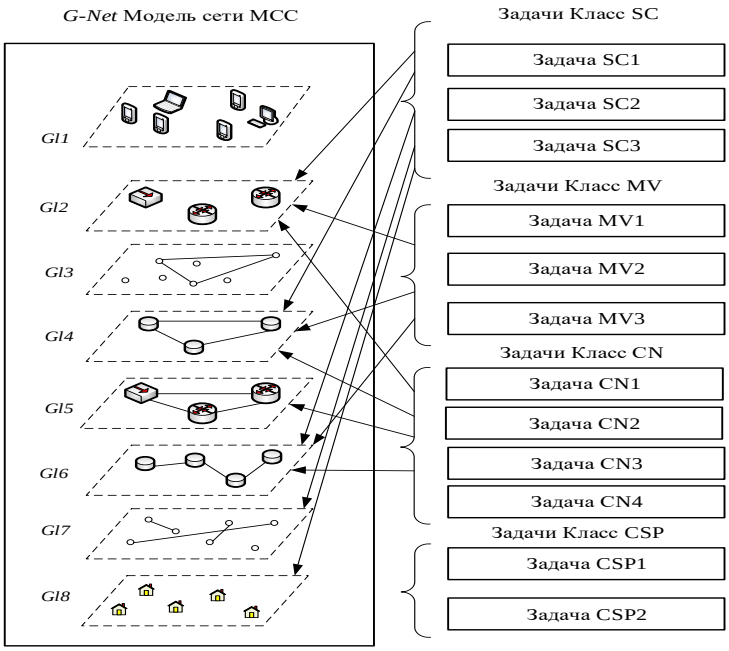


Рисунок 4 - Соответствие уровней модели $G - Net$ классам решаемых задач

Класс MV, задачи поиска медианных вершин в графах и гиперсетях.

С помощью задач этого класса осуществляется поиск мест расположения элементов *NE* сети МСС, других элементов в сети с использованием кабельных линий связи, а также определение границ влияния соответствующих узлов связи, как правило, осуществляются с помощью алгоритмов поиска медианных вершин, определение центра тяжести графа.

Классической является задача MV1 – поиск медианы во взвешенном графе, решается на уровнях G_{L2}, G_{L4}, G_{L6} модели $G - Net$. Подобная постановка задачи возможна для любых взвешенных точек, расположенных на поверхности.

Задача MV3, поиск b – медианы графа является классической и решается с помощью различных алгоритмов на уровнях G_{L2}, G_{L4}, G_{L6} модели $G - Net$. В данной работе приведены приближённые алгоритмы, основанный на “разумном” переборе исходных данных.

Семейство перечисленных задач класса MV решает важную проблему, связанную с поиском мест расположения элементов NE и границ влияния (тяготения) на проектируемой сети МСС.

Класс CN, задачи поиска связующих сетей.

Для организации каналов связи между узлами уровня G_{l2} модели $G - Net$ возникают задачи поиска структур с заданными способами организации связей (систем связи), связывающих эти узлы, имеющие минимально возможный вес, либо другие заданные характеристики с ограничениями.

Целесообразно, применять следующие задачи:

CN1 – задача поиска наименьшего циклического маршрута, проходящего через заданное множество вершин гиперсети, на уровне G_{l2}.

CN2 - задача поиска минимального дерева связывающее заданное подмножество вершин (дерево Штейнера) в гиперсети на уровнях G_{L2}, G_{L4} модели $G - Net$.

Для повышения устойчивости сегментов сети МСС может решаться задача,

CN3 – поиск части графа (уровни G_{l2}, G_{l5}, G_{l6}) модели $G - Net$ с заданной связностью содержащей выделенные вершины.

Четвёртая задача CN4 – поиск покрывающей сети является обобщением предыдущих задач в том смысле, что вес медианных вершин x_i^m увеличивается на величину $\varphi(N_i)$, где N_i - суммарный вес вершин входящих в зону действия вершин x_i^m. Так же, учитывается "вес" части графа, связывающего все медианные вершины.

Класс CSP. Задачи поиска покрывающего множества вершин или рёбер.

Задачи этого класса как правило используются при решении задач построения беспроводных сетей связи, а также при синтезе сегментов первичной (транспортной) части сети МСС.

CSP1 – Задача наименьшего рёберного покрытия во взвешенном гиперграфе.

Эта задача возникает в связи с оценкой построения устойчивой беспроводной сети и размещения базовых станций в этом сегменте сети МСС.

CSP2 – Задача поиска максимально независимого множества рёбер в гиперграфе. К этой задаче сводятся задачи размещения элементов NE в МСС на уровнях G_{L4}, G_{L6}.

Далее предлагается математическая модель топоосновы для пространственного размещения элементов сети МСС, уровень G_{L8} , модели $G - Net$.

Дано:

1. Рельеф местности представлен в виде клеточной структуры с шагом клетки l метров и минимальным перепадом высот h – метров (определяется проектировщиком).

2. Карта препятствий (градостроительные факторы, рельеф местности), клеточная модель, отображающая участки, на которых невозможно размещение коммутационных узлов сети МСС, а также прокладка линейных сооружений.

3. Карта существующих линейных сооружений, узлов сети МСС (в случае модернизации сети МСС) для поправок весовых характеристик рёбер гиперсети ситуационных трасс.

Сопоставим каждой клетке карты рельефа вершину графа $TO = (X, V)$ топоосновы. Каждой ветви сопоставим вес равный:

1 случай - вершины соседних клеток $(x1, x2)$ на одном уровне $\rho\,(x1, x2) = l$;

2 случай - вершины соседних клеток $(x2, x3)$ на разных уровнях $\rho\,(x2, x3) = \sqrt{l^2 + h^2}$;

3 случай - вершины соседних клеток $(x2, x6)$ на разных уровнях (диагональ с двумя ступенями) $\rho\,(x2, x6) = \sqrt{2l^2 + 4h^2}$;

4 случай - вершины соседних клеток $(x3, x5)$ на одном уровне (диагональ) $\rho\,(x3, x5) = l\sqrt{2}$

5 случай - вершины соседних клеток $(x1, x5)$ на разном уровне (диагональ с одной ступенью) $\rho\,(x1, x5) = \sqrt{2l^2 + h^2}$ на рисунке 5 представлена графовая структура топоосновы, уровень G_{L8}, модели $G - Net$.

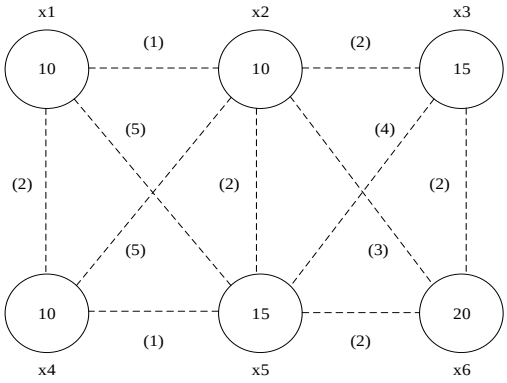


Рисунок 5 - Графовая модель топоосновы уровня G_{L8}, модели $G - Net$

В четвёртой главе рассматриваются вопросы, связанные с повышением структурной надёжности, живучести сетей МСС, рассмотрены задачи эффективного резервирования сетей МСС. Поставлена и решена задача создания системы оповещения короткими сообщениями в условиях ГО и ЧСС с использованием подхода и реализации межсетевых узлов.

Для таких публичных сетей связи как ТФОП, сеть Интернет и сети мобильной связи, целесообразно использовать унифицированную систему передачи тревожных сообщений, которая

могла бы функционировать на различных абонентских терминалах пользователей, таких как обычный городской телефон, сотовый телефон, переносной или стационарный компьютер, подключённый к сети Интернет.

В случае, если чрезвычайная ситуация (ЧС) несёт угрозу жизни людей, её спасение становится наиболее приоритетной задачей. При решении этой задачи наиболее актуальным является своевременное информирование всех заинтересованных лиц, которое производится с использованием всех доступных видов связи. Чрезвычайные ситуации можно условно разделить на прогнозируемые и возникающие вне прогноза, природные и техногенные. В любом случае, ЧС требуют скоординированной и оперативной работы на всех уровнях единой государственной системы ликвидации и предупреждения ЧС России. Среди задач этой системы можно выделить следующие, основные – оповещение ответственных должностных лиц в оперативных единых дежурно - диспетчерских службах (ЕДДС) МЧС РФ, управлениях, ведомствах, департаментах, службах, а также населения, которое находится в районе ЧС.

СПИСОК ЛИТЕРАТУРЫ

1. ITU-T X.805: Security architecture for systems providing end-to-end communications, 2003. URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=7024
2. ITU-T Y.2701: Security requirements for NGN release 1, 2007. URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=8899
3. ITU-T Y.2704: Security mechanisms and procedures for NGN, 2010. URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=10237
4. ITU-T Y.2760: Mobility security framework in NGN, 2011. URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11094
5. ITU-T Y.2770: Requirements for deep packet inspection in next generation networks, 2012. URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11566
6. *Орлов С. А.,* Программная инженерия//Изд. - во. Питер, 2018. с. 640 ил.
7. *Попков Г. В*., Перспективное проектирование сети абонентского доступа с использованием восьмиуровневой модели//журнал. “Программные продукты и системы”, no 2 (114), 2016. с. 139 – 145.
8. *Бирюков А. А.,* Информационная безопасность: защита и нападение//М.: Изд. – во. ДМК, 2013. с. 472 ил.
9. *Назаров А. Н., Сычёв К. И.,* Модели и методы расчёта показателей качества функционирования узлового оборудования и структурно – сетевых параметров сетей связи следующего поколения//Изд. – во. “Поликом”, 2011. с. 491.
10. Попков Г. В. К вопросу оценки устойчивости функционирования элементов сети связи / Г. В. Попков // журнал Программные продукты и системы. – 2018. - №2. – с. 316 – 320.
11. Попков Г. В. К вопросу проектирования мультисервисных сетей связи, устойчивых к разрушающим деструктивным воздействиям / Г. В. Попков // журнал Телекоммуникации. - 2020. - №1. - с. 35 – 40.
12. Попков Г. В. К вопросу формирования частных моделей угроз для мультисервисных сетей связи / Г. В. Попков // журнал Телекоммуникации. - 2021. - №10.

Путято М.М.
Кубанский государственный технологический университет, доцент,
putyato.m@gmail.com

РАЗРАБОТКА ТЕОРЕТИЧЕСКИХ И МЕТОДОЛОГИЧЕСКИХ ОСНОВ ПОСТРОЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ РАСПРЕДЕЛЕННЫХ СИСТЕМ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ

Аннотация: В рамках научного проекта проведены исследования моделей интеллектуальных распределенных систем управления кибербезопасностью на основе детерминированно-стохастических моделей и обеспечения процесса непрерывной идентификации; методов построения и реализации комплекса моделей для формирования объектов и процессов функционирования распределенной системы управления кибербезопасностью; математического и алгоритмического обеспечения процессов функционирования распределенной системы управления кибербезопасностью; методик построения интеллектуальной распределенной системы управления кибербезопасностью на основе детерминированно-стохастических моделей и обеспечения процесса непрерывной идентификации; программных комплексов реализации интеллектуальной распределенной системы управления кибербезопасностью на основе детерминированно-стохастических моделей и обеспечения процесса непрерывной идентификации.

Ключевые слова: киберугрозы, распределённые системы, адаптивные системы, DDOS-атака, аутентификация, информационная безопасность, искусственный интеллект, нейронные сети, цифровое информационное пространство.

Процесс цифровизации предполагает, что к данным может обращаться любой процесс или система. Поэтому подтверждение и поддержка легитимности доступа и защиты современной архитектуры информационной безопасности (ИБ), с классическим подходом к реализации системы защиты, становятся все более затруднительными.

На первое место выходят угрозы ИБ, структура, форма и методы реализации которых сосредоточены в той части информационного пространства (ИПр), где данные передаются, обрабатываются и хранятся в цифровом виде. Появление новейших информационных технологий и систем, развитие и расширение функций социальных сетей, внедрение в социальные сети различных сервисов и их алгоритмизация формируют не просто отдельную систему внутри ИПр, а отдельную область – киберпространство (КПр). Так как КПр — это частный случай ИПр, то все характеристики последнего применимы и к КПр. Однако ввиду долгосрочного развития КПр, как неконтролируемой самостоятельно развивающейся среды, применить характеристики киберпространства к ИПр нельзя. Аналогично информационному пространству, для информации в КПр существуют угрозы ИБ, которые могут нарушать доступность, целостность и конфиденциальность данных. Такие угрозы в терминологии, соответствующей рассматриваемой теме, называются киберугрозами. Согласно экспертным оценкам доля киберугроз в общей массе угроз информационной безопасности будет неуклонно расти. Особую опасность представляет дериметризация и размытие границ объектов защиты, которые являются основой использования классических моделей информационной безопасности. В связи с этим традиционные подходы к построению систем информационной безопасности теряют свою эффективность. Данные обстоятельства требуют постановки новых целей и задач, а также выработки новых решений и способов противодействия постоянно эволюционирующим киберугрозам. Необходимо четко представлять структуру и взаимосвязи компонентов киберпространства, что позволит обеспечить выработку подходов к достижению необходимого уровня кибербезопасности каждого из элементов иерархической системы кибернетического пространства и интегральной оценки кибербезопасности в целом [29].

Адаптивная комплексная система обеспечения безопасности, как общая платформа обеспечит своевременный мониторинг, контекст и возможности управления в различных ситуациях.

Проблемное поле, в которое входят вопросы обеспечения кибербезопасности, формирования защищенного киберпространства, а также различного класса системы детектирования, упреждения, предотвращения, пресечения и противодействия кибератакам и анализа новых киберугроз формируется в течение последних лет. Такие ведущие отечественные и зарубежные ученые как Котенко И. В., Чечулин А. А., Петренко С. А., Белов Е. Б., Калинин М. О., Бородакий Ю. В., Ревенков П. В., Бердюгин А. А., Зегжда Д. П., Лаврова Д. С., Лахно В. А., Лаута О. С., Промыслов В. Г., Дойникова Е. В., Васильев В. И., Соколов С. С., Зегжда П. Д., Максимов Р. В., Макаревич О. Б.,

Назаренко М. А., Воропай Н. И., JulianJang-Jaccard, DanCraigen, PeterWarrenSinger, FedericoCalzolari, AthanasiosVasilakos, Yuguang "Michael" Fang, AngelosD. Keromytis, MerrillWarkentin, WillySusilo, MuhammadKhurramKhan, JosepDomingo-Ferrer, DavidDeRoure, DimitrisA. Gritzalis, AliGhorbani затрагивают основные фундаментальные вопросы, которые подтверждают свою актуальность каждый день.

Доля киберугроз в общей массе угроз информационной безопасности неуклонно растет. Особую опасность представляет депериметризация и размытие границ объектов защиты, которые являются основой использования классических моделей информационной безопасности. В связи с этим традиционные подходы к построению систем информационной безопасности теряют свою эффективность. Данные обстоятельства требуют постановки новых целей и задач, а также выработки новых решений и способов противодействия постоянно эволюционирующим угрозам информационной безопасности и интегральной оценки кибербезопасности в целом.

Сегодня в России в наибольшей степени атакам подвержены различные структуры и объекты: операторы связи, финансовые организации, ритейл-сети, промышленный сектор, социально-значимые объекты. При этом малый и средний бизнес по мере его цифровизации привлекает все больше внимания киберпреступников. Это объясняется тем, что конкуренция в нем достаточно высока, а возможности киберзащиты и оценки рисков зачастую ограничены. Усугубляет проблему массовый переход, в связи с пандемией, на удаленную работу, из-за чего периметр сети компаний по сути распространился на дома сотрудников и их личные устройства. Хотя этот шаг в целом соответствует духу прогресса, из-за стихийного характера он умножил слабые места в цифровой обороне предприятий.

Первостепенная задача определяется требованиями времени и предполагает решение фундаментальной проблемы организации многоуровнеого киберпространства региона для максимально эффективного управления вопросами кибербезопасности на основе интеллектуальной адаптивной интегрированной платформы с применением вероятностных методов машинного обучения. В свою очередь необходимо решение ряда задач в различных предметных областях:

А) В области кибербезопасности:

- Исследование теоретических подходов к формированию методологии кибербезопасности, позволяющих формализовать требования конфиденциальности, целостности и доступности, создания архитектуры агентно-ориентированного моделирования киберфизических систем, методики оценки эффективности защиты информационно-телекоммуникационной сети в условиях таргетированных кибернетических атак,современных средств и методов мониторинга и управления инцидентами комплексной безопасности систем различного класса, средств управленияинформационными потоками и разграничения доступа к ним и средства создания доверенной среды,методик визуализации метрик кибербезопасности, синтеза архитектуры кибербезопасности для систем управления.

- Разработка новых методов детектирования и анализа перспективных кибернетических угроз в системах различного класса, в том числе в динамических сетях передачи данных (VANET, FANET, MARINET, MANET, WSN) и в киберфизических системах.

- Исследование методов и методик выявления и противодействия кибератакам в автоматизированных системах, в том числе динамическихинфраструктур сложных систем;

- Формирование аналитического и математического моделирования для прогнозирования векторов кибератак, моделирования сетевой и цифровой инфраструктуры региона для решения задачи противодействия кибератакам;

Б) В области функционирования сложных многоуровневых систем:

- Исследование методов организации и функционирования сложных иерархических систем.

- Разработка теоретических положений по организации и функционированию иерархических систем управления социальными и технологическими объектамирегиона в киберпространстве.

- Разработка методик и технологий, позволяющих извлекать знания и определять закономерности функционирования в рамках цифровой инфраструктуры региона и методы обеспечения его безопасности.

- Создание методик, позволяющих проектировать и моделировать многоуровневые мультиагентные системы управления на основе интеллектуальных методов с учетом критериев безопасности.

- Разработка методов и алгоритмов функционирования распределенной многоуровневой адаптивной системы для обеспечения управления организацией в условиях изменяющегося киберпространства и увеличения количества киберпреступлений и кибертерроризма.

В) В области искусственного интеллекта:

- Проведение аналитического исследования методов, алгоритмов и теорий управления многоагентных систем и систем управления кибербезопасностью на основе методов искусственного интеллекта.

- разработка новых интеллектуальных подходов к управлению системами кибербезопасности на основе технологии искусственных нейронных сетей и глубоко машинного обучения;

- формирование математического и алгоритмического аппарата теории организации интеллектуальных адаптивных систем, функционирующих в растущем киберпространстве;

- реализация интеллектуальных агентов в рамках единой интегрированной платформы управления кибербезопасностью цифровой инфраструктурой региона;

- оценка достижимости поставленных целей и сравнение результатов исследований с мировыми аналогами в области искусственного интеллекта.

Разработка новых методов детектирования и анализа перспективных кибернетических угроз в системах различного класса [1,2,3,4,5,6,7], в том числе в динамических сетях передачи данных (VANET, FANET, MARINET, MANET, WSN) [8] и в киберфизических системах [17] и исследование методов и методик выявления и противодействия кибератакам в автоматизированных системах, в том числе динамических инфраструктур сложных систем [10,11,12,13,14,19, 26]. Формирование аналитического и математического моделирования для прогнозирования векторов кибератак [22,23], моделирования сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам [24] и исследование теоретических подходов к формированию методологии кибербезопасности [5,9,10,11,12,13,14,15,16], в том числе функционально-семантических моделей кибербезопасности, позволяющих формализовать требования конфиденциальности, целостности и доступности [15], создания архитектуры агентно-ориентированного моделирования киберфизических систем [9,12,14,16,20,21,25,27,28], методики оценки эффективности защиты информационно-телекоммуникационной сети в условиях таргетированных кибернетических атак [23], современных средств и методов мониторинга и управления инцидентами комплексной безопасности систем различного класса [20], средств управления информационными потоками и разграничения доступа к ним и средства создания доверенной среды [5], методик визуализации метрик кибербезопасности [18], синтеза архитектуры кибербезопасности для систем управления [31].

Для получения существенных перспективных результатов в указанных выше направлениях необходимо используя методы ансамблевоемого, дискретно-событийного, агентного моделирования построить многоуровневые модели киберпространства; с использованием факторного, кластерного, корреляционного анализа провести работы по анализу и совершенствованию методов и средств построения интеллектуальных адаптивных систем управления кибербезопасностью; разработать методики построения интеллектуальных адаптивных систем управления кибербезопасностью на основе детерминированно-стохастических моделей и обеспечить процесс непрерывной идентификации с использованием методов вероятностного программирования, пространственно-векторных моделей, теоретико-графовых моделей защищенности; сформировать математическое и алгоритмическое обеспечение с использованием методов математической статистики, методов вероятностного программирования и корреляционного анализа, а также использовании пространственно-векторных моделей.

Формирование нового подхода к процессу противодействия киберугрозам продиктовано не только повышением функциональности современных технологий, но и требованиями к созданию адаптивных интегрированных решений, масштабируемых в рамках архитектуры для защиты от различного типа угроз.

Создание и разработка фундаментальных и прикладных положений по созданию, функционированию и организации адаптивных интеллектуальных многоагентных систем управления безопасностью киберпространства на основе вероятностных методов машинного обучения для формирования основы построения методологии создания и построения интеллектуальных адаптивных многоагентных систем управления кибербезопасностью.

В ходе реализации гранта реализовано несколько последовательных этапов для достижения поставленных целей и задач:

1. Проведение аналитического исследования методов, алгоритмов и теорий управления в области кибербезопасности, теории иерархических систем и искусственного интеллекта. Разработка теоретических положений по организации функционирования систем управления кибербезопасностью. Идентификация и систематизация задач кибербезопасности с определением их характеристик и показателей. Выделение главных концепций, отражающихмнеобходимые знания в

исследуемых предметных областях. Участие коллектива исследователей в проведении процесса аналитического исследования и первичного поиска материалов.

2. Разработка методик, позволяющих выявить и сформулировать понятия, определить функционирование цифровой инфраструктуры региона в киберпространстве. Определить формальные средства представления знаний о киберугрозах, выбор типа системы иерархического типа и методов реализации искусственного интеллекта.

3. Разработка методов и алгоритмов функционирования адаптивной интеллектуальной системы управления кибербезопасностью цифровой инфраструктуры региона. Разработка структуры знаний о киберугрозах с возможностью включения процессов моделирования, прогнозирования и принятия решений.

4. Программная и аппаратная реализация прототипа инетгрированного адаптивного интеллектуального мультиагентногокомплекса на основе разработанных теоретических положений. Задействование в реализации работ Центра коллективного пользования «Исследовательский центр компьютерных технологий, систем управления и комплексной безопасности» ФГБОУ ВО «Кубанский государственный технологический университет». Оформление лицензионных прав на программный комплекс. П

5. Тестирование системы путем решения конкретных проверочных задач. Разработка положений и рекомендаций о реализации и применении разработанной интеллектуальной системы управления кибербезопасностью для социальных, общественных и государственных структур. Подготовка отчета о проделанной работе и достижения целей и задач проекта.

Проблемное поле, в которое входят вопросы обеспечения кибербезопасности, формирования защищенного киберпространства, а также различного класса системы детектирования, упреждения, предотвращения, пресечения и противодействия кибератакам и анализа новых киберугроз формируется в течение последних лет. Такие ведущие отечественные и зарубежные ученые как Котенко И. В., Чечулин А. А., Петренко С. А., Белов Е. Б., Калинин М. О., Бородакий Ю. В., Ревенков П. В., Бердюгин А. А., Зегжда Д. П., Лаврова Д. С., Лахно В. А., Лаута О. С., Промыслов В. Г., Дойникова Е. В., Васильев В. И., Соколов С. С., Зегжда П. Д., Максимов Р. В., Макаревич О. Б., Назаренко М. А., Воропай Н. И.,JulianJang-Jaccard, DanCraigen, PeterWarrenSinger, FedericoCalzolari, AthanasiosVasilakos, Yuguang "Michael" Fang, AngelosD. Keromytis, MerrillWarkentin, WillySusilo, MuhammadKhurramKhan, JosepDomingo-Ferrer, DavidDeRoure, DimitrisA. Gritzalis, AliGhorbani затрагивают основные фундаментальные вопросы, которые подтверждают свою актуальность каждый день.

Логическим продолжением пройденных этапов и полученных данных будут мероприятия по тестированию и апробации методического, математического и алгоритмического в рамках методологии построения многоагентного комплекса противодействия киберугрозам, а также разработка и тестирование программного продукта.

Ввиду этого предложим модифицированную структуру кибернетического пространства и структурную модель, построенную в нотации BPMN 2.0. Исходя из сформулированного определения, киберпространство охватывает три области: физическое, информационное и социальное пространства (рис. 1,2).

Физическое пространство возможно определить через программно-аппаратную инфраструктуру взаимосвязи открытых систем (ВОС) регламентированную ГОСТ Р ИСО/МЭК 7498-1-99. Подобный подход с использованием модели ISO/OSI схожей по составу с ВОС был представлен одним из исследователей. Но для описания роли физического пространства как канала доступа к киберпространству, определим дополнительный уровень программного обеспечения, который формирует возможности взаимодействия с другими элементами.

Технический уровень позволяет определить субъект физического пространства как устройство, а объект как пакет данных.

Сервисный уровень позволяет определить субъект физического пространства как интерфейс, а объект как протокол.

Уровень программного обеспечения позволяет определить субъект физического пространства как приложение, а объект как цифровые данные.

Информационное пространство включает обобщенный информационный уровень, представленный в структуре социокиберфизической системы и в структуре киберпространства и семантический уровень.

Информационный уровень позволяет определить субъект информационного пространства как база данных, а объект как блок данных.

Семантический уровень позволяет определить субъект информационного пространства как база знаний, а объект как семантический блок.

Социальное пространство включает персональный уровень и социальный уровень.

Индивидуальный уровень позволяет определить субъект социального пространства как человек, а объект как сообщение.

Социальный уровень позволяет определить субъект социального пространства как социальная группа, а объект как сообщение.

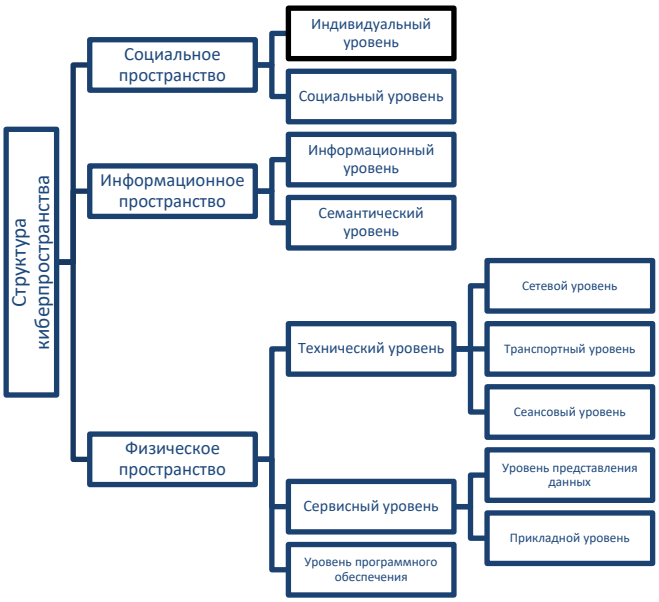


Рис. 1. Модифицированная иерархическая структура киберпространства

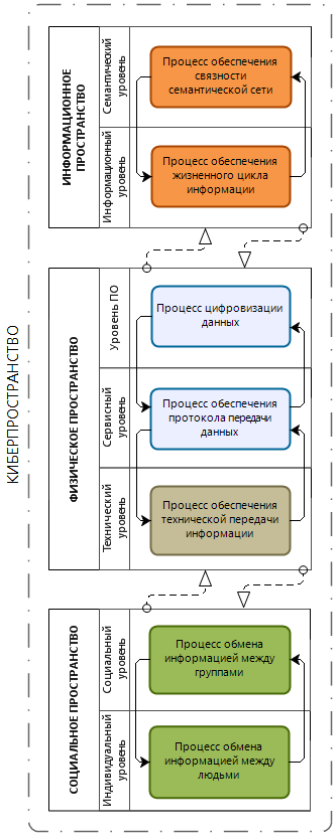


Рис. 2. Структурная модель киберпространства в нотации BPMN 2.0

Представленная структурная модель позволяет перейти к определению контроля целостности, конфиденциальности и доступности информации для каждого уровня, процесс обеспечения безопасности которых формирует понятие защищенного киберпространства. Опираясь на предложенную структурную модель добавим уровень кибербезопасности, в котором организован непрерывный процесс обеспечения состояния защищенности информации в киберпространстве (рис. 3).

В рамках непрерывного процесса обеспечения кибербезопасности опишем процессы для каждого из структурных элементов.

Социальное пространство реализует информационный обмен на индивидуальном и социальном уровнях, а также между ними, формируя *процесс обмена информацией*. При этом на *индивидуальном уровне* происходит общение между людьми, а на *социальном уровне* между *социальными группами*.

Физическое пространство объединяет три уровня: на *техническом уровне* реализуется *процесс технической передачи информации*, на *сервисном уровне – процесс обеспечения протокола передачи данных*, а на *уровне программного обеспечения – процесс цифровизации данных*. При этом обмен данными происходит при участии всех указанных уровней.

Рис. 3. Структурная модель защищенного киберпространства
в нотации BPMN 2.0

Информационное пространство реализует этапы обработки информации на информационном и семантическом уровнях, формируя при этом *процесс обеспечения жизненного цикла информации* на *информационном уровне* и *процесс обеспечения связности семантической сети* на *семантическом уровне*.

Для каждого из пространств определен уровень кибербезопасности. Составляющие процесса обеспечения кибербезопасности интегрируются в существующие процессы на этом уровне, поддерживая на необходимом уровне конфиденциальность, целостность и доступность информации.

Характеристиками киберпространства являются безопасность, доступность, непрерывность, масштабируемость, мобильность и разнородность.

Границы киберпространства вариативны и охватывают каждого отдельного человека как источника, так и получателя информации в цифровом виде в течение времени взаимодействия с устройствами.

Обеспечение необходимого уровня кибербезопасности и формирование защищенного многоуровневого киберпространства становится возможным на основании сформированной структурной многоуровневой модели в нотации BPMN 2.0.

Структурная модель защищенного киберпространства включает социальное, физическое и информационное пространства для которых неотъемлемым атрибутом является кибербезопасность.[29]

На рисунке 4 приведена схема включения адаптивной системы комплексной безопасности в структуру интеллектуального ситуационного центра обеспечения кибербезопасности[30].

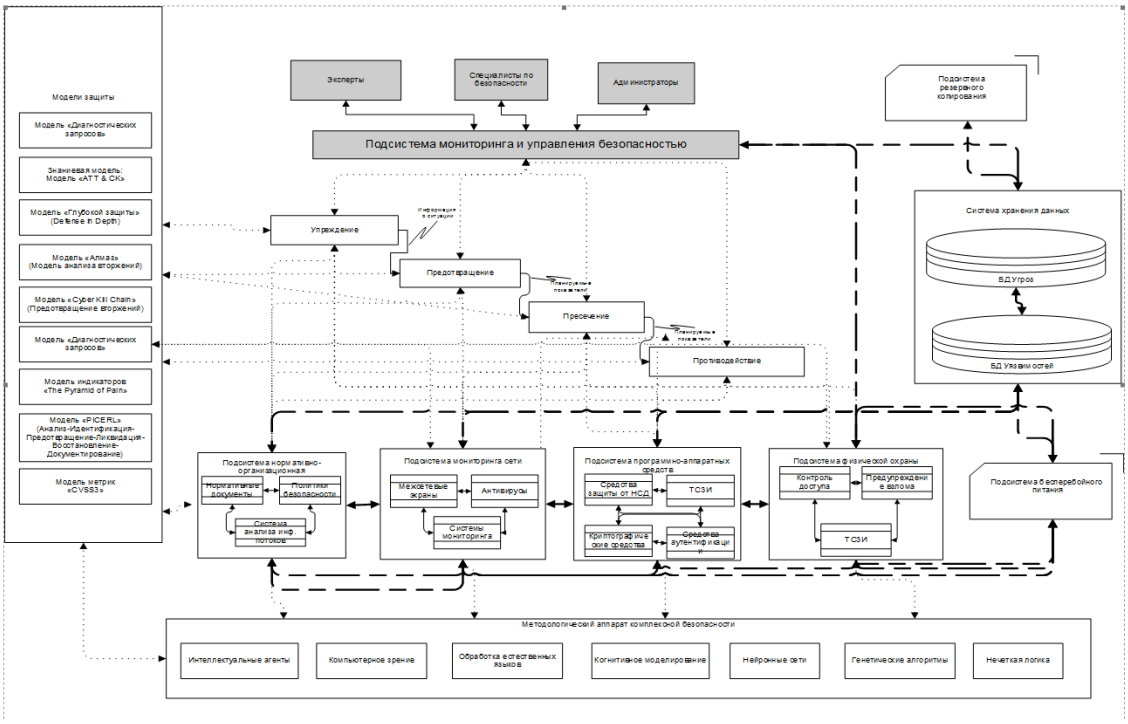


Рис. 4. Структурная схема интеллектуальной распределенной системы управления кибербезопасностью

Модель адаптивного управления безопасностью предлагается описывать формулой Безопасность = Мониторинг + Аудит + Анализ риска + Политика безопасности + Средства защиты + Реализация контрмер + Реагирование (рисунок 5).

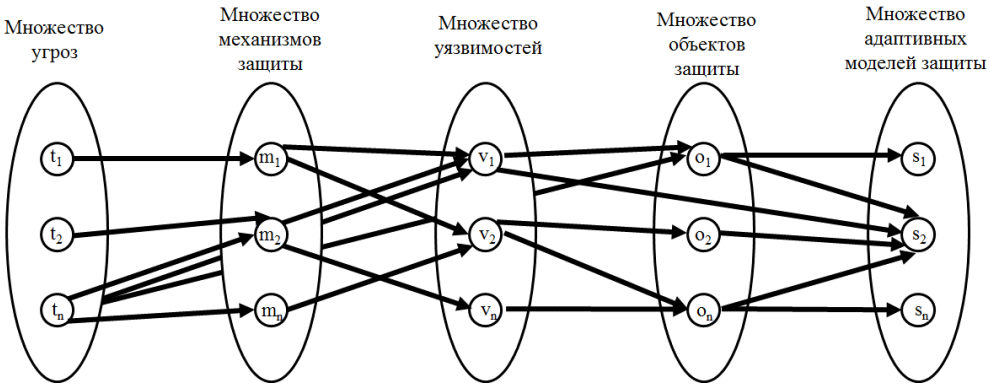


Рис. 5. Модель интеллектуальной распределенной системы управления кибербезопасностью с полным перекрытием

При этом использование моделей информационной безопасности будет определно исходя из онтологической структуры моделей и методов (рисунок 6).

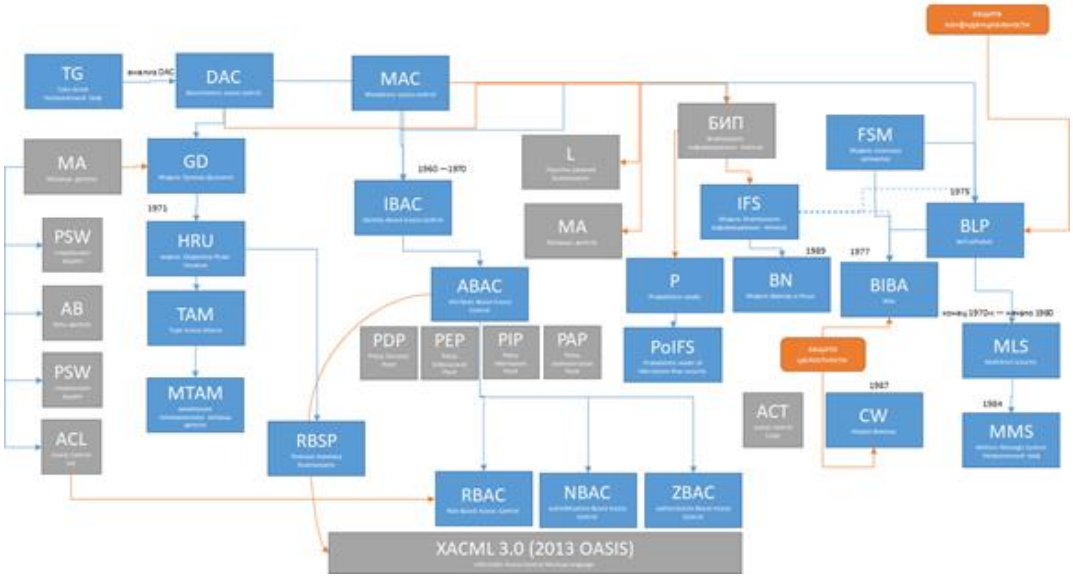


Рис. 6. Онтологическая структура математических моделей обеспечения информационной безопасности

Проанализировав основные функции и характеристики адаптивной комплексной системы обеспечения безопасности определим, что предложенный подход продиктован не только повышением функциональности современных технологий, но и требованиями к созданию адаптивных интегрированных решений, масштабируемых в рамках архитектуры для защиты от различного типа угроз; использование КССОБ в рамках предложенного подхода позволит оперативно реагировать на инциденты как внешнего, так и внутреннего характера, что позволит своевременно нейтрализовать последствия их влияния; адаптивная комплексная система обеспечения безопасности, как общая платформа обеспечит своевременный мониторинг, контекст и возможности управления в различных ситуациях.

Разработка такой платформы интеграции позволит усовершенствовать процесс автоматизации и значительно улучшить качество информации, предоставляемой продуктами для обеспечения ИБ.

В рамках научно-исследовательского проекта предложена разработка теоретических положений, методологии, алгоритмов функционирования и практическая реализация адаптивной интеллектуальной многоагентной системы управления киберугрозами в рамках цифровой инфраструктуры региона на основе методов машинного обучения.

Разработка интеллектуальной системы будет обеспечиваться на основе ряда теоретических предпосылок, методик, методов и алгоритмов и предусматривает последовательность ряда задач для достижения ожидаемых результатов.

В рамках исследования проведен перечень аналитических мероприятий с целью выявления слабых сторон цифровой региональной инфраструктуры киберпространства и обобщения полученных результатов для разработки необходимых методик.

А) в области кибербезопасности:

- проведена идентификация и систематизация киберугроз с определением их характеристик и показателей будет проведена на основе методик лингвосемантического, морфологического и эвристического анализа;

- разработана методика определения типа атак и способов их обнаружения с применением экспертных методов, вероятностных методов машинного обучения и методов искусственного интеллекта;

- создана методика оценки инцидентов и полного спектра уязвимостей на основе статистических характеристик корреляционного анализа;

- определены методы разработки системы управления кибербезопасностью на основе теории сложных систем и ситуационного управления.

Б) в области распределенных иерархических систем:

- аналитический отчет о возможности функционирования многоагентных иерархических систем в современном киберпространстве: подходы, методы и алгоритмы функционирования. Для полноценного исследования будут привлечены теория системного анализа, теория сложных иерархических систем, методы аналитического моделирования;

- разработка методик, позволяющих выявить и сформулировать понятия, определить критерии эффективности функционирования интеллектуальных иерархических систем в рамкахкиберпространства с учетом влияния киберугроз применительно к цифровой инфраструктуре регионабудет проведена на основе методов моделирования, экспертной оценки и теории принятия решений.

-определить формальные средства представления информации в едином цифровом пространстве для адаптивной иерархической интеллектуальной системы управления кибербезопасностьюна основе методов искусственного интеллекта (нейронные сети, генетические алгоритмы и т.д.).

В) в области искусственного интеллекта:

- провести поиск оптимальных методов искусственного интеллекта для реализации отдельных агентов реализуемой системы: типов нейронных сетей и методов глубокого машинного обучения на основе методов системного анализа, экспертных методов, статистического и аналитического анализа;

- разработка структуры для представления знаний о киберугрозах и о цифровой инфраструктуре региона для реализации непосредственного построения базы знаний системы будет проведена путем структурно-функционального и логического моделирования с последующей отработкой на имитационной модели.

В рамках этапа работ предусматривается выполнение следующих видов задач.

А) в области кибербезопасности:

- разработка методологии построения адаптивной интеллектуальной системы управления кибербезопасностью на основе детерминированно-стохастических моделей и обеспечения процесса непрерывной идентификации;

- создание модели интеллектуальной распределенной системы управления кибербезопасностью на основе ряда методологий структурно-функционального, имитационного и когнитивного моделирования;

- разработка математического и алгоритмического обеспечения процессов функционирования интеллектуальной системы управления кибербезопасностью на основе теории иерархических систем, систем информационной безопасности путем аналитического, математического и логического моделирования с последующей отработкой на имитационной модели;

Б) в области распределенных иерархических систем:

- разработка теоретических положений по организации устойчивого функционирования иерархических систем в киберпространстве будет проведена с использованием положений теории систем, системного анализа и теории имитационного моделирования.

- определение принципов координации, согласования и прогнозирования уровней взаимодействия подсистем с целью определения зависимостей между уровнями декомпозиции мультиагентной системы с использованием теории сложных и иерархических систем, теории системного анализа;

- разработка архитектуры программных агентов и системы в целом с целью определения механизмов взаимодействия агентов на основе аксиоматических логических структур и алгебраической теории систем.

В) в области искусственного интеллекта:

- определение методы представления интеллектуальной системы на основе одного из типов: аксиоматического, логики предикатов и высказываний, продукционных систем;

- определеение стратегии и процедуры решения задач адаптивной интеллектуальной многоагентной системы в рамках комплексного применения эвристического поиска, поиска в глубину и ширину.

- поиск аппаратного обеспечения для реализации интеллектуальных агентов для дальнейшей интеграции в единую платформу.

Следующий этап предусматривает выполнение следующих видов работ.

А) в области кибербезопасности:

- программная и аппаратная реализация прототипа универсальной интеллектуальной многоагентной системы управления кибербезопасностьюс учетом разработанных теоретических положенийпредполагаетсяпровести с использованием языков PHP,Python, технологий облачных вычисленийс последующей апробацией для социальных и экономических процессов субъектов РФ.

- оценка достижения поставленных целей по реализации системы определяется на основе экспертных методов, методов вероятностного и статистического анализа по пресечению, упреждению, противодействию и предотвращению киберугроз.

- подготовка необходимой технической и отчетной документации по проекту с использованием нормативной литературы и экспертных мнений.

Б) в области распределенных иерархических систем:

-тестирование многоагентной иерархической структуры системы в современном киберпространстве путем решения конкретных проверочных задач на основе имитационного и ситуационного моделирования, что позволит оценить достижение целей и задач проекта;

- определение процессов устойчивости, вычислимости, непротиворечивости и полноты реализации функций мультиагентной системы управления кибербезопасностью в рамках цифровой инфраструктуры региона.

В) в области искусственного интеллекта:

- для реализации интеллектуальных методов для разрабатываемой системы предполагается провести с использование языка Python, для математических расчетов модули NumPy, SciPy, Sklearn, среды моделирования имитационного AnyLogic, среды математического моделирования Matlab с модулем Simulinkили аналогов российского производства.

- подготовка данных для тестирования интеллектуальной адаптивной многоагентной системы на основе нейронных сетей и с использование леса решений, модифицированного метода деревьев решений.

Этап реализации проекта предусматривает проведение всестороннего исследования различных аспектов научно-исследовательского проекта по следующим направлениям:

А) в области кибербезопасности:

- аналитическое исследование подходов к обнаружению атак и киберугроз различного формата, с целью их идентификации и систематизации для определения необходимых характеристик и показателей;

- определение критичных данных цифровой инфраструктуры региона с целью разработки с целью оценки защищенности информации;

- определение перечня динамических методов поиска киберугроз;

- созданиеметодики проактивной защиты объекта и процессов управления инцидентами;

- разработка модели обнаружения киберугроз с целью автоматизации процессов управления инцидентов для адаптивной интеллектуальной многоагентной системы управления кибербезопасностью;

- разработка фундаментальных положений о построении и функционировании многоуровневой защиты киберпространства;

- создание организационной структуры интеллектуальной многоагентной системы управления кибербезопасностью;

Б) в области распределенных иерархических систем:

- проведение анализа методов, процедур и алгоритмов функционирования и применения многоуровневой мультиагентной систем в современном киберпространстве;
- определение общих контуров системы конечных целей и ограничений на условия функционирования системы;
- разработка методик, позволяющих определить особенности архитектур мультагентной системы и онтологий иерархической распределенной системы;
- формирование общей организационной структуры иерархической системы: количество уровней иерархии для каждого из иерархических направлений, общее число подсистем на каждом уровне иерархии и во всей системе, сложность подчинения отдельных подсистем;
- определение архитектур программно-информационных агентов, типологий агентов, системы их взаимодействия, множества факторов, ресурсов и действия агентов;
- разработка методики синтеза индивидуальных свойств агентов и общей структуры мультиагентной системы, с определением принципов координации, согласованности и планирования иерархии;
-определение формальные средства представления информации в киберпространстве для многоуровневой иерархической системы.

В) в области искусственного интеллекта:

- поиск оптимальных методов искусственного интеллекта для реализации отдельных агентов реализуемой системы;
- определить способы формализации интеллектуальной системы на основе одного из подходов: пространства состояний, решение системы подзадач, графическое представление примитивных задач;
- разработка структуры представления знаний о киберугрозахи типах данных, используемой в цифровой инфраструктуре региона;
- разработка ряда методик, позволяющих определить интеллектуальные процедуры решения задач на основе алгоритмов пространства состояний или пространства задач.

Результатами выполнения проекта являются:

- модель интеллектуальной распределенной системы управления кибербезопасностью на основе детерминированно-стохастических моделей и обеспечения процесса непрерывной идентификации;
- методика построения интеллектуальной распределенной системы управления кибербезопасностью на основе детерминированно-стохастических моделей и обеспечения процесса непрерывной идентификации;
- математическое и алгоритмическое обеспечение процессов функционирования интеллектуальной распределенной системы управления кибербезопасностью на основе детерминированно-стохастических моделей и обеспечения процесса непрерывной идентификации;
- универсальная интеллектуальная распределенная система управления кибербезопасностью на основе детерминированно-стохастических моделей и обеспечения процесса непрерывной идентификации (программный продукт), которая может быть внедрена в социальные и экономические процессы субъектов РФ, а также в учебный процесс при подготовке специалистов УГСН 10.00.00 «Информационная безопасность».
-

СПИСОК ЛИТЕРАТУРЫ

1. Бородакий Ю.В., Кибербезопасность как основной фактор национальной и международной безопасности XXI Века (часть 1) / Ю.В. Бородакий, А.Ю. Добродеев, И.В. Бутусов // Вопросы кибербезопасности – 2013 - № 1 (1) - С. 2-9
2. Бородакий Ю.В., Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 2) / Ю.В. Бородакий, А.Ю. Добродеев, И.В. Бутусов // Вопросы кибербезопасности – 2014 - № 1 (2) - С. 5-12
3. Васильев В.И., Анализ рисков кибербезопасности с помощью нечетких когнитивных карт / В.И. Васильев, А.М. Вульфин, И.Б. Герасимова, В.М. Картак // Вопросы кибербезопасности – 2020 - № 2 (36) - С. 11-21
4. Васильев В.И., Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) / В.И. Васильев, А.Д.

Кириллова, С.Н. Кухарев // Вестник УрФО. Безопасность в информационной сфере – 2018 - № 4 (30) - С. 66-74
5. Васильев Ю.С., Проблемы безопасности цифрового производства и его устойчивость к киберугрозам / Ю.С. Васильев, Д. П. Зегжда, М.А. Полтавцева // Проблемы информационной безопасности. Компьютерные системы – 2017 - № 4 - С. 47-63
6. Гайфулина Д.А., Применение методов глубокого обучения в задачах кибербезопасности. Часть 1 / Д.А. Гайфулина, И.В. Котенко // Вопросы кибербезопасности – 2020 - № 3 (37) - С. 76-86
7. Гайфулина Д.А., Применение методов глубокого обучения в задачах кибербезопасности. Часть 2 / Д.А. Гайфулина, И.В. Котенко // Вопросы кибербезопасности – 2020 - № 4 (38) - С. 11-21
8. Демидов Р.А., Анализ угроз кибербезопасности в динамических сетях передачи данных с применением гибридной нейросетевой модели / Р.А. Демидов, П.Д. Зегжда, Калинин М.О. // Проблемы информационной безопасности. Компьютерные системы. – 2018 - № 2 - С. 27-33
9. Зегжда Д.П., Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации / Д.П. Зегжда, Ю.С.Васильев, М.А.Полтавцева, И.Ф.Кефели, А.И.Боровков // Вопросы кибербезопасности – 2018 - № 2 (26) - С. 2-15
10. Зегжда Д.П., Управление динамической инфраструктурой сложных систем в условиях целенаправленных кибератак / Д.П. Зегжда, Д.С. Лаврова, Е.Ю. Павленко // Известия Российской академии наук. Теория и системы управления – 2020 - № 3 - С. 50-63
11. Зегжда Д.П., Прогнозирование кибератак на промышленные системы с использованием фильтра Калмана / Д.П. Зегжда, Д.С. Лаврова, А.В. Ярмак // Проблемы информационной безопасности. Компьютерные системы – 2019 - № 2 - С. 164-171
12. Зегжда Д.П., Гомеостатическая стратегия безопасности киберфизических систем / Д.П. Зегжда, Е.Ю.Павленко // Проблемы информационной безопасности. Компьютерные системы. – 2017 - № 3 - С. 9-22
13. Зегжда Д.П., Обеспечение киберустойчивости программно-конфигурируемых сетей на основе ситуационного управления / Д.П. Зегжда, Е.Ю. Павленко // Проблемы информационной безопасности. Компьютерные системы – 2018 - № 1 - С. 160-168
14. Зегжда Д.П., Подход к созданию критерия устойчивого функционирования киберфизических систем / Д.П. Зегжда, Е.Ю. Павленко, Д.С. Лаврова, А.А.Штыркина // Проблемы информационной безопасности. Компьютерные системы – 2019 - № 2 - С. 156-163
15. Зегжда П.Д., Подход к построению обобщенной функционально-семантической модели кибербезопасности / П.Д. Зегжда, Д.П. Зегжда, Т.В. Степанова // Проблемы информационной безопасности. Компьютерные системы – 2015 - № 3 - С. 17-25
16. Зегжда П.Д., Полтавцева М.А., Лаврова Д.С.; Систематизация киберфизическихсистеми оценка из безопасности; Проблемы информационной безопасности. Компьютерные системы; 2017; № 2; С. 127-138
17. Калинин М.О., Обнаружение угроз в киберфизических системах на основе методов глубокого обучения с использованием многомерных временных рядов / М.О. Калинин, Д.С. Лаврова, А.В. Ярмак // Проблемы информационной безопасности. Компьютерные системы – 2018 - № 2 - С. 111-117
18. Коломеец М.В., Методика визуализации метрик кибербезопасности / М.В. Коломеец, А.А.Чечулин, Е.В.Дойникова, И.В.Котенко // Известия высших учебных заведений. Приборостроение. – 2018 - Т. 61. № 10 - С. 873-880
19. Котенко И.В., Анализ процесса самоподобия сетевого трафика как подход к обнаружению кибератак на компьютерные сети / И.В.Котенко, А.М.Крибель, О.С.Лаута, И.Б.Саенко // Электросвязь – 2020 - № 12. - С. 54-59
20. Котенко И.В., Анализ задач и потенциальных направлений разработки современных методов и средств обеспечения комплексной безопасности киберфизических систем типа "умный транспорт" / И.В.Котенко, И.Б. Паращук // Научное обозрение – 2017 - № 25 - С. 26-30
21. Котенко И.В.; Команды агентов в киберпространстве: моделирование процессов защиты информации в глобальном интернете / И.В.Котенко, А.В.Уланов // Труды Института системного анализа Российской академии наук – 2006 - Т. 27. - С. 108-129

22. Коцыняк М.А., Модель воздействия таргетированной кибернетической атаки на информационно-телекоммуникационную сеть / М.А.Коцыняк, О.С.Лаута, Д.А.Иванов, О.М Лукина // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму – 2019 - № 3-4 (129-130) - С. 58-65
23. Коцыняк М.А., Методика оценки эффективности защиты информационно-телекоммуникационной сети в условиях таргетированных кибернетических атак / М.А.Коцыняк, О.С.Лаута, Д.А.Иванов, О.М.Лукина // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2018 - № 11-12 (125-126) - С. 71-79
24. Лаврова Д.С., Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам / Д.С.Лаврова, Д.П.Зегжда, Е.А. Зайцева // Вопросы кибербезопасности – 2019 - № 2 (30) - С. 13-20
25. Левшун Д.С., Комплексная модель защищенных киберфизических систем для их проектирования и верификации / Д.С. Левшун, А.А.Чечулин, И.В.Котенко // Труды учебных заведений связи – 2019 - Т. 5. № 4 - С. 114-123
26. Петренко А.А., Способ повышения устойчивости LTE-сети в условиях деструктивных кибератак / А.А.Петренко, С.А. Петренко // Вопросы кибербезопасности – 2015 - № 2 (10) - С. 36-42
27. Петренко С.А., Проблема самовосстановления критически важных информационных систем в условиях кибервойны / С.А.Петренко, А.Г.Ломако, О.Н.Амельченкова, А.В. Зотова // Защита информации. Инсайд. – 2012 - № 6; 1 - С. 2.
28. Петренко С.А., Онтология кибербезопасности самовосстанавливающихся SMART GRID / С.А.Петренко, А.А. Петренко // Защита информации. Инсайд. – 2016 - № 2 (68) - С. 12-24
29. Путято М.М., Кибербезопасность как неотъемлемый атрибут многоуровневого защищенного киберпространства / М.М.Путято, А.С.Макарян // Прикаспийский журнал: управление и высокие технологии – 2020 - №3 (51) – С. 94-102
30. Путято М.М., Адаптивная система комплексного обеспечения безопасности как элемент инфраструктуры ситуационного центра / М.М.Путято, А.С.Макарян, А.Н.Черкасов, И.Г.Горин // Прикаспийский журнал: управление и высокие технологии – 2020 - №4 (52) – С. 75-84
31. Промыслов В.Г., Синтез архитектуры кибербезопасности для систем управления атомных электростанций / В.Г.Промыслов, К.В.Семенков, А.С.Шумов // Проблемы управления – 2019 - № 3 - С. 61-71

РАЗДЕЛ 2. НАУЧНЫЕ ДОКЛАДЫ ГРАНТОПОЛУЧАТЕЛЕЙ 2022 ГОДА – СОИСКАТЕЛЕЙ УЧЁНОЙ СТЕПЕНИ ДОКТОРА НАУК

Золотарев В.В.
Сибирский государственный университет науки и технологий,
заведующий кафедрой безопасности информационных технологий,
к.т.н., доцент
amida.2@yandex.ru

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ЦИФРОВОЙ СРЕДЫ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Аннотация: В работе будут исследованы и представлены модели структурной динамики управляющих подсистем ООВО, задействованных в цифровой трансформации, с позиций управления информационной безопасностью, включая обеспечивающие и базовые процессы, сформированы критерии оценки и указаны параметры создания цифровой среды ООВО, регулируемые в рамках управления информационной безопасностью.

Для отдельных составляющих инфраструктуры, процессов, моделей и процедур будут представлены собственные низкоуровневые решения, агрегированные на более высоких уровнях в процессы и процедуры управления безопасностью. Такими составляющими будут разработка безопасного программного обеспечения, формирование и обеспечение информационной безопасности сети интернета вещей, управление доступом, повышение осведомленности и технологии работы с данными, информационная безопасность отдельных технологических процессов.

Такими решениями будут подходы по управлению уязвимостями, как в комплексе, в привязке к активам и инфраструктурным решениям, так и на уровне анализа и блокировки уязвимостей программного обеспечения. Будет создана лаборатория разработки безопасного программного обеспечения, исследовательский ситуационный центр управления информационной безопасностью, лаборатория разработки систем интернета вещей. Новые решения по управлению коммуникациями в области интернета вещей также позволят отработать концепцию единой управляемой среды сбора данных о состоянии инфраструктурных объектов, а также защиты информации при транзакциях кампусного проекта на основе технологий динамических сетей.

Ключевые слова: управление информационной безопасностью, цифровая среда, информационная инфраструктура, управление уязвимостями, управление непрерывностью.

Общей целью исследования является разработка методологических основ, комплекса моделей и алгоритмов многокритериального планирования для формирования единого подхода к управлению информационной безопасностью образовательной организации высшего образования в условиях переходных состояний цифровой трансформации.

Цель исследования полностью соответствует текущей цели диссертационного исследования и направлению проводимых исследований, собираемых данных и проектируемых моделей управления информационной безопасностью.

В соответствии с поставленной целью сформулированы следующие задачи:

1. Системный анализ проблемы планирования для задачи обеспечения информационной безопасности цифровой среды образовательной организации высшего образования, включая смежные системы и транзакции данных.
2. Исследование внутренних и внешних структур цифровой среды образовательной организации высшего образования, подвергающихся цифровой трансформации, с позиций единого подхода к управлению информационной безопасностью.
3. Формальное описание процессов и процедур, связанных с управлением информационной безопасностью в условиях цифровой трансформации, особенно в переходных состояниях, для образовательной организации высшего образования.
4. Формирование комплекса моделей и алгоритмов многокритериального планирования параметров цифровой среды образовательной организации высшего образования с позиций управления информационной безопасностью в переходных и итоговых (планируемых) состояниях цифровой трансформации.
6. Аналитико-имитационное моделирование условий реализации единого подхода к управлению информационной безопасностью образовательной организации высшего образования.

7. Проверка работоспособности и реализуемости разработанного специального модельно-алгоритмического обеспечения и апробация разработанных решений в образовательных организациях высшего образования.

Системный анализ проблемы планирования для задачи обеспечения информационной безопасности цифровой среды образовательной организации высшего образования, включая смежные системы и транзакции данных, включающий различные технологии управления информационной безопасностью – это необходимый элемент цифровой трансформации, включенный в различные типы современных стратегий цифровой трансформации предприятий, организаций и госструктур. Вместе с тем вопросы обеспечения информационной безопасности часто рассматриваются как побочные, не влияющие на основные процессы, вспомогательные [1-3]. Вместе с тем в сфере информационной безопасности новое качество этих подсистем означает и новые подходы к управлению информационной безопасностью, такие как решение задач безопасной разработки программного обеспечения, управления доступом, управления данными, работы с персоналом и оценки соответствия стандартам и иным требованиям [4-6].

Кроме того, образовательные организации высшего образования представляют собой объекты особой значимости, объекты критичной инфраструктуры, при этом имея разрозненный набор сил, средств и решаемых задач в области управления информационной безопасностью, а также проистекающий из применяемого подхода «снизу вверх» набор морально и технически устаревших инфраструктурных артефактов в области обеспечения информационной безопасности. Нормой является конфликт интересов, дублирование задач, снижение эффективности использования ресурсов [7]. Реализуемая цифровая трансформация может как усугубить, так и устранить часть этих проблем.

Существует объективная необходимость объединяющих подходов, учитывающих как переходные, так и итоговые состояния цифровой трансформации инфраструктуры, системы управления и технологий работы с данными образовательных организаций высшего образования (ООВО), снижающих влияние отрицательных эффектов цифровой трансформации на информационную безопасность внутренних и внешних (смежных) систем и подсистем, взаимодействующих в образовательном и исследовательском процессе ООВО. Дополнительную проблематику создают вопросы развертывания интеллектуальных киберфизических систем («умные здания», кампусные решения) [8].

При этом очевидно, что при едином подходе фундаментальной основой цифровой трансформации должна являться автоматизированная система управления с многоуровневой сетевой структурой, имеющая общие ситуационные центры управления, средства работы с озерами данных и формирования (накопления) этих данных, единые коммуникации и измерительные устройства, контролирующие инфраструктурные элементы [7, 9, 10, 11].

Исходными данными для выбора методов и подходов к решению поставленных задач были:

1. Усложнение и динамическая реконфигурация систем и подсистем, задействованных в цифровой трансформации ООВО.

2. Неполные или искаженные данные о состоянии систем и подсистем, указанных выше.

3. Неполная, не содержащая резерва, но при этом в отдельных моментах избыточная схема коммуникаций и технологий работы с данными.

Следовательно, в качестве методов и подходов должны быть выбраны декомпозиция, агрегация данных, координация, формирование моделей внутренних и внешних связей. Целесообразно также рассматривать процессную основу моделей и процедур управления безопасностью в общем контексте цифровой трансформации ООВО, особенно в переходных состояниях. Дополнительно возможно рассмотреть методы структурной трансформации сложных систем, в том числе технических и социально-экономических, управления структурной динамикой таких систем, обеспечения заданных параметров их надежности и безопасности.

Для отдельных составляющих инфраструктуры, процессов, моделей и процедур будут представлены собственные низкоуровневые решения, агрегированные на более высоких уровнях в процессы и процедуры управления безопасностью. Такими составляющими будут разработка безопасного программного обеспечения, формирование и обеспечение информационной безопасности сети интернета вещей, управление доступом, повышение осведомленности и технологии работы с данными, информационная безопасность отдельных технологических процессов.

СПИСОК ЛИТЕРАТУРЫ

1. Учебник 4CDTO. Версия 1.1.1. О цифровизации и цифровой трансформации. 2022.
2. Tikhomirov V. Development of University’s Web-Services Smart Education and Smart e-Learning / V. Tikhomirov, N. Dneprovskaya, E. Yankovskaya // Smart Innovation, Systems and Technologies, 41, 2015, p. 265-271.
3. Артамонов В.А. Кибербезопасность в условиях цифровой трансформации социума / В.А. Артамонов, Е.В. Артамонова // Большая Евразия: развитие, безопасность, сотрудничество. – 2022 – №5-1 – с. 777-783.
4. Лукацкий, А. Кибербезопасность цифровой трансформации 2.0 / А. Лукацкий, 2021.
5. Kim B.-H. Development of cyber information security education and training system / B.-H. Kim, K.-C. Kim, S.-E. Hong, S.-Y. Oh // Multimedia Tools and Applications – 2017 – vol. 76(4) – pp. 6051–6064.
6. Sillanpää M. Social Engineering Intrusion: A Case Study / M. Sillanpää, J. Hautamäki // in proc. IAIT2020: The 11th International Conference on Advances in Information Technology – 2020 – p. 1-5.
7. Офицеров, А.И. Концептуальные основы обеспечения комплексной безопасности критически важных объектов / А.И. Офицеров, О.О. Басов, С.С. Бачурин / Экономика. Информатика 2020 – Том 47, № 1. – с. 154-162.
8. Abramov M. V. The model of the attacker's competence profile in the task of analyzing the security of information systems personnel from socioengineering attacks / M. V. Abramov, A. A. Azarov, T. V. Tulupeva and al. // Information management systems. – 2016. – №. 4 (83). – С. 77–84.
9. Кушко Е.А. Метод реализации защищенного обмена данными на основе динамической топологии сети / Е.А. Кушко // Вестник СибГУТИ – 2020 – № 4 (52) – С. 39-52.
10. Garcia-Valls M. Reliable software technologies and communication middleware: A perspective and evolution directions for cyber-physical systems, mobility, and cloud computing / M. Garcia-Valls // Future Generation Computer Systems – Vol. 71 – pp. 171 –176.
11. Platzer A. Logical Foundations of Cyber-Physical Systems / A. Platzer // Springer, 2018. – 662 p.

Иванов Д.В.
Самарский национальный исследовательский университет имени академика С.П. Королева,
доцент кафедры безопасности информационных систем,
к.ф.-м.н., доц.,
dvi85@list.ru

КОМПЛЕКС МОДЕЛЕЙ С ДЛИННОЙ ПАМЯТЬЮ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ ТРАФИКА

Аннотация: В докладе исследования предлагается комплекс линейных и нелинейных моделей трафика компьютерных сетей на основе уравнений с разностями дробного порядка. Разработаны методы структурно-параметрической идентификации моделей трафика компьютерных сетей с длинной памятью при наличии ошибок в переменных на основе генетических алгоритмов, позволяющие выявлять аномалии трафика.

Ключевые слова: Моделирование трафика компьютерных сетей, аномалии трафика, временные ряды с длинной памятью, разности дробного порядка, ошибки в переменных, генетические алгоритмы.

Моделирование трафика компьютерных сетей является важной и актуальной задачей. Для моделирования трафика компьютерных сетей широко используются методы анализа временных рядов [1]. Было установлено, что трафик компьютерных сетей имеет ряд особенностей таких как самоподобие и наличие длинной памяти. [2-4]. Самой известной моделью, позволяющей моделировать эффекты длинной памяти является модель FARIMA (fractionally difference autoregressive integrated moving average) [5, 6]:

Говорят, что ряд z_i отвечает процессу FARIMA(r, α , r_1), если:

$$\Delta^{\alpha}\left(z_i - \sum_{m=1}^{r} b^{(m)} z_{i-m} \right) = \sum_{m=0}^{r_1} a^{(m)} \varepsilon_{i-m}, \qquad (1)$$

где, $\Delta^{\alpha} z_i = \sum_{j=0}^{i} (-1)^j \binom{\alpha}{j} z_{i-j}$, $\binom{\alpha}{j} = \frac{\Gamma(\alpha+1)}{\Gamma(j+1)\Gamma(\alpha-j+1)}$, $\Gamma(\alpha) = \int_0^{\infty} e^{-t} t^{\alpha-1} dt$ -Гамма-функция.

Обзор методов по выявлению аномалий трафика приведен в статье [7]. Как следует из обзора для выявления аномалий трафика на сегодняшний день используются только модели ARFIMA и GARMA (generalized autoregressive moving average) [8-11].

Модели трафика компьютерных сетей на основе моделей с длинной памятью не исчерпываются только моделями ARFIMA и GARMA. Для многих реализаций трафика характерно наличие трендовых и периодических составляющих. Кроме того, для трафика характерны различные нелинейные эффекты, связанные с ограничением пропускной способности канала и оборудования. Декомпозиция таких реализаций трафика и выделение стохастической компоненты с длинной памятью приводит к появлению ошибок в переменных.

Применение метода наименьших квадратов для идентификации моделей с ошибками в переменных с длинной памятью приводит к крайне неточным результатам. В работе предлагаются методы структурно-параметрической идентификации комплекса моделей с длинной памятью с ошибками переменных на основе метода обобщенных полных наименьших квадратов [12, 13] и генетических алгоритмов [14].

Одним из недостатков модели FARIMA является сложность в оценке коэффициентов $a^{(m)}$ правой части. В своей работе будем использовать авторегрессии, данные модели линейны по параметрам $b^{(m)}$. Это позволяет упростить процедуру оценивания при незначительном увеличении числа параметров.

Предполагается использовать следующий комплекс моделей:

1. Авторегрессии, описываемой уравнениями с разностями дробного порядка с помехой наблюдения в выходном сигнале

$$z_i = \sum_{m=1}^{r} b^{(m)} \Delta^{\alpha_m} z_{i-1} + \varepsilon_i, \; y_i = z_i + \xi_i. \qquad (2)$$

2.FAR (Fractional differencing autoregressive) с помехой наблюдения в выходном сигнале

$$\Delta^{\alpha}\left(z_i-\sum_{m=1}^{r}b_0^{(m)}z_{i-m}\right)=\varepsilon_i,\ y_i=z_i+\xi_i. \quad (3)$$

3.GAR (Gegenbauer autoregressive) с помехой наблюдения в выходном сигнале

$$\nabla_{\nu}^{\alpha}\left(z_i-\sum_{m=1}^{r}b_0^{(m)}z_{i-m}\right)=\varepsilon_i,\ y_i=z_i+\xi_i. \quad (4)$$

где $\nabla_{\nu}^{\alpha}\equiv\left(1-2\nu B+B^2\right)^{\alpha},0<\alpha,\ 0<\nu\le 1$оператор сдвига назад $Bz_i=z_{i-1}$. ∇_{ν}^{α} можно представить в виде

$$\nabla_{\nu}^{\alpha}z_i=\sum_{j=0}^{i}C_j^{\alpha}(\nu)z_{i-j},\ C_j^{\alpha}(\nu)=\sum_{k=0}^{[j/2]}(-1)^k\Gamma(\alpha+j-k)\frac{(2\nu)^{j-2k}}{\Gamma(\alpha)\Gamma(k+1)\Gamma(j-2k+1)}.$$

4. Авторегрессия с разностями дробного порядка с помехой наблюдения в выходном сигнале с билинейным обновлением:

$$z_i=\sum_{m=1}^{r}b^{(m)}\Delta^{\alpha_m}z_{i-1}+\sum_{m=1}^{r_1}c^{(m)}\Delta^{\gamma_m}z_{i-2}\varepsilon_{i-1}+\varepsilon_i,\ y_i=z_i+\xi_i. \quad (5)$$

5. Рассмотреть модели 1-4 в предположении, что помеха наблюдения дробный белый шум $\Delta^{\beta}\xi_i$.

Для определения аномалий трафика необходимо оценить параметры авторегрессий. Предлагается использовать итерационный двухэтапный алгоритм метода сепарабельных наименьших квадратов [15].

На первом этапе оцениваются линейные параметры методом обобщенных полных наименьших квадратов [12, 13]. На втором этапе с помощью генетического алгоритма оцениваются нелинейные параметры [14]. Представленные в [12-14] тестовые примеры показывают высокую точность оценки параметров моделей. Это, в свою очередь, должно способствовать лучшему выявлению аномалий, по сравнению с известными методами.

СПИСОК ЛИТЕРАТУРЫ

33. Jung, S. A Prediction Method of Network Traffic Using Time Series Models / S. Jung, C. Kim, Y. Chung // Computational Science and Its Applications. Lecture Notes in Computer Science. — 2006. — № 3682. https://doi.org/10.1007/11751595_26
34. Leland W.E., Taqqu M.S., Willinger W., and Wilson D.V. On the self-similarnature of ethernet traffic / W.E. Leland, M.S. Taqqu, W. Willinger, D.V. Wilson // IEEE/ACM Transactions of Networking. — 1994. — № 2(1). — pp 1-15.
35. Цыбаков Б.С. Модель телетрафика на основе самоподобного случайного процесса/ Б.С. Цыбаков // Радиотехника. — 1999. — 5. — С. 24–31.
36. Шелухин О.И., Осин А. В., Смольский С.М. Самоподобие и фракталы. Телекоммуникационные приложения. / Под ред. О. И. Шелухина. — М.:ФИЗМАТЛИТ, 2008. — 368 с. — ISBN 978-5-9221-0949-9.
37. Granger, C.W. An introduction to long-memory time series models and fractional differencing./ C.W. Granger; R. Joyeux // Time Ser. Anal. . — 1980. — №1. — pp.15–29.
38. Hosking, J.R.M. Fractional differencing. / J.R.M Hosking// Biometrika. — 1981. — № 68, pp. 165–176.
39. Husák M. Survey of Attack Projection, Prediction, and Forecasting in Cyber Security/ M. Husák, J. Komárková, E. Bou-Harb and P. Čeleda // IEEE Communications Surveys & Tutorials. — 2019. — № 21(1), pp. 640–660. doi: 10.1109/COMST.2018.2871866.
40. Zhan Z. Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study/Z. Zhan, M. Xu, S. Xu// IEEE Transactions on Information Forensics and Security. — 2013. — № 8. — pp. 1775-1789.
41. Zhan Z. Predicting Cyber Attack Rates With Extreme Values/ Z. Zhan, M. Xu, S. Xu // IEEE Transactions on Information Forensics and Security. — 2015. — № 10. — pp. 1666-1677.
10. Abdullah A. B. Intrusion detection forecasting using time series for improving cyber defence / A. B. Abdullah, T. R. Pillai, and L. Z. Cai //International Journal of Intelligent Systems and Applications in Engineering. — 2015. — № 3(1) pp. — 28–33.

11. Pillai T. R. Imran,Predictive modeling for intrusions in communication systems using GARMA and ARMA models. / T.R. Pillai, S. Palaniappan, A. Abdullah, and H. M. Imran // i 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW). — 2015.
12. Ivanov, D. Symmetrical augmented system of equations for the parameter identification of discrete fractional systems by generalized total least squares /D. Ivanov, A. Zhdanov // Mathematics. – 2021. – Vol. 9. – No 24. – DOI 10.3390/math9243250.
13. Ivanov, D. V. Identification of linear dynamic systems of fractional order with errors in variables based on an augmented system of equations / D. V. Ivanov // Journal of Samara State Technical University. Ser. Physical and Mathematical Sciences. – 2021. – Vol. 25. – No 3. – P. 508-518. – DOI 10.14498/vsgtu1854
14. Ivanov, D. V. Genetic algorithm of structural and parametric identification of Gegenbauer autoregressive with noise on output / D. V. Ivanov, V. V. Engelgardt, I. L. Sandler // Procedia Computer Science: 8, Xiamen, 27–28 января 2018 года. – Xiamen, 2018. – P. 619-625. – DOI 10.1016/j.procs.2018.04.304.
15. Golub G. H. Separable nonlinear least squares: the variable projection method and its applications/ G. H. Golub, V. Pereyra // Inverse Problems. — 2003. — № 19.

Когос К.Г.
НИЯУ МИФИ, доцент, зам. директора, к.т.н.,
kgkogos@mephi.ru

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СКРЫТОГО КАНАЛА В СЕТЯХ ПАКЕТНОЙ ПЕРЕДАЧИ ДАННЫХ

Аннотация: В данном докладе исследуются скрытые каналы, устойчивые к традиционным способам защиты информации ограниченного доступа, передаваемой по сети, таким как шифрование, туннелирование и межсетевое экранирование трафика. Задача состоит в построении математической модели для оценки пропускной способности скрытого канала, заданного в общем виде, не имеющего ограничений на способ построения, мощность используемого алфавита, распределение случайных величин, описывающих входные характеристики скрытого канала.

Ключевые слова: СКРЫТЫЕ КАНАЛЫ, МЕЖПАКЕТНЫЕ ИНТЕРВАЛЫ, УТЕЧКА ИНФОРМАЦИИ, ЗАЩИТА ИНФОРМАЦИИ

Для оценки пропускной способности скрытого канала ν здесь и далее выбран метод, основанный на оценке взаимной информации случайных величин *X* и *Y*, описывающих входные и выходные характеристики скрытого канала соответственно (1):

$$\nu = \max_X \left\{ \frac{I(X,Y)}{\tau} \right\}, \tag{1}$$

где τ — среднее время передачи одного пакета.

Взаимную информацию случайных величин *X, Y* предлагается оценить как (2)

$$I(X,Y) = H(Y) - H(Y|X), \tag{2}$$

где $H(Y) = -\sum_{i=1}^{n} p_{вых}(i) \log_2 p_{вых}(i)$ — энтропия случайной величины *Y*, $H(Y|X) = -\sum_{j=1}^{n} p_{вх}(j) \left(\sum_{i=1}^{n} p_{вых}(i|j) \log_2 p_{вых}(i|j) \right)$ — условная энтропия случайной величины *Y* относительно случайной величины *X*, $p_{вх}(j)$ — вероятность отправки символа «*i*», $p_{вых}(i)$ — вероятность распознавания получателем символа «*i*», $p_{вых}(i \mid j)$ — условная вероятность распознавания получателем символа «*i*» при отправке символа «*j*».

Пакеты имеют различную длину и требуют определенного времени на передачу в зависимости от их длины. Кроме того, пакеты не передаются подряд друг за другом, а между ними присутствуют межпакетные интервалы, что также влияет на среднее время передачи пакета. В связи с этим полное среднее время передачи пакета τ может быть получено как сумма двух величин: среднего времени для отправки пакета в зависимости от его длины $\tau_{отпр}$ и средней длины межпакетного интервала $t_{ср}$.

Пропускная способность канала связи β может быть представлена в следующем виде (3):

$$\beta = \frac{l_{ср}}{\tau_{отпр}}, \tag{3}$$

где $l_{ср}$ — средняя длина передаваемых пакетов.

Отсюда τ равно (4)

$$\tau = \frac{l_{ср}}{\beta} + t_{ср}. \tag{4}$$

Рассмотрим скрытый канал по памяти, в котором данные передаются только с помощью изменения длин пакетов. Пусть $L_{вх}$ — случайная величина, описывающая входные характеристики такого скрытого канала (5):

$$L_{вх} = \begin{pmatrix} l(1) & l(2) & \cdots & l(n) \\ p_{L_{вх}}(1) & p_{L_{вх}}(2) & \cdots & p_{L_{вх}}(n) \end{pmatrix}, \quad (5)$$

где $l(i)$ — длина пакета, которую отправитель должен послать для передачи символа *«i»*, $p_{L_{вх}}(i)$ — вероятность передачи символа *«i»*, $i = \overline{1,n}; n \in N$, — параметр скрытого канала (количество различных используемых длин пакетов).

С целью минимизации средней длины передаваемых по скрытому каналу пакетов здесь и далее без потери для общности считаем, что значения случайной величины $L_{вх}$ упорядочены по убыванию вероятностей, то есть $l(i) < l(i+1)$, $p_{L_{вх}}(i) \geq p_{L_{вх}}(i+1)$, $i = \overline{1,n-1}$.

Таким образом, случайная величина, описывающая выходные характеристики скрытого канала по памяти $L_{вых}$, в условиях отсутствия переупорядочивания пакетов, остается практически неизменной: $L_{вх} = L_{вых}$, а ее энтропия определяется значениями параметров скрытого канала $n, \{p_{L_{вх}}(i)\}, i = \overline{1,n}$ (6):

$$H(L_{вых}) = -\sum_{i=1}^{n} p_{L_{вх}}(i) \log_2 p_{L_{вх}}(i). \quad (6)$$

Тогда средняя взаимная информация в случае канала без ошибок, то есть без переупорядочения пакетов, определяется выражением (7):

$$I(L_{вх}, L_{вых}) = H(L_{вых}) = -\sum_{i=1}^{n} p_{L_{вх}}(i) \log_2 p_{L_{вх}}(i). \quad (7)$$

Средняя взаимная информация при возможности переупорядочения пакетов определяется выражением (8):

$$\begin{aligned} &I(L_{вх}, L_{вых}) = H(L_{вых}) - H(L_{вых} | L_{вх}) = \\ &= -\sum_{i=1}^{n} p_{L_{вых}}(i) \log_2 p_{L_{вых}}(i) + \sum_{j=1}^{n} p_{L_{вх}}(j) \left(\sum_{i=1}^{n} p_{L_{вых}}(i|j) \log_2 p_{L_{вых}}(i|j) \right), \end{aligned} \quad (8)$$

где $p_{L_{вых}}(i \mid j)$ — условная вероятность получения пакета длины $l(i)$ при отправке пакета длины $l(j)$, $p_{L_{вых}}(i)$ — вероятность получения пакета длины $l(i)$.

Средняя длина передаваемых по скрытому каналу пакетов равна математическому ожиданию случайной величины $L_{вх}$ (9):

$$E(L_{вх}) = \sum_{i=1}^{n} p_{L_{вх}}(i) l(i). \quad (9)$$

Теперь рассмотрим второй параметр исследуемого гибридного скрытого канала — межпакетные интервалы. Пусть $T_{вх}$ — случайная величина, описывающая входные характеристики скрытого канала по времени (10):

$$T_{вх} = \begin{pmatrix} t(1) & t(2) & \cdots & t(m) \\ p_{T_{вх}}(1) & p_{T_{вх}}(2) & \cdots & p_{T_{вх}}(m) \end{pmatrix}, \quad (10)$$

где $t(i)$ — длина межпакетного интервала, которую отправитель должен послать для передачи символа *«i»*, $p_{T_{вх}}(i)$ — вероятность передачи символа *«i»*, $i = \overline{1,m}; m \in N$, — параметр скрытого канала (количество различных используемых длин межпакетных интервалов).

С целью минимизации средней длины межпакетных интервалов при передаче пакетов по скрытому каналу по времени здесь и далее без потери для общности считаем, что значения случайной величины $T_{вх}$ упорядочены по убыванию вероятностей, то есть (11):

$$t(i) < t(i+1),\ p_{T_{вх}}(t_i) \geq p_{T_{вх}}(t_{i+1}) \text{ для } i = \overline{1, m-1}. \qquad (11)$$

На рисунке 1 приведена схема изменения значения длины межпакетного интервала при движении пакетов от отправителя к получателю. Здесь d_1 и d_2 — конкретные значения, принимаемые одинаково распределенными случайными величинами D_1 и D_2, описывающими время следования пакетов от отправителя до получателя по скрытому каналу.

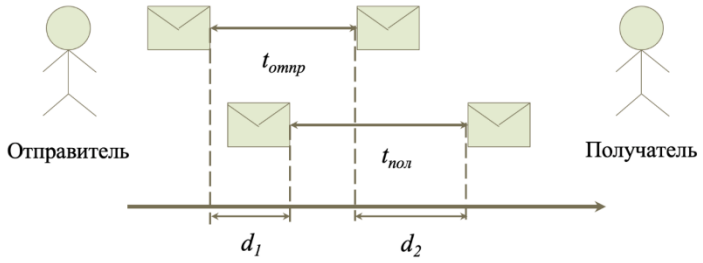


Рис. 1. Изменение длины межпакетного интервала вследствие передачи пакетов

Итак, длина полученного межпакетного интервала на стороне получателя $t_{пол}$ равна (12)

$$t_{пол} = t_{отпр} + d_2 - d_1, \qquad (12)$$

где $t_{отпр}$ — длина отправленного межпакетного интервала.

На основе полученного интервала $t_{пол}$ получатель находит наиболее близкое к нему значение межпакетного интервала $t(j)$ из набора $\{t(j)\}, j = \overline{1, m}$. На рисунке 2 приведена схема декодирования информации из межпакетных интервалов.

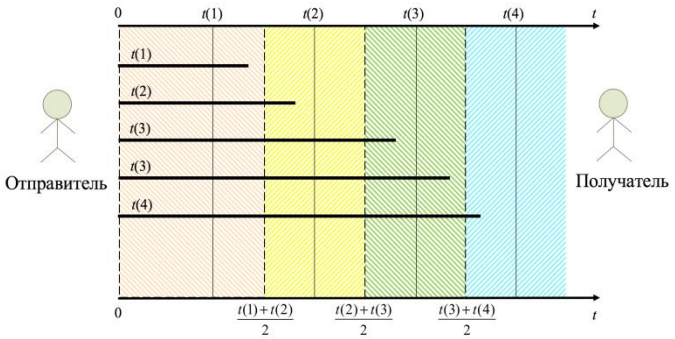


Рис. 2. Схема декодирования информации из полученных длин межпакетных интервалов

Таким образом, получатель декодирует интервал $t(j)$, $j = \overline{2, m-1}$, если значение полученного интервала $t_{пол}$ лежит в следующих пределах (13):

$$\frac{t(j-1) + t(j)}{2} < t_{пол} \leq \frac{t(j) + t(j+1)}{2}. \qquad (13)$$

Для $t(1)$ условие декодирования выглядит следующим образом (14):

$$t_{пол} \leq \frac{t(1) + t(2)}{2}. \qquad (14)$$

А для того, чтобы получить интервал $t(m)$ необходимо выполнение условия (15)

$$\frac{t(m-1) + t(m)}{2} < t_{пол}. \qquad (15)$$

Для того чтобы не учитывать граничные условия для $t(1)$ и $t(m)$, вводятся две новые величины: $t(0) = -\infty$ и $t(m+1) = +\infty$. Таким образом, формула (12) (первая для интервалов) становится применима для всех возможных межпакетных интервалов.

Найдем условную вероятность $p_{T_{вых}}(j \mid i)$ получения интервала $t(j)$ при условии отправки $t(i)$. Для этого после отправки интервала $t(i)$ полученный интервал должен попасть в промежуток, в котором интервал будет распознан получателем как $t(j)$, то есть должно быть выполнено неравенство (16):

$$\frac{t(j-1)+t(j)}{2} - t(i) < d_2 - d_1 \le \frac{t(j)+t(j+1)}{2} - t(i). \tag{16}$$

Таким образом, условная вероятность $p_{T_{вых}}(j \mid i)$ зависит от значения разности времени следования двух соседних пакетов в канале $d_2 - d_1$, которое принимает случайная величина $D_{2D} = D_2 - D_1$. Обозначим функцию распределения случайной величины D_{2D} как $F_{2D}(x)$, а плотность распределения — $\rho_{2D}(x)$.

С использованием плотности распределения формула для $p(j \mid i)$ выглядит следующим образом (17):

$$p_{T_{вых}}(j \mid i) = \int_{\frac{t(j-1)+t(j)}{2}-t(i)}^{\frac{t(j)+t(j+1)}{2}-t(i)} \rho_{2D}(x)dx. \tag{17}$$

Пусть $T_{вых}$ — случайная величина, описывающая выходные характеристики скрытого канала на основе изменения длин межпакетных интервалов. Она имеет следующий вид (18):

$$T_{вых} = \begin{pmatrix} t(1) & t(2) & \cdots & t(m) \\ \sum_{i=1}^{m} p_{T_{вх}}(i)\, p_{T_{вых}}(1 \mid i) & \sum_{i=1}^{m} p_{T_{вх}}(i)\, p_{T_{вых}}(2 \mid i) & \cdots & \sum_{i=1}^{m} p_{T_{вх}}(i)\, p_{T_{вых}}(m \mid i) \end{pmatrix}. \tag{18}$$

Тогда энтропия случайной величины $H(T_{вых})$ принимает вид (19):

$$H(T_{вых}) = -\sum_{i=1}^{m} p_{T_{вых}}(i) \log_2 p_{T_{вых}}(i) = -\sum_{i=1}^{m} \left(\sum_{j=1}^{m} (p_{T_{вх}}(j)\, p_{T_{вых}}(i \mid j)) \log_2 \sum_{j=1}^{m} (p_{T_{вх}}(j)\, p_{T_{вых}}(i \mid j)) \right), \tag{19}$$

где $p_{T_{вых}}(i)$ — вероятность распознавания символа «*i*».

Условная энтропия $H(T_{вых} \mid T_{вх})$ случайной величины $T_{вых}$ относительно случайной величины $T_{вх}$ с учетом полученных ранее выражений равна (20):

$$H(T_{вых} \mid T_{вх}) = -\sum_{i=1}^{m} p_{T_{вх}}(i) \left(\sum_{j=1}^{m} p_{T_{вых}}(j \mid i) \log_2 p_{T_{вых}}(j \mid i) \right). \tag{20}$$

Средняя длина межпакетного интервала $E(T_{вх})$ — математическое ожидание случайной величины $T_{вх}$ (21):

$$E(T_{вх}) = \sum_{i=1}^{m} t(i)\, p_{T_{вх}}(i). \tag{21}$$

На основе приведенных выше рассуждений составим математическую модель гибридного скрытого канала на основе изменения длин пакетов и межпакетных интервалов. Пропускную способность предложенного скрытого канала можно вычислить по следующей формуле (22):

$$\begin{aligned} \nu &= \max_{L_{вх}, T_{вх}} \left\{ \frac{I(L_{вх}, L_{вых}) + I(T_{вх}, T_{вых})}{\tau} \right\} = \\ &= \beta \max_{L_{вх}, T_{вх}} \left\{ \frac{H(L_{вых}) - H(L_{вых} \mid L_{вх}) + H(T_{вых}) - H(T_{вых} \mid T_{вх})}{\left(E(L_{вх}) + E(T_{вх})\beta\right)} \right\}. \end{aligned} \tag{22}$$

Максимизация производится по параметрам $L_{вх}, T_{вх}$, которые определяют входные характеристики скрытого канала. Среди них мощности n и m алфавитов, которыми кодируется передаваемая информация, параметры $\{l(i)\}, i = \overline{1,n}$ и $\{t(i)\}, i = \overline{1,m}$, которые характеризуют конкретные значения, кодирующие передаваемую информацию, а также $\{p_{L_{вх}}(i)\}, i = \overline{1,n}$ и $\{p_{T_{вх}}(i)\}, i = \overline{1,m}$ — распределения вероятностей отправки символов для передачи информации.

Формула для пропускной способности скрытого канала принимает следующий вид (23):

$$\nu = \beta \max_{\{p_{L_{вх}}(i)\},\{l(i)\},n,\{p_{T_{вх}}(i)\},\{t(i)\},m} \frac{\left(\begin{array}{l} -\sum\limits_{i=1}^{n} p_{L_{вх}}(i)\log_2 p_L(i) + \sum\limits_{j=1}^{n} p_{L_{вх}}(j)\left(\sum\limits_{i=1}^{n} p_{L_{вых}}(i|j)\log_2 p_{L_{вых}}(i|j) \right) - \\ -\sum\limits_{i=1}^{m}\sum\limits_{j=1}^{m} \left(p_{T_{вх}}(j) \int\limits_{\frac{t(j-1)+t(j)}{2}-t(i)}^{\frac{t(j)+t(j+1)}{2}-t(i)} \rho_{2D}(x)dx \right) \log_2 \sum\limits_{j=1}^{m} \left(p_{T_{вх}}(j) \int\limits_{\frac{t(j-1)+t(j)}{2}-t(i)}^{\frac{t(j)+t(j+1)}{2}-t(i)} \rho_{2D}(x)dx \right) + \\ +\sum\limits_{i=1}^{m} p_{T_{вх}}(i) \sum\limits_{j=1}^{m} \left(\int\limits_{\frac{t(j-1)+t(j)}{2}-t(i)}^{\frac{t(j)+t(j+1)}{2}-t(i)} \rho_{2D}(x)dx \right) \log_2 \left(\int\limits_{\frac{t(j-1)+t(j)}{2}-t(i)}^{\frac{t(j)+t(j+1)}{2}-t(i)} \rho_{2D}(x)dx \right) \end{array} \right)}{\sum\limits_{i=1}^{n}\left(l(i)p_{L_{вх}}(i) \right) + \beta \sum\limits_{i=1}^{m}\left(t(i)p_{T_{вх}}(i) \right)}. \quad (23)$$

В скрытом канале по времени увеличение разности $t(i+1) - t(i)$ ведет за собой увеличение среднего времени передачи пакетов и снижение пропускной способности скрытого канала. Указанная величина для каждого $i = \overline{1, m-1}$ определяется плотностью вероятности $\rho_{2D}(x)$ разности независимых одинаково распределнных случайных величин D_1 и D_2. В связи с этим здесь и далее считаем, что случайная величина $T_{вх}$ принимает следующий вид (24):

$$T_{вх} = \begin{pmatrix} T & 2T & \cdots & mT \\ p_{T_{вх}}(1) & p_{T_{вх}}(2) & \cdots & p_{T_{вх}}(m) \end{pmatrix}, \quad (24)$$

где T — параметр скрытого канала, при котором его пропускная способность максимальна в условиях заданной нагрузки на сеть.

При таких значениях длин межпакетных интервалов условная вероятность декодировать символ *«j»* при отправке символа *«i»* по скрытому каналу по времени (по формуле условной вероятности (17)) равна (25)

$$p_{T_{вых}}(j \mid i) = \begin{cases} \int\limits_{(j-i-\frac{1}{2})T}^{(j-i+\frac{1}{2})T} \rho_{2D}(x)dx,\ j = \overline{2, m-1} \\ \int\limits_{-\infty}^{(j-i+\frac{1}{2})T} \rho_{2D}(x)dx,\ j = 1 \\ \int\limits_{(j-i-\frac{1}{2})T}^{+\infty} \rho_{2D}(x)dx,\ j = m \end{cases}. \quad (25)$$

Вопросы применения методов поточного шифрования для защиты трафика исследовали, например, авторы [2]. При использовании поточных алгоритмов шифрования длина сообщения не изменяется, поэтому для исследования выбран скрытый канал, построенный следующим образом: с целью минимизации нагрузки на канал связи и увеличения пропускной способности скрытого канала для передачи символа *«i»* необходимо отправить пакет длины $l(i) = l_{фикс} + i - 1$, где $l_{фикс} \in N$ — минимально возможная длина пакета, которая равна длине заголовка пакета, то есть это параметр используемого протокола. Таким образом, $L_{вх}$ имеет следующий вид (26):

$$L_{вх} = \begin{pmatrix} l_{фикс} & l_{фикс}+1 & \cdots & l_{фикс}+n-1 \\ p_{L_{вх}}(1) & p_{L_{вх}}(2) & \cdots & p_{L_{вх}}(n) \end{pmatrix}. \quad (26)$$

На основе приведенных выше рассуждений формула пропускной способности (ПС два) для случая поточного шифрования трафика приобретает следующий вид (27):

$$\nu = \beta \max_{\{p_{L_{вх}}(i)\},n,\{p_{T_{вх}}(i)\},T,m} \frac{\left(\begin{array}{l} -\sum_{i=1}^{n} p_{L_{вх}}(i)\log_2 p_{L_{вх}}(i) + \sum_{j=1}^{n} p_{L_{вх}}(j)\left(\sum_{i=1}^{n} p_{L_{вых}}(i|j)\log_2 p_{L_{вых}}(i|j) \right) - \\ -\sum_{i=1}^{m}\sum_{j=1}^{m}\left(p_{T_{вх}}(j) \int_{(j-i-\frac{1}{2})T}^{(j-i+\frac{1}{2})T} \rho_{2D}(x)dx \right)\log_2 \sum_{j=1}^{m}\left(p_{T_{вх}}(j) \int_{(j-i-\frac{1}{2})T}^{(j-i+\frac{1}{2})T} \rho_{2D}(x)dx \right) + \\ +\sum_{i=1}^{m} p_{T_{вх}}(i)\sum_{j=1}^{m}\left(\int_{(j-i-\frac{1}{2})T}^{(j-i+\frac{1}{2})T} \rho_{2D}(x)dx \right)\log_2 \left(\int_{(j-i-\frac{1}{2})T}^{(j-i+\frac{1}{2})T} \rho_{2D}(x)dx \right) \end{array} \right)}{l_{фикс} - 1 + \sum_{i=1}^{n} i p_{L_{вх}}(i) + \beta T \sum_{i=1}^{m} i p_{T_{вх}}(i)}. \quad (27)$$

СПИСОК ЛИТЕРАТУРЫ

1. Popescu, A. On Kleinrock's Independence Assumption / Network Performance Engineering. Lecture Notes in Computer Science. — 2011.
2. Архангельская, А.В. Характеристики области эффективного применения методов поточного шифрования для защиты трафика в телекоммуникационных системах / Информационное противодействие угрозам терроризма. — 2005.
3. Hernandez, A. One-way delay measurement and characterization / Proceedings of the International Conference on Networking and Services. — 2007.
4. Sagatov, E.S. Composite distribution for one-way packet delay in the global network / Proceedings of the 24th Telecommunications Forum. — 2016.
5. Sukhov, A. Generating function for network delay / Journal of High Speed Networks. — 2016.
6. Грушо, А.А. Статистические скрытые каналы / Материалы XVII Общероссийской научной конференции «Методы и технические средства обеспечения безопасности информации». — 2008.
7. Cabuk, S. IP covert timing channels: design and detection / Proceedings of the eleventh ACM conference on computer and communications security. — 2004.
8. Shah, G. Keyboards and Covert Channels / Proceedings of The15th USENIX Security Symposium. — 2009.
9. Sellke, S.H. Covert TCP/IP timing channels: theory to implementation / Proceedings of the twenty-eighth conference on computer communications. — 2009.
10. Armitage, G.J. Stealthier inter-packet timing covert channels / G/ Proceedings of 10th International IFIP TC 6 Networking Conference. — 2011.

Частикова В.А.
ФГБОУ ВО «Кубанский государственный технологический университет», доцент кафедры компьютерных технологий и информационной безопасности, канд. техн. наук, доцент,
chastikova_va@mail.ru

МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ АНАЛИЗА ИНЦИДЕНТОВ ДЛЯ РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация: в статье изложено построение методологии интеллектуального анализа событий безопасности, предназначенной для мониторинга распределённых информационных систем и содержащей совокупность подходов, использующих различные методы машинного обучения, а именно: методы глубокого обучения, искусственные иммунные систем, алгоритмы роевого интеллекта, генетические алгоритмы, экспертные системы. Основу методологии составляет принцип гибридизации данных интеллектуальных методов в контексте подмодулей системы анализа событий для решения специализированных задач. В исследовании представлены анализ современного состояния исследований в области, новизна предлагаемой методологии и ожидаемые научные результаты реализации проекта.

Ключевые слова: система обнаружения вторжений, сетевая атака, модифицированный генетический алгоритм дуэлей, глубокое обучение, искусственная иммунная система, нейроиммунный подход.

Ключевой целью исследования является разработка методологии анализа событий информационной безопасности в распределенных системах. Значимость и актуальность связана с острой необходимостью обеспечения сетевой безопасности информационных систем средних и крупных организаций, хранящих и обрабатывающих существенный объем конфиденциальных сведений, требующий регулярного контроля и защиты. Для мониторинга безопасности специалисты применяют различные продукты, предоставляющие инструменты контроля за состоянием среды по ключевым показателям, логам инцидентов, сетевому трафику. Но для таких систем остаётся актуальным вопрос эффективности механизмов, обеспечивающих автоматический анализ событий. Она определяется адаптивностью алгоритмов под новые схемы атак, цепочек инцидентов для своевременного и системного выявления действий злоумышленников с минимальной нагрузкой на операторов системы безопасности. Данные инструментальные комплексы требуют регулярной поддержки баз сигнатур, настройки, используют классические подходы, основанные на методах сигнатурного анализа, статистической вероятности, экспертных систем, которые характеризуются малой гибкостью, адаптивностью, в отличие от методов машинного обучения. Предложенная методология предполагает построение комплексной системы анализа инцидентов безопасности (САИБ), выполняющей множество разнородных функций. Для неё требуется определение перечня ключевых модулей, решаемых ими задач и подходов их реализации.

В качестве основных задач исследования необходимо провести анализ интеллектуальных подходов построения систем обнаружения и анализа инцидентов, разработать методики построения систем обнаружения вторжений, анализа инцидентов биометрической идентификации и аутентификации в распределенных средах, анализа и корреляции событий безопасности, модуля агрегации и визуализации данных, а также модуля сжатия данных. Разработка комплекса программных продуктов, реализующих предложенные методики для распределенных систем различных объектов экономической инфраструктуры.

Наиболее распространёнными методами анализа событий являются классические экспертные системы, сигнатурные методы, методы статистического анализа, зарекомендовавшие себя благодаря стабильности, эффективности при определении известных инцидентов [1]. Системы, основанные на подходах машинного обучения, несмотря на высокую гибкость и эффективность в прикладных задачах [2, 3], ещё не получили широкого распространения в современных комплексах мониторинга безопасности, т.к. менее исследованы и отработаны. Но в связи с высокими перспективами систем, адаптивных к малознакомым схемам инцидентов, многие корпорации заинтересованы развиваться в направлении внедрения нейронных сетей и иных интеллектуальных методов [4]. Это связано и с сложностью формирования специалистами для классических систем баз сигнатур, требующих регулярного обновления.

Помимо названных недостатков, в данный момент всё большее распространение получают системы биометрической аутентификации, которые характеризуются рядом особенностей, в силу чего

инциденты, связанные с их эксплуатацией могут быть нетипичными для классических методов идентификации личности [5] и требуют отдельного подхода к анализу.

Таким образом, методы машинного обучения являются перспективным направлением развития современных САИБ, т.к. их комплексное применение с классическими подходами способно обеспечить одновременно и устойчивость, и адаптивность идентификации угроз.

Главной задачей САИБ является анализ и корреляция событий ИБ, для чего проводится агрегация, нормализация, фильтрация, классификация, корреляция и приоритезация событий.

Результаты формируются в виде настраиваемых графических отчетов и предупреждений, облегчающих мониторинг инфраструктуры распределённой системы путём выявления отклонений ключевых показателей по выбранным критериям [6, 7].

В основу модулей системы САИБ вошли наиболее перспективные, активно развивающиеся и демонстрирующие эффективность интеллектуальные методы машинного обучения различных классов: нейросетевые методы глубокого обучения, искусственные иммунные системы, генетические алгоритмы эволюционной имитации, метаэвристические алгоритмы роевого интеллекта, а также классические экспертные системы [8].

Современные архитектуры нейронных сетей характеризуются высокой гибкостью, адаптивностью, поэтому они повсеместно применяются для решения различных видов прикладных задач, в том числе и для распознавания образов атак в информационных системах [9, 10]. В качестве глубоких нейронных сетей в разработанной САИБ применяются архитектуры свёрточных сетей. В свою очередь, иммунные системы также являются перспективным направлением в рамках решения задачи обнаружения вторжений в виду основных принципов иммунологии [11, 12]. В качестве ИИС используется гибридная искусственная иммунная система (ГИИС), представляющая слияние классического клонального типа ИИС и модифицированного генетического метода дуэлей (МГАД), также применяемого для настройки гиперпараметров систем САИБ.

Подход гибридизации архитектур данных методов для построения модулей САИБ был именован нейроиммунным подходом, являющимся основой исследования, обеспечившей повышение эффективности целевой системы анализа инцидентов [8].

Для описания методики обнаружения, анализа и корреляции инцидентов информационной безопасности, в том числе обусловленных применением систем биометрической аутентификации, в комплексной системе анализа распределённых инцидентов предлагается использовать следующие основные функциональные модули САИБ: сенсорный модуль и сеть сбора данных с узлов; модуль генерации и обучения детекторов; модуль сжатия и хранения данных; модуль анализа и корреляции; административный модуль управления [13, 14].

Общий алгоритм работы нейроиммунной системы анализа инцидентов ИБ распределённых систем следующий: для обучения нейроиммунных модулей формируется репрезентативная выборка инцидентов ИБ, которые предоставляются системе защиты для формирования базы антител-распознавателей угроз по выделенным признакам. Далее обученная нейроиммунная система вводится в узлах в режиме распознавания и при обнаружении инцидентов в анализируемой среде формирует уведомление об обнаруженной проблеме, лог события.

Новизна исследования заключается в предлагаемой методике анализа инцидентов безопасности распределённых систем на основе разработанного нейроиммунного подхода, реализованного и исследованного с использованием гибридизации структур интеллектуальных методов машинного обучения. В работе предпринята попытка использовать преимущества каждого из подходов для решения своей специализированной подзадачи. Предложенное решение способно обеспечить повышение надёжности, гибкости, комплексной эффективности современных систем анализа событий [7].

В рамках исследования подхода анализа уникальных событий биометрической идентификации и аутентификации личности получены 2 патента на изобретения: «Способ опознавания личности по радужной оболочке глаза» (RU 2672279 C1) и «Способ опознавания личности по рисунку вен ладони» (RU 2761776 C1).

Ожидаемыми по окончании проекта научными результатами являются: формирование методов построения надёжных и точных систем анализа событий информационной безопасности, повышение защищенности распределенных систем от различных видов угроз, включая сетевые атаки, вредоносное программное обеспечение, взлом учетных записей, атаки на системы аутентификации, в том числе биометрические.

Полученные теоретические и практические результаты будут использованы в лекционном, лабораторном и практическом курсах дисциплины «Технологии искусственного интеллекта в области

безопасности и защиты информации» для студентов специальностей 10.05.01 Компьютерная безопасность, 10.05.03 Информационная безопасность автоматизированных систем и магистров направления подготовки 10.04.01 Информационная безопасность кафедры компьютерных технологий и информационной безопасности КубГТУ. Программно-методические комплексы данных дисциплин разработаны для новых учебных планов ФГОС ВО 3++, введенных с 2021 г.

СПИСОК ЛИТЕРАТУРЫ

1. Andress, J. The basics of information security: understanding the fundamentals of InfoSec in theory and practice / J. Andress // Syngress. — 2014. — 190.
2. Kahraman, K. Anomaly Detection in Networks Using Machine Learning / K. Kahraman // School of Computer Science and Electronic Engineering University of Essex. — 2018. — 71.
3. Alfredo, C. An Analysis of Deep Neural Network Models for Practical Applications / C. Alfredo, P. Adam, C. Eugenio // ArXiv:1605.07678v4. — 2017. — 1-6.
4. Poltavtseva, M.A. Modeling big data management systems in information security / M.A. Poltavtseva, M.O. Kalinina //Automatic Control and Computer Sciences. — 2019. — №53(8). — 895-902.
5. Gernot, T. Biometric Masterkeys / T. Gernot, P. Lacharme // Comput. Secur. — 2022. —№116. — 102642.
6. Berdibayev, R. A concept of the architecture and creation for SIEM system in critical infrastructure / R. Berdibayev, S. Gnatyuk, Y. Yevchenko, V. Kishchenko // Systems, Decision and Control in Energy II. — 2021. — 221-242.
7. Сухов, В.Е. Система обнаружения аномалий сетевого трафика на основе искусственных иммунных систем и нейросетевых детекторов / В.Е. Сухов // Вестник рязанского государственного радиотехнического университета. — 2015. — №54(1). — 84-90.
8. Частикова, В.А. Методика построения системы анализа инцидентов информационной безопасности на основе нейроиммунного подхода / В.А. Частикова, А.И. Митюгов // Электронный сетевой политематический журнал "Научные труды КубГТУ". — 2022. — №1. — 98-105.
9. Alfredo, C. An Analysis of Deep Neural Network Models for Practical Applications / C. Alfredo, P. Adam, C. Eugenio // ArXiv:1605.07678v4. — 2017. — 1-6.
10. Матвеев, М.Г. Модели и методы искусственного интеллекта. Применение в экономике / М.Г. Матвеев, А.С. Свиридов // Издательский дом «ИНФРА-М». — 2014. — 316-324.
11. Васильев, В.И. Распределенная система обнаружения атак на основе механизмов иммунной системы / В.И. Васильев, Р.Р. Шамсутдинов // Информационные технологии интеллектуальной поддержки принятия решений (ITIDS 2018), Труды VI Всероссийской конференции (с приглашением зарубежных ученых). — 2018. — 237-244.
12. Gallais-Jimenez, M., Nguyen, H.A., Saied, M.A., Nguyen, T.N., & Sahraoui, H.A. (2020). API Misuse Detection An Immune System inspired Approach / M. Gallais-Jimenez, H.A. Nguyen, M.A. Saied, T.N. Nguyen, H.A. Sahraoui // ArXiv:abs/2012.14078. — 2012. — 2-4.
13. Miller, D. Security information and event management (SIEM) implementation / D. Miller // New York: McGraw-Hill. — 2011.

Штеренберг С.И.
Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»,
доцент, к.т.н.,
stas.shterenberg.89@mail.ru

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА МУЛЬТИАГЕНТНОГО ТИПА

Аннотация: Что актуально в современном мире, так это приобретение общего единого механизма, который мог бы подчинить себе основную автоматическую среду промышленности цивилизации, анализировать состояние в информационном пространстве и выдавать верные решения, которые бы оказали значительную помощь операторам и специалистам промышленности. Общая **идея** заключается в том, чтобы системы обнаружения вторжения оснастить надежным искусственным интеллектом (далее – ИИ), который будет сопровождать распределенную интеллектуальную систему (далее – РИС) и интеграцию в нее различных технологий интеллектуальных систем, от Больших данных до машинного обучения (далее – МО).

Ключевые слова: искусственный интеллект, Большие данные, машинное обучение, нейронные сети, программные агенты.

Введение. Необходимо также в определённой степени подчеркнуть, что технологическое отставание технологического комплекса Российской Федерации и IT-промышленности и создание отечественных систем защиты информации (далее – СЗИ) накладывает дополнительную актуальность к данной теме исследований и разработок. А именно, необходимо на имеющемся базисе отечественных РИС построить подходящую архитектуру СЗИ, которая была бы оснащена новыми ИИ, т.к. в условиях нарастающего мирового экономического кризиса, полноценный переход на Индустрию 4.0 и т.д. жизненно необходим [1]! Стремительное развитие человечества в эпоху так называемой «Индустрии 4.0» заставляет инженеров и программистов всего мира второпях принимать самые необычных решения для построения новых систем обнаружения вторжений (далее – СОВ).

Однако и сам ИИ нуждается в собственной самозащите от атак, например, нарушения целостности [4]. Для формирования систем ИИ задействуются такие концепции технического развития как искусственное сознание, интеллектуальная робототехника, машинное творчество, инженерия знаний, гибридные подходы синергийных комбинаций нейронных и символьных моделей, агентно-ориентированный подход [2]. Очевидно, что синтез всех этих технологий, лишь малая часть, которую предстоит пройти человечеству, чтобы сформировать полноценный интеллектуальный механизм, способный воистину мыслить, составлять и решать различного рода задачи и доводить их до логического завершения.

Разработка модели. На основании этого в работе формируется **цель** – разработка комплекса технологий для ИИ с обеспечением его «жизнеспособности» и киберустойчивости. Под «живучестью» ИИ будем понимать совокупность оценок к методологии построения самоорганизующихся карт программных агентов (далее - ПА, они же «нейроны») и воздействию атак, направленных на нарушение целостности. Под киберустойчивостью – способность ИИ обеспечивать дальнейшее функционирование в РИС и сопровождение СОВ [3]. Определим возможность РИС описывать состояния «жизнеспособности» следующей формулой:

$$[ABC] \approx \frac{(n-1)N}{n^2} \frac{[AB][AC][BC]}{[A][B][C]}, \quad (1)$$

где A, B и C – состояния входов, выходов и обработки данных для ИИ, а $\frac{(n-1)N}{n^2}$ - количество атак, совершенных на них как успешных, так и провальных. А киберустойчивость, определим в свою очередь как:

$$\frac{1}{n} \ln[N(\frac{1}{k_{вторж.нач}}) - 1], \quad (2)$$

где $k_{вторж.нач}$ – обнаружение искажений в начальный момент времени t_0 когда совершается атака на систему ИИ. Следует заметить в дальнейшем при проектировании концептуального, а затем и имитационного моделирования, что при построении будущих перцептронов ИИ, нейросетей и систем

с МО [5], будет принята событийная схема проведения на них компьютерных атак. Здесь в силу будет вступать новая симуляционая **модель** сбора и обработки Больших данных [10], которая основана на использовании входных данных о РИС и ее уязвимостях, зависимостях сервисов (см. рис 1).

Рис. 1. Концептуальная модель обработки Больших данных, которая основана на использовании входных данных о распределенной информационной системе и ее уязвимостях, зависимостях сервисов

В модели, где уже имеются предметы контроля «жизнеспособности» и кибербесопасности, основными достоинством будет являться установление коэффициента достижения порога насыщения, позволяющий контролировать распространения ПА по системе с обработкой механизмов Больших данных [6,7]. Обработка Больших данных в дальнейшем будет влиять на приобретение ассоциативной память у ИИ, а также обеспечивать синхронизацию компонентов мультиагентной нейронной системы [8], имеющая в основе квазибиологическую парадигму, которая позволяет определить условия сохранности ИИ от деструктивных действий [9].

Используя в своем обороте так называемую квазибиологическую парадигму решено, на начальных этапах формирования мультиагентной системы для нового ИИ составить схему их взаимодействия. Поскольку все ПА системы новые и проходят на данный момент этап первичного внедрения в перцептрон, то также принято решении о самоназвании каждого из ПА и символьного представления в схеме для придания аутентичности разрабатываемого программного обеспечения (далее - ПО) (см. рис 2).

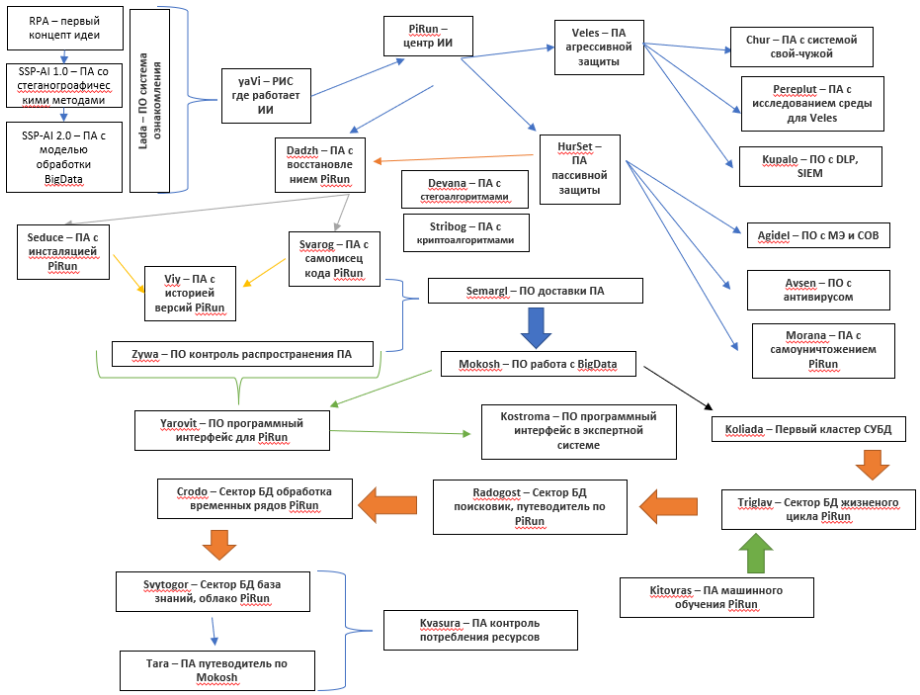


Рис. 2. Концептуальная схема взаимосвязи ПА с кратким описанием компоненов всей системы ИИ

Соответственно по рис. 2 выполнена табл. 1 с кратким названием и описанием всех компонентов новой интеллектуальной системы. Каждый модуль – эта программа и/или ПО («нейрон») со встроенными функциями СЗИ, которые связаны единым процессом перцептрона, носящего название PiRun. Благодаря данному концепту, в дальнейшем будет выстраиваться и методология и защита ПО во всей РИС (которое в свою очередь носит название yaVi). **Суть** этой концептуальной модели обеспечить зарождающийся ИИ математической методологией, обработкой Больших данных

для накопления ассоциативной памяти, проводить ассимиляцию дополнительных СЗИ и компонентов перцептрона, а также развивать и улучшать строящийся ИИ.

Табл. 1. Описание компонентов концептуальной модели обеспечения защиты системы искусственного интеллекта мультиагентного типа

Название компонента	**Тип ПО**	**Функции ПО**
Veles	ПА	ПА для ведения активных защитных функции перцептрона PiRun
PiRun	ПА	Головной модуль принятия решений перцептрона
HurSet	ПА	ПА для ведения функций пассивной защиты перцептрона PiRun
Chur	ПА	ПА с определением системы свой-чужой
Pereplut	ПА	ПА в функция исследования среды для внедрения нейрона Veles
Kupalo	ПО	ПО для интеграции DLP- и SIEM-систем в комплекс yaVi
Agidel	ПО	ПО для интеграции СОВ и межсетевого экранирования в комплекс yaVi
Avsen	ПО	ПО для интеграции антивирусных систем в комплекс yaVi
Morana	ПА	ПА, отвечающий за оперативной самоуничтожение перцептрона PiRun
Dadzh	ПА	ПА, отвечающий за восстановление работоспособности PiRun
Devana	ПА	ПА с встроенными библиотечными данными для проведения стеганографических операций [12] перцептрона PiRun
Stribog	ПА	ПА с встроенными библиотечными данными для проведения криптографических операций [11] перцептрона PiRun
Seduce	ПА	Отвечающий за самоинсталяцию компонентов перцептрона PiRun
Svarog	ПА	ПА-самописец кода компонентов перцептрона PiRun
Viy	ПА	Модуль память версий перцептрона PiRun
Zywa	ПА	ПА для контроля распространения компонентов перцептрона PiRun
Semargl	ПА	ПА контроля доставки компонентов перцептрона PiRun в РИС
Mokosh	СУБД	Система управления базой данных и базой знаний для ресурсов комплекса yaVi
Koliada	БД	Первый резервный программный кластер СУБД Mokosh
Yarovit	Интерфейсная оболочка	ПО с интерфейсной оболочной для контроля функций перцептрона PiRun
Kostroma	Интерфейсная оболочка	ПО с интерфейсной оболочкой для развития экспертной системы управления комплексом yaVi
Triglav	БД	Сектор информации о жизненном цикле ИИ
Radogost	БД	Сектор БД поисковик, путеводитель по комплексу yaVi
Crodo	БД	Сектор БД, в котором идет обработка временных рядов для перцептрона PiRun
Kitovras	ПО	Комплекс, отвечающий за машинное обучение перцептрона PiRun
Svytogor	БД	Облачное хранение систем Mokosh и PiRun
Tara	ПО	Справочная система по Mokosh
Kvasura	ПА	ПА контроля потребления ресурсов комплексом yaVi

Заключение. В ходе построения и написания данной концептуальной модели, в дальнейшем выполняются следующие научные задачи:

1. Проводится модификация методики построения самоорганизующейся карты программных агентов (нейронов) для СОВ.
2. Проектируется ассимиляционная модель обработки Больших данных в РИС с использованием перцептрона, которая в отличие от существующих решений применяет ассоциативную память ИИ.
3. Строится новая архитектура системы ИИ в едином программном комплексе с синхронизацией компонентов мультиагентной нейронной системы, имеющая в основе квазибиологическую парадигму.
4. Разрабатывается новая методика обеспечения «жизнеспособности» ПА в РИС, в которой сформулирован новый принцип киберустойчивости архитектуры системы ИИ, обеспечивающий «переключение» на децентрализацию самоорганизующейся карты ПА.

Подобный ИИ приобретет инструмент, который обеспечит защитным функционалом его самого, выстроенные концепты компонентов предложенного перцептрона будут импульсом для развития СЗИ. *Данное исследование выполнено при финансовой поддержке Минцифры России (грант ИБ) в рамках научного проекта, Соглашение №. 40469-05/2022-д от 30.06.2022 г.*

СПИСОК ЛИТЕРАТУРЫ

5. Петренко С.А., Киберустойчивость Индустрии 4.0: научная монография / СПб. «Издательский дом «Афина», 2020. 226 с.
6. Хапке Х., Нельсон К., Разработка конвейеров машинного обучения. Автоматизация жизненных циклов модели с помощью TensorFlow / пер. с анг. Н. Б. Желновой. – М.: ДМК Пресс, 2021. – 346 с.: ил.
7. Штеренберг С.И., Обнаружение вторжений в распределенных информационных системах на основе методов скрытого мониторинга и анализа больших данных: диссертация на соис. уч. степ.кандидата технических наук: 05.13.19 /г. СПб, 2018 г.
8. Бостром Ник, Искусственный интеллект. Этапы. Угрозы. Стратегии / Ник Бостром ; пер.с англ. С. Филина. —М.: Манн, Иванов и Фербер, 2016. —496 с.
9. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. — СПб.: Питер, 2018. — 480 с.: ил. — (Серия «Библиотека программиста»).
10. Ушаков И.А., Обнаружение инсайдеров в корпоративной компьютерной сетина основе технологий анализа больших данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2019. № 4. С. 38-43.
11. Котенко И.В., Ушаков И.А., Технологии больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд. 2017. № 3 (75). С. 23-33.
12. Степанов М.Д., Павленко Е.Ю., Лаврова Д.С., Обнаружение сетевых атак в программно-конфигурируемых сетях с использованием алгоритма изолирующего леса // Проблемы информационной безопасности. Компьютерные системы. 2021. № 1. С. 62-78.
13. Васильева К.В., Лаврова Д.С., Обнаружение аномалий в киберфизических системах с использованием графовых нейронных сетей // Проблемы информационной безопасности. Компьютерные системы. 2021. № 1. С. 117-130.
14. Полтавцева М.А., Управление данными при мониторинге информационной безопасности КФС // Защита информации. Инсайд. 2022. № 2 (104). С. 10-15.
15. Korzhik V.I., Starostin V.S., Kabardov M.M., Gerasimovich A.M., Yakovlev V.A., Zhuvikin A.G., Information theoretically secure key sharing protocol executing with constant noiseless public channels // Математические вопросы криптографии. 2021. Т. 12. № 3. С. 125-141.
16. Коржик В.И., Нгуен З.К., Ахрамеева К.А., Модификация шифров для защиты от атаки обнаружения стегосистем, использующей NIST-тесты // Проблемы информационной безопасности. Компьютерные системы. 2020. № 1. С. 33-43.

РАЗДЕЛ 3. НАУЧНЫЕ ДОКЛАДЫ ГРАНТОПОЛУЧАТЕЛЕЙ 2021 ГОДА – СОИСКАТЕЛЕЙ УЧЁНОЙ СТЕПЕНИ КАНДИДАТА НАУК

Асяев Г.Д.
Аспирант ЮУрГУ,
asyaev1996@mail.ru

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ НА ОСНОВЕ ГИБРИДНЫХ МЕТОДОВ ПРЕДИКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация: В статье представлен подход, позволяющий увеличить обучающую выборку и уменьшить несбалансированность классов для решения задач классификации трафика. Рассмотрены основные принципы и архитектура генеративно состязательных сетей. Описана математическая модель классификации сетевого трафика. Проанализирована обучающая выборка, взятая для решения поставленной задачи. Проведен и обоснован пропроцессинг данных. Построена архитектура генеративно-состязательной сети и разработан алгоритм генерации новых признаков. Рассмотрены и построены модели машинного обучения в рамках задачи классификации траффика: Logistic regression, K Nearest Neighbors, Decision tree, Random forest. Проведен сравнительный анализ результатов моделей машинного обучения без применения и с генерации новых признаков. Полученные результаты могут применяться как в задачах классификации сетевого траффика, так и в общих случая многоклассовой классификации и исключения несбалансированности признаков.

Ключевые слова: информационная безопасность, машинное обучение, генеративные сети, несбалансированная выборка.

Кибербезопасность - постоянно развивающаяся область исследований, в которой часто меняются подходы и парадигмы. Сообщество кибербезопасности признает тот факт, что киберугрозы не могут быть полностью устранены, поэтому исследования и разработки направлены на предотвращение и снижение последствий инцидентов безопасности. Однако большинство существующих подходов, по сути, являются реактивными. Темы обнаружения вторжений и реагирования на инциденты интенсивно изучались в последние годы и дали хорошие результаты. Тем не менее, они реагируют только на события, которые уже произошли [1]. Существует тенденция перехода к более проактивным подходам [2], которые позволят предотвратить или смягчить последствия инцидентов безопасности до того, как они принесут вред. Путь к этому прокладывают разведка киберугроз, киберситуационная осведомленность, сотрудничество и обмен информацией и другие перспективные направления исследований и разработок.

Методы прогностической аналитики - перспективное направление исследований в области кибербезопасности, которое позволит применять более проактивный подход к операциям безопасности [3]. Предсказания могут служить в качестве раннего предупреждения, чтобы администраторы информационной безопасности могли заранее узнать об угрозах, разработать надлежащие контрмеры и упреждающе уменьшить негативные последствия или полностью предотвратить инциденты безопасности [3]. Ситуация с безопасностью всей сети, например, увеличение или уменьшение количества атак, может быть спрогнозирована [3], конкретные инциденты могут быть предсказаны различными способами [3], и даже когда происходит атака, можно предсказать следующие действия злоумышленника [4]. Тем не менее, из-за сложности постоянно меняющейся киберсреды, все еще существует множество проблем, требующих решения, многие из которых глубоко укоренились в основах данного направления исследований. Сложно определить, что именно предсказывается и как использовать предсказания. Прогнозирование на ретроспективных данных является распространенным подходом, который, однако, не отражает новые формы атак и эксплойтов "нулевого дня", появляющихся ежедневно. Прогнозирование увеличения или уменьшения количества атак, как правило, мало что говорит об исполнителях этих атак; прогнозирование следующего хода злоумышленника мало что говорит о ландшафте угроз. Таким образом, важно найти общую методологию, на которой можно сравнивать и анализировать различные подходы и методы, чтобы узнать о сильных и слабых сторонах каждого подхода. Существуют различия в экспериментальных работах и исследованиях из-за многочисленных проблем в операционной среде, таких как

недостаточные или ошибочные данные на входе, что приводит к значительному снижению точности прогнозирования.

Существует достаточное число систем обнаружения вторжений, однако потребность в создании комплексной системы поддержки принятия решения на реагирование компьютерных инцидентов по-прежнему остается актуальной. В настоящий момент нет такой системы, которая бы позволяла последовательно и достаточно быстро решать ряд следующих задач:

- Обнаружение злоупотреблений данных в информационной системе.
- Многоклассовая классификация атак
- Формирование «кандидатов» из множества стратегий защиты информационной безопасности
- Ранжирование стратегий, основываясь на скорости и полноте предотвращения наступившей атаки.
- Логирование и самообучение.

В настоящее время существует множество моделей для решения задач классификации траффика [5]. Это могут быть как обычные модели машинного обучения (random forest, catboost, lightGBM), кластерные модели, так и использование моделей глубокого обучения - нейронные сети. Однако большинство задач в области классификации сетевого трафика обучаются на размеченных данных [6]. Стоит отметить, что для того, чтобы получить хороший, разнообразный объемный набор данных требуется достаточно времени и ресурсов, что в большинстве случаев является достаточно проблематичным [7]. Основной идеей данного исследования является применение генеративно-состязательных сетей для генерации обучающей выборки. Это позволит значительно сократить время для получения данных, его разметки и предобработки, а также повысит метрику качества при достаточно выраженной несбалансированной выборке.

1.2. Генеративное моделирование

Пусть имеется некоторое конечное количество признаков X и целевых переменных Y в обучающем наборе данных. Пусть z имеет некоторые распределение (1.1):

$$z \sim N(0,1) \tag{1.1}$$

Тогда в обобщенном случае существует такая функция (1.2):

$$f: Z \to X, \text{ что } f(z) \sim P(X). \tag{1.2}$$

Не зная P(X) в явном виде модель получает некоторые общие базисы неявно. Так можно восстановить f(z), по чего записи P(X) могут быть получены как (1.3):

$$f(z), z \sim N(0,1) \tag{1.3}$$

Данное обстоятельство и послужило развитию генеративного моделирования, которое представляет собой метод обучения без учителя, где происходит автоматизированное обнаружение различных закономерностей и зависимостей, признаки которого можно использовать для генерации новых данных [8]. При этом считается, что новые признаки будут максимально схожи по своему распределению с имеющимся набором данных.

Ключевой особенности генеративно-состязательных сетей (GAN) заключается в формировании критерия качества в виде отдельной нейронной сети [9].

1.3. Генеративное-состязательная сеть

Именно с развитием генеративного моделирования появились генеративно-состязательные сети (рис. 1), которые состоят из двух нейронных сетей:

- Генератор. Данная нейронная сеть необходима для обучения генерации новых признаков X. При этом генератор должен таким образом формировать признаки, чтобы дискриминатор не смог классифицировать его как поддельный признак [9]. Дискриминатор представляет собой некий критерий качества работы генератора.

- Дискриминатор. Основной задачей которого является определить реальные признаки X, от поддельных X˜. То есть, когда на вход модели дискриминатора будет подаваться истинный признак, у него на выходе будет некоторое число (в диапазоне от 0 до 1) с пометкой real, а когда на вход модели будет подаваться сгенерированный признак, то на выходе, соответственно, будет некое число с меткой «fake» [10]. Данные числовые значения можно трактовать как степень уверенности дискриминатора в том, что входной признак относится либо к реальному классу, либо сгенерированному (Рис. 2). Так, например, когда вход будет подаваться реальный признак, то на выходе дискриминатора класс «real» должен стремиться к 1.

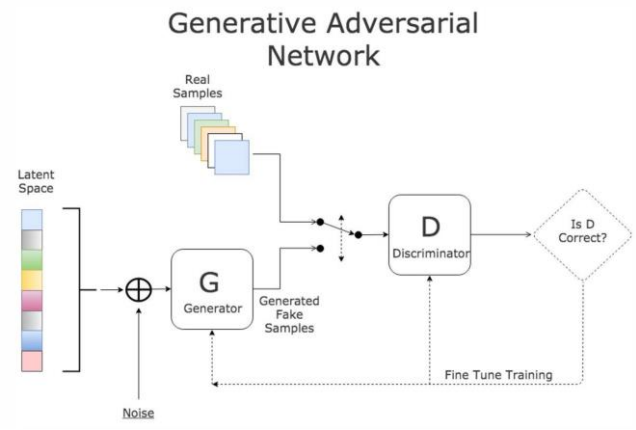


Рис. 1. Общая архитектура GAN

Так как дискриминатор представляет собой бинарный классификатор (признак либо реальный, либо сгенерированный), то в качестве функции потерь рационально использовать бинарную кросс-энтропию (1.4) [11]:

$$\begin{cases} loss_{dis_{real}} = -t_R * \log(real) - (1 - t_R) * \log(1 - real) \\ loss_{dis_{fake}} = -t_F * \log(fake) - (1 - t_F) * \log(1 - fake) \end{cases} \quad (1.4)$$

где $loss_{dis_{real}}$ – потери при реальном признаке, где t_R=1, а $loss_{dis_{real}}$ – потери при сгенерированном признаке, где t_F=0.

Подставив данные значения, можно записать обобщенную функцию потерь [11] для рассматриваемого случая (1.5):

$$loss_{dis} = -\log(real) - \log(1 - fake) \quad (1.5)$$

Таким образом показатель качества должен быть минимален для реальных признаков и максимален для сгенерированных [11].

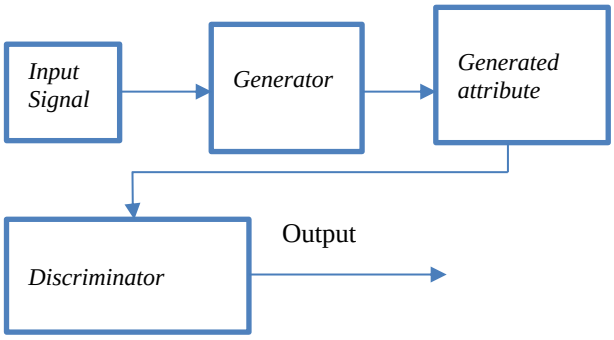


Рис. 2. Режим обучения генератора

Функцию потерь для генератора можно описать как (1.6):

$$loss_{dis} = -\log(fake) \quad (1.6)$$

Тем самым генератор и дискриминатор обучаются независимо друг от друга.

Для построения модели был взят датасет с сайта kaggle «UNSW_NB15 by the ixia perfectstorm tool. Australian centre for cyber security (ACCS)». Необработанные сетевые пакеты из набора данных UNSW-NB 15 были созданы с помощью инструмента IXIA Perfectstorm в лаборатории Cyber Range Lab австралийского центра кибербезопасности (ACCS) для создания гибрида реальной современной

нормальной деятельности и синтетического современного поведения атаки. Размер обучающей выборки составляет 82332 записей (Рис. 3).

	id	dur	proto	service	state	spkts	dpkts	sbytes	dbytes	rate	...	ct_dst_sport_ltm	ct_dst_src_ltm	is_ftp_login
0	1	0.000011	udp	-	INT	2	0	496	0	90909.090200	...	1	2	0
1	2	0.000008	udp	-	INT	2	0	1762	0	125000.000300	...	1	2	0
2	3	0.000005	udp	-	INT	2	0	1068	0	200000.005100	...	1	3	0
3	4	0.000006	udp	-	INT	2	0	900	0	166666.660800	...	1	3	0
4	5	0.000010	udp	-	INT	2	0	2126	0	100000.002500	...	1	3	0
5	6	0.000003	udp	-	INT	2	0	784	0	333333.321500	...	1	2	0

Рис. 3. Набор признаков обучающей выборки

В обучающем наборе данных представлено 44 признака и 1 целевая переменная attack_cat. Она принимает следующие значения (Рис. 4):

- 'Normal',
- 'Reconnaissance',
- 'Backdoor',
- 'DoS',
- 'Exploits',
- 'Analysis',
- 'Fuzzers',
- 'Worms',
- 'Shellcode',
- 'Generic'

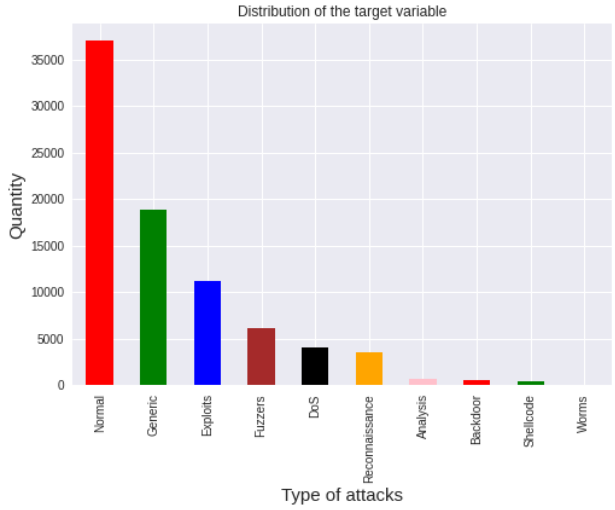


Рис. 4. Распределение целевой переменной

Исходя из распределения целевой переменной, выборка достаточно несбалансированная. Атаки типа 'Analysis', 'Fuzzers', 'Worms', 'Shellcode', 'Generic' имеют меньше 700 записей. Именно для этих типов атак целесообразно применить генеративно состязательную сеть для генерации новых записей, чтобы исключить дисбаланс классов.

Стоит отметить, что записи, где количество пропущенных значений превышало 40 % были заменены медианными значениями. Так как в обучающем наборе присутствовали категориальные признаки (Табл. 1), и очевидно, что они несут в себе полезную информацию, то они были переведены в числовые с помощью метода One Hot Encoding. Выбор метода был обусловлен тем, что он не придает при обучении модели вес к какому-либо признаку:

Табл. 1 Пример категориальных признаков

service	**http**	**ftp**	**ftp-data**	**dns**	**snmp**	**ssl**	**dhcp**	**…**	**irc**
state	INT	FIN	REQ	ACC	CON	RST	CLO	…	no

Данные были отнормализованы с помощью StadartScaler, а также исключен уникальный номер каждой строки вследствие неинформативности.

Данные были разделены на тестовую и обучающую выборку в соотношении 70/30. Стоит отметить, что каждый класс целевой переменной попал в обучающую выборку.

Для обучения были выбраны следующие модели:

- Logistic Regression
- K-nearest Neighbors
- Decision tree
- Random Forest (with gini criterion)
- Random Forest (with entropy criterion).

1.4. Logistic Regression

Первой моделью для обучения была выбрана простая логистическая регрессия с целью определить насколько хорошо данные были предобработаны и очищены, а также посмотреть на таблицу ранжированности важности признаков. Коэффициент регуляризации составил 0.1, количество эпох было выбрано 40, значение кросс валидации составило 10. Стоит отметить, что даже без точной настройки простая модель показала точность порядка 90% (Рис. 5). А значение average precision-recall score составило 82%.

```
Accuracy: 90.74
Accuracy of CV: 86.94
Execution time: 15.5252412412562
```

Рис. 5. Показатели качества модели

Была построена таблица степени важности признаков. На рисунке 6 представлены топ 5 признаков.

	Feature	Importance
7	dttl	7.0
181	service_smtp	3.0
190	state_INT	3.0
159	proto_unas	2.0
24	dmean	2.0

Рис. 6. Градация степени важности признаков

1.5. K-nearest neighbors

Данный метод относится к методу обучения без учителя. Количество ближайших соседей было равно 3. Стоит отметить, что качество модели на кросс-валидации составило порядка 67%, что чуть лучше чем наивный байесовский классификатор (Рис. 7).

```
Accuracy: 76.74
Accuracy of CV: 66.94
Execution time: 35.958560943603516
```

Рис. 7. Показатели качества модели

1.6. Decision tree

Основная цель данного алгоритма состоит в том, чтобы создать модель, которая предсказывает значение целевой переменной, изучая простые правила принятия решений, выводимые из функций данных. Дерево можно рассматривать как кусочно-постоянное приближение.

На рис. 8 Представлен участок построенного дерева решений. Наглядно видно, что построенная модель имеет небольшое количество листьев.

Рис. 8. Участок построенного дерева решений

1.7. Random Forest

Random Forest представляет ансамбль классификаторов дерева решений для различных подвыборок набора данных и использует усреднение для повышения точности прогнозирования и контроля над подгонкой. На рисунке ниже (Рис. 9) представлена сравнительная таблица результатов работы модели random forest при разных параметрах finetuning и препроцессинге данных.

PreProcessing	Parameters	Train Acc	Test Acc
OneHot encoding, StandardScaler	n_estimators 10, max_depth 10, max_features 10, class_weight {0:2, 1: 1}	94.10	91.05
	n_estimators 10, max_depth 10, max_features 20, class_weight {0:2, 1: 1}	94.16	91.61
	n_estimators 10, max_depth 20, max_features 20, class_weight {0:2, 1: 1}	95.64	89.16
	n_estimators 30, max_depth 10, max_features 30, class_weight {0:2, 1: 1}	94.19	91.66
	n_estimators 10	95.66	87.90
	n_estimators 10, max_depth 20	95.73	86.91
	n_estimators 10, max_features 20	95.76	87.57
	n_estimators 50	96.06	87.31
OneHot encoding, MinMaxScaler	n_estimators 10, max_depth 10, max_features 30, class_weight {0:2, 1: 1}	93.98	91.49
	n_estimators 10, max_depth 10, max_features 10, class_weight {0:2, 1: 1}	94.20	91.32
OneHot encoding, RobustScaler	n_estimators 10, max_depth 10, max_features 30, class_weight {0:2, 1: 1}	94.08	91.90
	n_estimators 50, max_depth 10, max_features 30, class_weight {0:2, 1: 1}	94.21	91.68
	n_estimators 20, max_depth 10, max_features 10, class_weight {0:2, 1: 1}	94.21	91.36
OneHot encoding	n_estimators 10, max_depth 10, max_features 10, class_weight {0:2, 1: 1}	94.20	91.02

Рис. 9. Сравнительная таблица параметров модели и ее качества

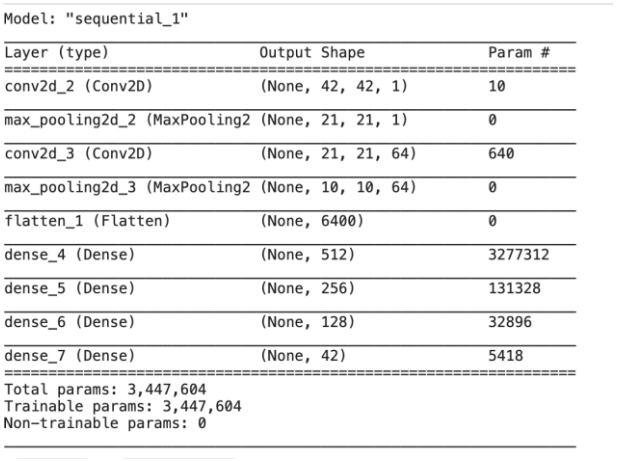
Отдельно стоит отметить, что ни одна модель не превысила значение точности в 95%.

Для того, чтобы увеличить такие критерии качества как precion, recall, accuracy было решено использовать генеративно состязательную сеть для таких целевых переменных как 'Analysis', 'Fuzzers', 'Worms', 'Shellcode', 'Generic'. Выбор переменных был обусловлен малым количеством записей в обучающей выборке.

Ниже представлен алгоритм работы формирования сгенерированных записей:

1. Поочередно формировалась выборка по одной из целевой переменной.
2. Данные записи подавались на вход convolutional neural networks без дополнительной группировки по батчам (вектор размерности один).
3. На выходе нейронной сети формировалась сгенерированная последовательность.
4. С помощью модуля random выбиралась либо реальная последовательность признаков из датасета, либо сгенерированная последовательность от генератор (CNN)
5. На вход дискриминатора подавался набор признаков, выбранный на шаге 4.
6. На выходе дискриминатора формировалась метка «real» / «fake» для последовательности.
7. п. 1 – 6 повторялся до тех пор, пока дискриминатор не стал путать реальный и сгенерированный набор признаков с вероятностью 75%.

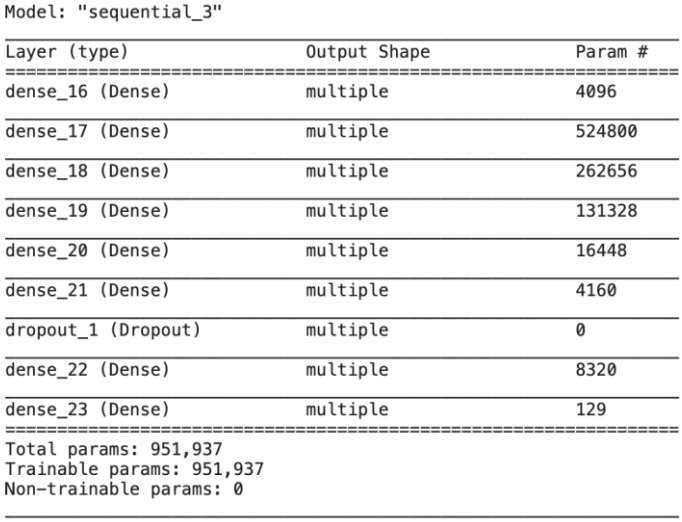
В качестве генератора использовалась convolutional neural networks (CNN). Ее архитектура представлена на рисунке 10.



```
Model: "sequential_1"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
conv2d_2 (Conv2D)            (None, 42, 42, 1)         10
_________________________________________________________________
max_pooling2d_2 (MaxPooling2 (None, 21, 21, 1)         0
_________________________________________________________________
conv2d_3 (Conv2D)            (None, 21, 21, 64)        640
_________________________________________________________________
max_pooling2d_3 (MaxPooling2 (None, 10, 10, 64)        0
_________________________________________________________________
flatten_1 (Flatten)          (None, 6400)              0
_________________________________________________________________
dense_4 (Dense)              (None, 512)               3277312
_________________________________________________________________
dense_5 (Dense)              (None, 256)               131328
_________________________________________________________________
dense_6 (Dense)              (None, 128)               32896
_________________________________________________________________
dense_7 (Dense)              (None, 42)                5418
=================================================================
Total params: 3,447,604
Trainable params: 3,447,604
Non-trainable params: 0
_________________________________________________________________
```

Рис. 10. Архитектура генератора

Полносвязная нейронная сеть выступала в роли дискриминатора. Она состоит из 8 dense слоев, lasso регуляризации (0.3) для уменьшения вероятности переобучения и выходом размерности 1 (метка real/fake) (Рис. 11).



```
Model: "sequential_3"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
dense_16 (Dense)             multiple                  4096
_________________________________________________________________
dense_17 (Dense)             multiple                  524800
_________________________________________________________________
dense_18 (Dense)             multiple                  262656
_________________________________________________________________
dense_19 (Dense)             multiple                  131328
_________________________________________________________________
dense_20 (Dense)             multiple                  16448
_________________________________________________________________
dense_21 (Dense)             multiple                  4160
_________________________________________________________________
dropout_1 (Dropout)          multiple                  0
_________________________________________________________________
dense_22 (Dense)             multiple                  8320
_________________________________________________________________
dense_23 (Dense)             multiple                  129
=================================================================
Total params: 951,937
Trainable params: 951,937
Non-trainable params: 0
_________________________________________________________________
```

Рис. 11. Архитектура дискриминатора

Сгенерированные записи были добавлены в датасет и рассмотренные модели были обучены заново.

В таблице 2 ниже представлена сравнительная характеристика моделей без применения препроцессинга данных и с применением искусственного сгенерированных признаков для лейблов, у которых число записей менее 700 с помощью GAN.

Таблица 2. Сравнительная таблица моделей

	ACC	**ACC with GAN**	**Precision**	**Precision with GAN**	**Recall**	**Recall with GAN**
Logistic Regression	90.74	93.3	86.4	89.4	80.4	90.1
K Nearest Neighbours	76.74	82.2	70.1	77.3	65.2	80.1
Decision Tree	93.74	97.7	88.6	92.1	83.1	95.3
Random Forest	95.74	99.21	90.2	98.8	88.4	99.1

Наглядно видно, что лучшей моделью оказалась Random Forest, а использование GAN для уменьшения несбалансированности классов позволило определять типы атак со значением метрики качества precision составила 99%. Кроме того, у всех моделей полнота правильных ответов

увеличилась, что доказывает применимость методов генерации искусственных признаков на практике в задаче классификации трафика.

СПИСОК ЛИТЕРАТУРЫ

1. Гарбук С.В., Правиков Д.И., Полянский А.В., Самарин И.В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты // Вопросы кибербезопасности. - 2019. - №3(31). С. 30-36.
2. Боровков А.И. «Умные» цифровые двойники – основа новой парадигмы цифрового проектирования и моделирования глобально конкурентоспособной продукции нового поколения. Трамплин к успеху// Журнал АО «ОДК». - 2018. - № 13. С. 12-18.
3. Правиков Д.И. Об одном подходе к обеспечению информационной безопасности автоматизированных систем // Вопросы защиты информации. - 2007. - № 3. С. 17-19.
4. Гарбук С.В., Бурцев А.Г. Методические основы исследования уязвимостей компонентов АСУ ТП // Защита информации. Inside. - 2012. - № 3. С. 34-38.
5. Гарбук С.В. Перспективы применения интеллектуальных технологий для решения задач безопасности // Национальная безопасность / 2016. - № 4. С. 451-457.
6. H. Chen and L. Jiang, “Efficient GAN-based method for cyber-intrusion detection,” ArXiv, 2019
7. D. P. A. R. Vinchurkar, “A Review of Intrusion Detection System Using Neural Network and Machine Learning Technique,” International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012
8. S. R. Chhetri, A. B. Lopez, J. Wan, and M. A. Al Faruque, “GAN-Sec: Generative Adversarial Network Modeling for the Security Analysis of Cyber-Physical Production Systems,” in Proceedings of the 2019 Design, Automation and Test in Europe Conference and Exhibition, DATE 2019.Institute of Electrical and Electronics Engineers Inc., may 2019, pp. 770–775.
9. Luzhnov V.S Simulation of Protected Industrial Control Systems Based on Reference Security Model using Weighted Oriented Graphs / V.S. Luzhnov, A.N. Sokolov, A.E. Barinov //Proceedings - 2019 International Russian Automation Conference, RusAutoCon 2019. – 2019
10. Sokolov A.N. Applying Methods of Machine Learning in the Task of Intrusion Detection Based on the Analysis of Industrial Process State and ICS Networking / A.N. Sokolov, I.A. Pyatnitsky, S.K. Alabugin //FME Transactions. – 2019. –Vol. 47 No. 4. – P.782-789
11. Соколов А.Н. Применение методов одноклассовой классификации для обнаружения вторжений / А.Н. Соколов, С.К. Алабугин, И.А. Пятницкий //Вестник УрФО. Безопасность в информационной сфере. – 2018. –Том - No 2(28). – С.43-48

Белова Е.И.
Вологодский техникум железнодорожного транспорта – филиал федерального государственного бюджетного образовательного учреждения высшего образования «Петербургский государственный университет путей сообщения Императора Александра I», преподаватель,
elenabelovavm@yandex.ru

ОЦЕНИВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ПАССАЖИРСКИМИ ПЕРЕВОЗКАМИ

Аннотация: В докладе рассмотрен подход к решению научной задачи повышения уровня безопасности АСУ пассажирскими перевозками (АСУ ПП) на основе разработки моделей и методик оценивания информационной безопасности АСУ пассажирскими перевозками (АСУ ПП), как объекта КИИ ЖТ при возможной нечёткости в имеющихся данных.

Ключевые слова: Информационная безопасность, критическая информационная инфраструктура, компьютерные атаки, критические процессы, значимые объекты, функциональные задачи, параметры критической информационной инфраструктуры.

Актуальность темы исследования:

Новые цифровые технологии нашли свое применение практически во всех функциональных областях железнодорожной отрасли и направлены на повышение эффективности деятельности железнодорожной транспортной системы. В тоже время повышается чувствительность производственных процессов, комплексов и системы железнодорожного транспорта (ЖТ) к деструктивным воздействиям, в том числе компьютерным атакам, что свидетельствует об актуальности создания и постоянного совершенствования системы информационной безопасности (ИБ) информационной инфраструктуры железнодорожного транспорта [1].

В настоящее время со стороны регуляторов в области информационной безопасности ФСТЭК России, ФСБ России, Минцифры России осуществляется переход от оценок таких свойств информации, как конфиденциальность, целостность и доступность к ущербам от нарушений информационной безопасности бизнес-процессов организаций. В соответствии с Федеральным законом от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Постановлением Правительства Российской Федерации от 08.02.2018 №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», Положениями ОАО «РЖД» и другими нормативными правовыми документами в области обеспечения комплексной безопасности и управлении рисками и инцидентами информационной безопасности проводить оценку информационной безопасности АСУ ПП, как объекта КИИ ЖТ необходимо на уровне бизнес-процессов.

Это требует разработки соответствующего методического аппарата оценки информационной безопасности АСУ (АСУ ПП).

Степень разработанности темы исследования:

Значительный вклад в формирование теоретической и методологической основы исследований по информационной безопасности, в том числе и железнодорожного транспорта, внесли отечественные учёные: Аверкин А.Н., Ададуров С.Е., Ажмухамедов И.М., Берштейн Л.С., Борисов Л.Ю., Васильев В.И., Герасименко В.А., Глухов А.П., Зегжда П.Д., Катасёв А.С., Корниенко А.А., Котенко И.В., Кравец А.Г., Нырков А.П., Саенко И.Б., Шелупанов А.А., Юсупов Р.М. и другие; а также зарубежные учёные - Авен Т., Найт Ф., Саати Т.Л., Скотт Д., Заде Л.А., Мамдами Э., Сугено М., Абрахам А., Ценг Г. и другие.

В результате решены многие вопросы, связанные с созданием систем защиты информации на ЖТ. Однако решение проблемы, связанной с оценкой влияния компьютерных атак на бизнес-процессы организаций, в том числе ОАО «РЖД», в настоящее время находится в начальной стадии и требует дальнейшей активной разработки.

Объект исследования:

АСУ ПП как объект критической информационной инфраструктуры железнодорожного транспорта.

Предмет исследования:

Модели и методики оценивания информационной безопасности АСУ ПП.

Цель и задачи исследования:

Основной целью исследования является повышение уровня информационной безопасности АСУ пассажирских перевозок (АСУ ПП) на основе разработки моделей и методик оценивания информационной безопасности АСУ ПП КИИ ЖТ. В диссертационной работе поставлены и решены следующие задачи:

1. Анализ научной задачи оценки эффективности и управления информационной безопасностью АСУ пассажирскими перевозками КИИ ЖТ.
2. Анализ целевого бизнес–процесса АСУ ПП и разработка иерархической модели (бизнес–процессы, функциональные задачи, модули АСУ ПП и показатели качества функционирования модулей АСУ ПП в условиях компьютерных атак).
3. Анализ показателей результативности управления безопасностью АСУ ПП.
4. Разработка методики определения значимости критических процессов пассажирских перевозок, функциональных задач, модулей АСУ ПП и показателей функционирования модулей АСУ ПП.
5. Подход к формированию экспертных групп.
6. Разработка модели и методики определения границ областей безопасности для критических процессов пассажирских перевозок, функциональных задач, модулей АСУ ПП и показателей функционирования АСУ ПП.
7. Разработка методики ситуационного управления в нечёткой среде.

Методы исследования:

Для решения поставленных задач были использованы методы системного анализа, метод анализа иерархий, теории нечётких множеств и нечёткой логики, теории защиты информации.

Положения, выносимые на защиту:

1. Иерархическая модель, описывающей различные виды активов АСУ ПП (бизнес-процессы, функциональные задачи, модули АСУ ПП и показатели качества функционирования модулей АСУ ПП) и особенности их взаимодействия.
2. Методика определения значимости критических процессов пассажирских перевозок, функциональных задач, модулей АСУ ПП и показателей качества функционирования модулей АСУ ПП.
3. Показатели информационной безопасности, модель и методика определения границ областей безопасности для критических процессов пассажирских перевозок, функциональных задач, модулей АСУ ПП и показателей качества функционирования модулей АСУ ПП в условиях компьютерных атак.
4. Методика ситуационного управления информационной безопасностью АСУ ПП в нечёткой среде на основе полученных оценок информационной безопасности.

Научная новизна исследования:

Впервые, применительно к АСУ ПП, как объекту КИИ ЖТ, разработано методическое обеспечение, выключающее в себя:

1. Иерархическую модель позволяющую выполнять детальный анализ активов АСУ ПП (бизнес-процессы, функциональные задачи, модули подсистем АСУ ПП и показатели качества функционирования модулей подсистем) и особенностей их взаимодействия и использовать результаты данного анализа при оценке информационной безопасности АСУ пассажирскими перевозками.
2. Методику определения значимости элементов иерархической модели АСУ ПП на различных уровнях иерархии содержат подходы к формированию экспертных групп, количественной оценке частных показателей значимости, нечёткой оценке уровней значимости активов, а также наличие неопределенности и неполноты экспертных оценок и зависимостей элементов иерархии.
3. Показатели информационной безопасности, модель и методику оценки информационной безопасности АСУ ПП с использованием векторных и интегральных показателей, учитывающие наличие, как статистических данных, так и экспертные оценки. Оценка проводится с использованием пространственных моделей и экспертного метода анализа иерархий, для реализации которого предложены иерархические структуры и матрицы для установления и анализа взаимосвязей между элементами иерархий. Использование аппарата нечётких чисел позволяет учитывать наличие неопределённостей в исходных данных и выводах экспертов.
4. Методику ситуационного управления, в нечёткой среде, основанную на теории оптимального управления с использованием функций принадлежности в рамках нечеткого метода анализа иерархий.

Теоретическая и практическая значимость результатов исследования:

Разработка моделей и методик позволяет осуществить оценивание информационной безопасности АСУ пассажирскими перевозками и практически оценить уровень ущерба в случае возникновения инцидентов (компьютерных атак).

Степень достоверности и апробация результатов:

Полученные научные результаты подтверждены их апробацией на научных конференциях и семинарах, публикациями в журналах ВАК.

Реализация результатов работы:

Полученные результаты диссертационного исследования реализованы в отчётах по научно-исследовательской работе ФГБОУ ВО ПГУПС, кафедра «Информатика и информационная безопасность»: «Методическое обеспечение категорирования систем железнодорожной автоматики и телемеханики критической информационной инфраструктуры ОАО «РЖД», 2020 г.; «Разработка требований по обеспечению информационной безопасности систем ЖАТ», 2020 г.

Часть исследований проведены в рамках конкурса «Гранты ИБ МТУСИ» 2021-2022 и используются в учебном процессе ФГБОУ ВО ПГУПС в рамках изучения особенностей защиты информации КИИ ЖТ, в том числе АСУ пассажирскими перевозками.

Краткое содержание диссертации с упором на результаты, полученные за период реализации научного проекта в рамках гранта:

За время реализации проекта для первой главы диссертации был проведён анализ бизнес-процессов пассажирского комплекса АСУ ПП, по результатам которого разработана иерархическая модель АСУ ПП, описывающая различные виды активов АСУ ПП (бизнес-процессы, функциональные задачи, модули подсистем АСУ ПП и показатели качества функционирования модулей подсистем) и особенности их взаимодействия. Часть иерархической модели представлена на Рис. 1:

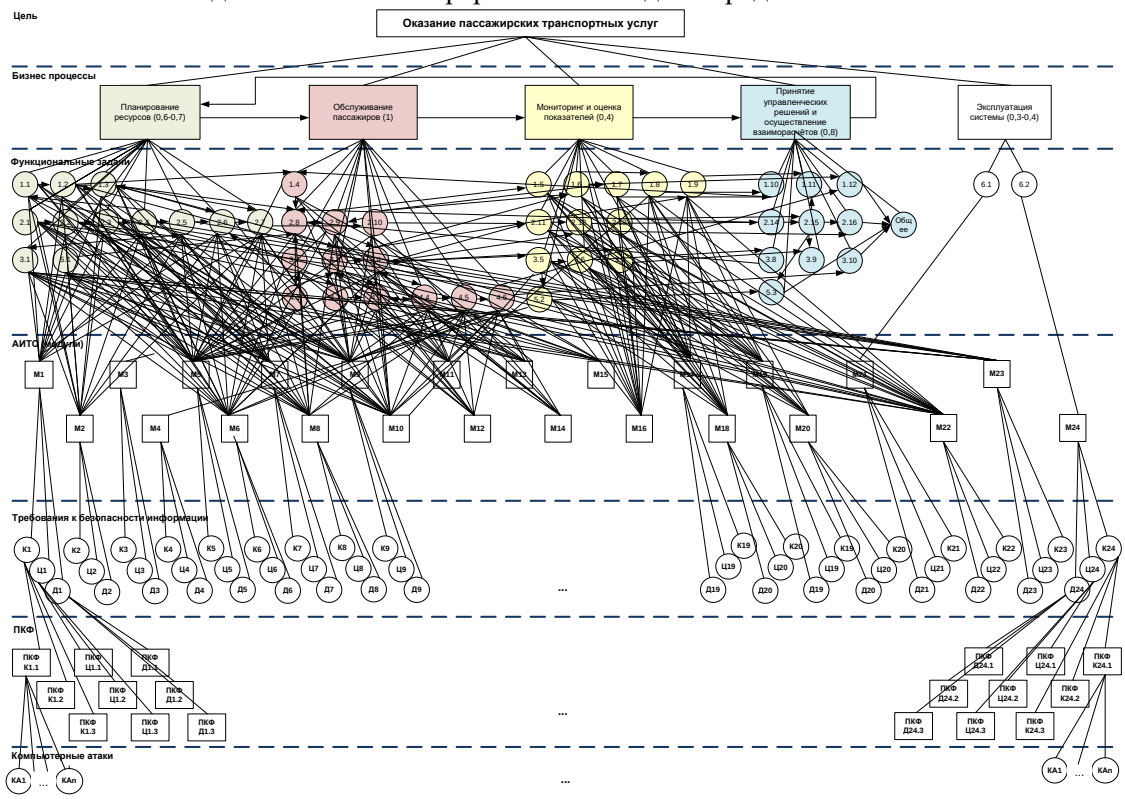


Рис. 1. Часть иерархической модели активов АСУ ПП

Данная иерархическая модель необходима для оценки значимости активов АСУ ПП, векторной оценки состояния информационной безопасности АСУ ПП и ситуационного управления информационной безопасностью АСУ ПП [2].

Во второй главе в рамках проекта усовершенствован обобщенный алгоритм определения значимости критических процессов пассажирских перевозок, функциональных задач, модулей АСУ ПП и показателей функционирования модулей АСУ ПП в условиях нечёткости исходных данных с использованием метода анализа иерархии (в частности нечёткий МАИ) [3,4,5]. Внесено дополнение для случая наличия неопределенности или неполноты экспертных оценок с учётом результатов в [6] (Рис. 2):

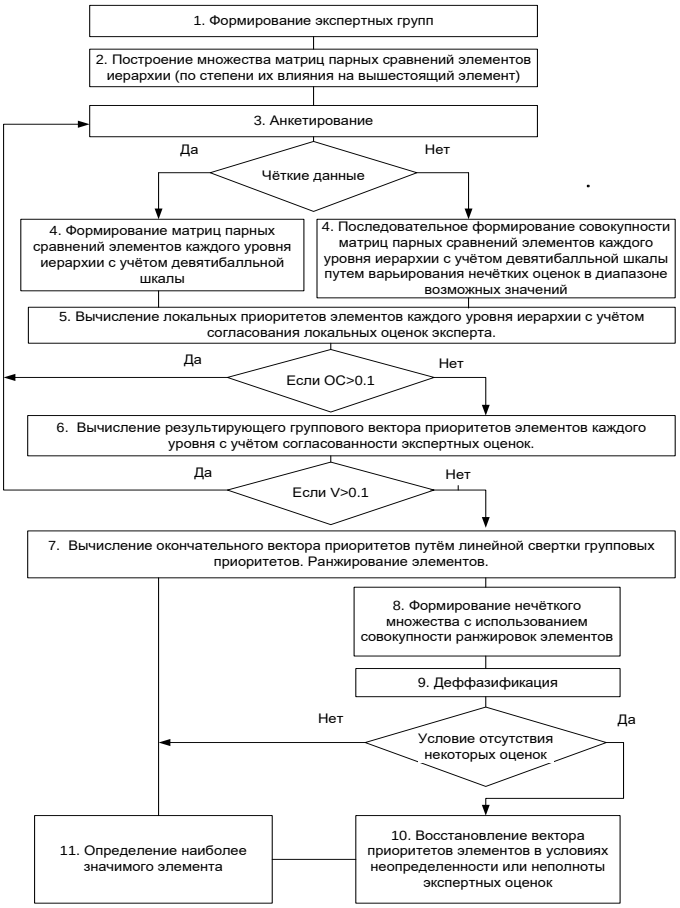


Рис. 2. Алгоритм определения значимости критических процессов пассажирских перевозок, функциональных задач, модулей АСУ ПП и ПКФ модулей подсистем АСУ ПП

По результатам построения иерархической модели был также разработан алгоритм определения значимости элементов иерархической модели АСУ ПП при наличии зависимостей между элементами иерархии с использованием метода аналитических сетей [7] (Рис. 3):

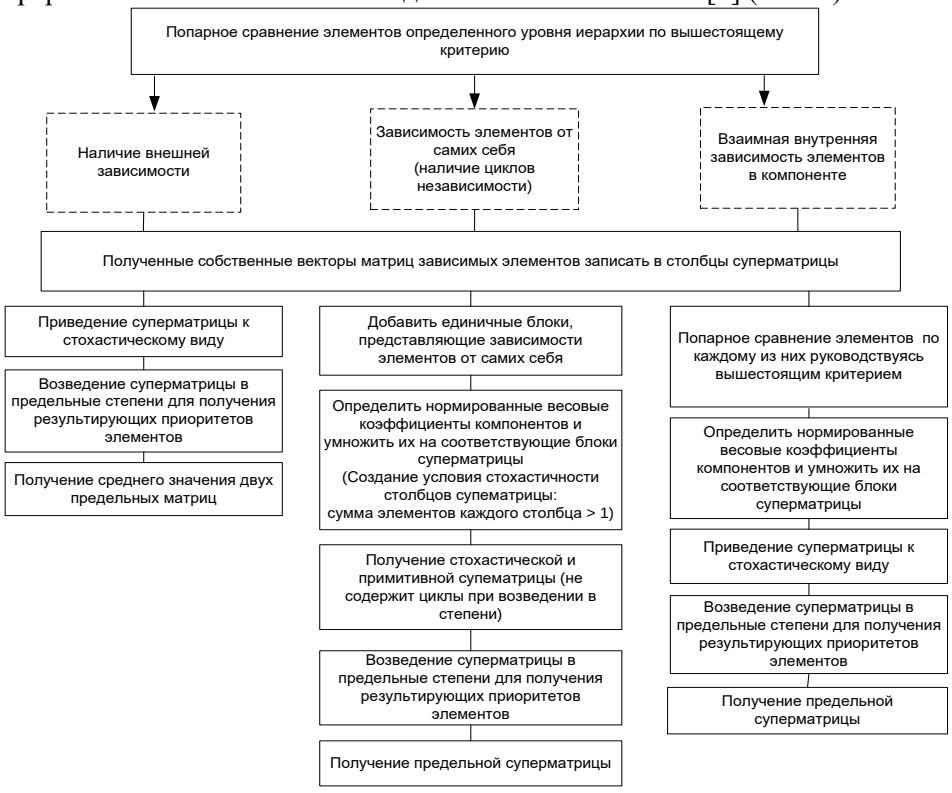


Рис. 3. Алгоритм определения значимости при наличии зависимостей между элементами иерархии

В третьей главе в рамках выполнения проекта проведён анализ показателей безопасности,

построена пространственная модель областей информационной безопасности критических процессов, функциональных задач модулей АСУ ПП, модулей подсистем АСУ ПП и показателей качества функционирования модулей АСУ ПП и получены аналитические зависимости для определения границ безопасности [8].

На Рис. 4 представлен пространственный облик области критических процессов пассажирских перевозок, функциональных задач (ФЗ), модулей АСУ ПП и показателей функционирования АСУ ПП (ПКФ АСУ ПП):

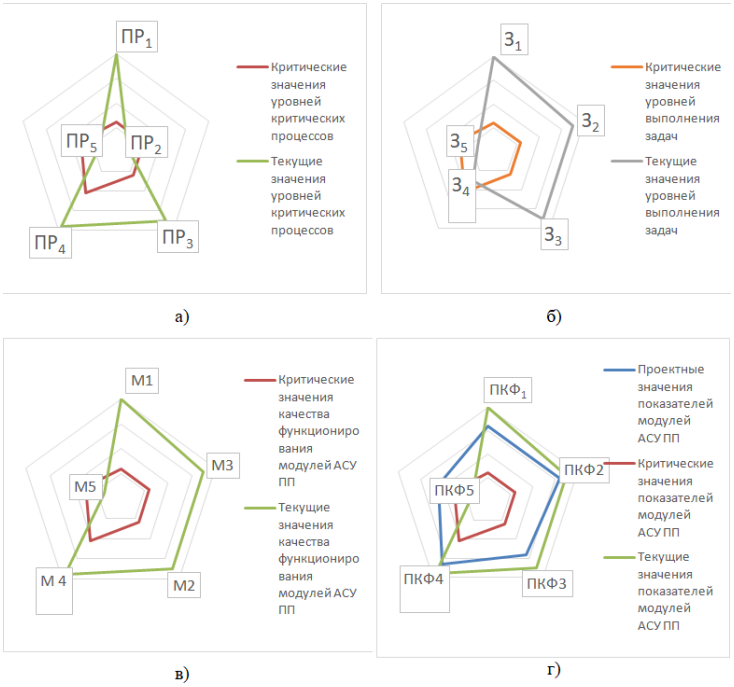


Рис. 4. Пространственный облик области критических процессов (а), функциональных задач (б), модулей АСУ ПП (в) и показателей качества функционирования модулей АСУ ПП (г)

Для целей анализа безопасности и определения уровня безопасности критического процесса, ФЗ, модуля подсистемы АСУ ПП или ПКФ модуля подсистемы АСУ ПП использованы показатели $z_i(k)$, определяемые следующим образом [9]:

$$z_i(k) = \alpha_i \frac{q_i(k) - q_{imp}}{q_{imp}}, \quad (1)$$

для требований вида $q_i(k) \geq q_{imp}$;

или

$$z_i(k) = \alpha_i \frac{q_{imp} - q_i(k)}{q_{imp}}, \quad (2)$$

для требований вида $q_i(k) < q_{imp}$.

Здесь $q_i(k)$ – текущее значение i-го показателя; α_i – весовой коэффициент, характеризующий степень значимости i-го показателя для интегральной оценки уровня безопасности процесса, ФЗ, модуля АСУ ПП или ПКФ модуля АСУ ПП.

При определении границ областей безопасности с использованием формулы (1) рассмотрены различные варианты. В качестве примера ниже представлены случаи, когда:

1. $\alpha_i, q_i(k), q_{imp}$ – нечеткие треугольные числа, например, определяемые на основе мнений экспертов:

$$\alpha_i = (l_{\alpha_i}, m_{\alpha_i}, u_{\alpha_i});$$

$$q_i(k) = (l_{q_i(k)}, m_{q_i(k)}, u_{q_i(k)});$$

$$q_{imp} = (l_{q_{imp}}, m_{q_{imp}}, u_{q_{imp})}).$$

В этом случае, с учетом алгебраических правил [10], получаем формулу (3):

$$z_l(k) = (\frac{l_{\alpha_i} l_{q_i(k)}}{l_{q_{imp}}} - l_{\alpha_i}, \frac{l_{\alpha_i} l_{q_i(k)} u_{q_{imp}} + l_{q_{imp}} (l_{q_i(k)} m_{\alpha_i} + l_{\alpha_i} m_{q_i(k)})}{l_{q_{imp}}^2} + \\ + m_{\alpha_i}, \frac{l_{\alpha_i} l_{q_i(k)} (l_{q_i(k)} m_{\alpha_i} + l_{\alpha_i} m_{q_i(k)}) + l_{q_{imp}} (l_{q_i(k)} u_{\alpha_i} + l_{\alpha_i} u_{q_i(k)})}{l_{q_{imp}}^2} + u_{q_{\alpha_i}}). \quad (3)$$

2. α_i, q_{imp} – нечёткие треугольные числа, а $q_i(k) = P(\prod_{q_i(k)} \le \prod^{\lim}_{q_i(k)})$ имеет значение вероятности того, что рассчитываемое значение частного показателя $\prod_{q_i(k)}$ будет не выше определенного уровня $\prod^{\lim}_{q_i(k)}$:

$$z_l(k) = (\frac{l_{\alpha_i} P(\prod_{q_i(k)} \le \prod^{\lim}_{q_i(k)})}{l_{q_{imp}}} - l_{\alpha_i}, \frac{l_{\alpha_i} P(\prod_{q_i(k)} \le \prod^{\lim}_{q_i(k)}) u_{q_{imp}} + l_{q_{imp}} m_{\alpha_i} P(\prod_{q_i(k)} \le \prod^{\lim}_{q_i(k)})}{l_{q_{imp}}^2} + \\ + m_{\alpha_i}, \frac{l_{\alpha_i} P(\prod_{q_i(k)} \le \prod^{\lim}_{q_i(k)}) m_{\alpha_i} P(\prod_{q_i(k)} \le \prod^{\lim}_{q_i(k)}) + l_{q_i mp} u_{\alpha_i} P(\prod_{q_i(k)} \le \prod^{\lim}_{q_i(k)})}{l_{q_{imp}}^2} + u_{\alpha_i}). \quad (4)$$

Второй вариант, представленный в формуле (4), возможен в том случае, когда показатель $q_i(k)$ является случайным, распределённым в некотором интервале значений по определённому вероятностному закону, и имеется статистическая информации в виде указанного закона распределения вероятностей для параметра, характеризующего влияние фактора (компьютерных атак) на значение показателя.

Предлагаемый методический подход к решению задачи определения границ областей безопасности КИИ ЖТ может применяться для различных уровней иерархии в условиях как точно заданных, так и нечётко определённых параметров, а также их совокупностей, и использоваться в системе управления информационной безопасностью АСУ ПП.

В рамках проекта разработан алгоритм ситуационного управления в нечёткой среде. Анализ состояний при обработке нечётких ситуаций основан на понятии нечёткого равенства ситуаций. На Рис. 5 представлен алгоритм анализа состояния текущей ситуации и проверка её соответствия некоторому эталонному значению:

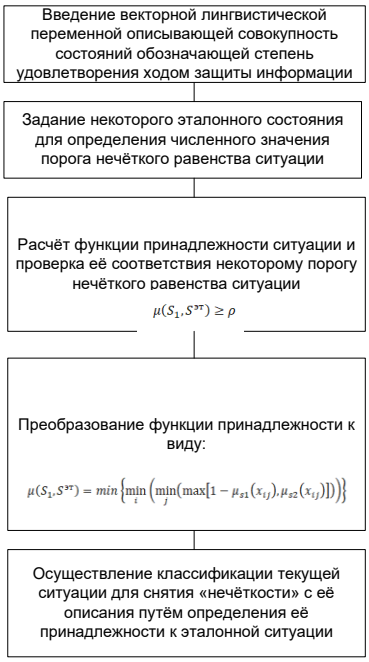


Рис. 5. Алгоритм анализа состояний при обработке нечётких ситуаций

На Рис. 6 представлен смоделированный пример функций принадлежности с учётом кусочно-линейной интерполяции, который наглядно демонстрирует, что при сравнении экспертной оценки текущего состояния информационной безопасности с эталонным (допустимым) состоянием было выявлено несоответствие значению порога нечёткого равенства ситуаций:

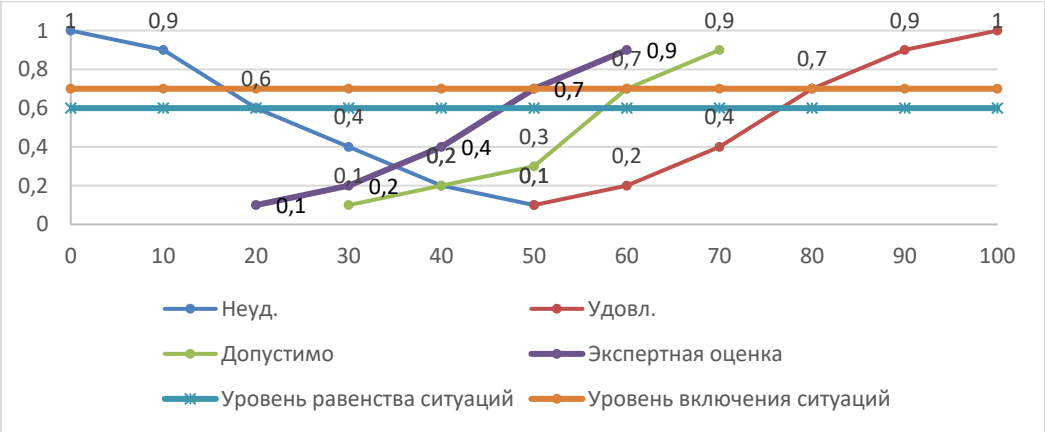


Рис. 6. Значения и уровни функций принадлежности нечёткой переменной

Вывод: текущее состояние информационной безопасности является неудовлетворительным.

Рекомендации и перспективы дальнейшей разработки темы:

Результаты научной работы могут быть использованы в системах оценки защищённости, в центрах мониторинга информационной безопасности, а также в нормативных документах ОАО «РЖД».

СПИСОК ЛИТЕРАТУРЫ

1. Белова, Е.И. Методика оценивания состояния безопасности значимых объектов критической информационно инфраструктуры железнодорожного транспорта // Материалы II Всероссийской научно–практической конференции. г.Пермь. – 2021. – С.44–48.
2. Глухов, А.П. К вопросу о безопасности критической информационной инфраструктуры ОАО «РЖД» / Е.И. Белова, Н.И. Туманов // Международная научно–практическая конференции «Наука и образование транспорту 2020». – 2020. – Том 2. – С.17–19.
3. Глухов, А.П. Определение уровня безопасности значимых объектов критической информационной инфраструктуры железнодорожного транспорта / В.В. Василенко, А.А. Сидак, С.Е. Ададуров, Е.И. Белова // Двойные технологии. – 2020. – №1. – С.84–88. – ISSN 1680–2780.
4. Саати, Т. Принятие решений. Метод анализа иерархии / Т. Саати. – М.: Радио и связь, 1993. – 312 с.
5. Мухаметзянов, И.З. Нечёткий логический вывод и нечёткиё метод анализа иерархий в системах поддержи принятия решений: положение о оценке надежности технических систем // Кибернетика и программирование. – 2017. – №2. – с. 59–77.
6. Бочков, А.В. Метод восстановления вектора приоритетов альтернатив в условиях неопределённости или неполноты экспертных оценок / Н.Н. Жигирев, А.Н. Ридли // Надёжность. – 2017. – Том 17, №3. – С.41–48.
7. Саати, Т. Принятие решений при зависимостях и обратных связях. Аналитические сети / Т. Саати. – М.: ЛЕНАНД, 2019. – 312 с.
8. Глухов, А.П. Определение границ областей безопасности объектов критической информационной инфраструктуры железнодорожного транспорта / В.В. Василенко, А.А. Сидак, Е.И. Белова, Н.И. Туманов // Двойные технологии. – №4. – 2020. – С.63–68.
9. Зиновьев, П.А. Моделирование «дрейфа» нечетких границ области функциональной живучести корпоративной информационной системы // Труды II международной научно–практической конференции. ФГБОУ «Южно–Уральский государственный университет» (национальный исследовательский университет). – 2016. – С.452–457.
10. Alim, F. T. Elementary Operations on L–R Fuzzy Number / S. Johora, A. Sultana Babu // Advances in Pure Mathematics. – 2015. – Vol.05. – No.03.

Буртыка Ф.Б.
ИКТИБ ЮФУ, м.н.с.
bbfilipp@yandex.ru

АВТОМАТИЗИРОВАННЫЙ АНАЛИЗ И ПРЕОБРАЗОВАНИЯ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ С ЦЕЛЬЮ ОПТИМИЗАЦИИ ГОМОМОРФНЫХ ВЫЧИСЛЕНИЙ ЭТИХ СХЕМ

Аннотация: Гомоморфное шифрование (ГШ) позволяет выполнять вычисления с зашифрованными данными, но эффективное применение ГШ — сложная задача, требующая глубокого понимания базовых криптографических протоколов. Современные криптостойкие схемы ГШ типа Джентри вводят в шифртекст компоненту ошибки, называемую шумом, которая увеличивается во время операций, особенно при умножении шифровок. Эту компоненту ошибки необходимо ограничивать, так как обработка большего шума требует установки больших параметров криптосистемы, что приводит к более медленным гомоморфным вычислениям. Есть множество методов, позволяющих уменьшить уровень шума и оптимизировать время гомоморфного вычисления. Однако для их грамотного применения необходимо обладать высокой квалификацией. В данной работе рассмотрены различные эвристические оценки роста шума при вычислениях и методы автоматического преобразования арифметических схем из функциональных элементов с целью оптимизации производительности. Приведен обзор существующих методов переработки арифметических схем на основе критерия минимизации мультипликативной глубины. А также предложен новый метод преобразования схем, отправной точкой которого является выявление областей в схеме, которые согласно эвристике провоцирует наиболее существенный рост шума. Далее для оптимизации критических участков применяется метод, основанный на добавлении дополнительных операций по переключению модулей, реализованный для ГШ в библиотеке Microsoft SEAL. Предложенный метод был реализован как вспомогательный модуль к данной библиотеке. Приводится анализ проведенных экспериментов и описывается класс схем, для коотрых данный метод работает наилучшим образом.

Ключевые слова: гомоморфное шифрование, вполне гомоморфное шифрование, компилятор, оптимизация, мультипликативная глубина, схема из функциональных элементов.

Введение и актуальность темы. Гомоморфное шифрование (ГШ) позволяет проводить операции над зашифрованными данными и получать результат, соответствующий результату операций над незашифрованными данными. ГШ имеет несколько разновидностей, включая полностью гомоморфное шифрование (ПГШ) и частично гомоморфное шифрование (ЧГШ). ПГШ позволяет выполнять *любые* вычисления на зашифрованных данных, выраженные через операции сложения и умножения [1]. ЧГШ также позволяет складывать и умножать, но лишь *ограниченное число* раз. При превышении лимита шифртекст не может быть расшифрован.

Большинство современных схем ГШ основано на задаче «Learning with Errors» (LWE) [1], и предполагает добавление шумовой компоненты к шифртекстам для обеспечения криптостойкости. Пока шум мал, можно расшифровать корректно. Гомоморфные операции увеличивают шум, особенно существенно это для операции умножения. В результате лишь фиксированное число операций можно выполнить. Изначально такие ЧГШ позволяли вычислить лишь логарифмическое от параметра безопасности λ число последовательных умножений. Впоследствии были предложены методики управления шумом [3, 4] такие, что для любой наперед заданной мультипликативной глубины L можно построить экземпляр криптосистемы, разрешающий корректное вычисление L умножений, где размер ключа и шифртекстов $\sim O(poly(L))$. Такие схемы называют вполне гомоморфными (ВГШ). Они являются наиболее перспективными для приложений.

Для получения чистого ПГШ единственный способ – методика «автокоррекции» Джентри (bootstrapping), применяемая к ЧГШ/ВГШ. Она уменьшает шум так, что применение ее после каждого умножения позволяет проводить неограниченное число умножений. Но на практике этот метод не эффективен, его стараются не использовать и обходиться с помощью ВГШ.

ГШ приближается к тому, чтобы стать практичным, но требует глубокого понимания принципов его работы, чтобы использовать его в разработке ПО. Это связано с тем, что в шифртекстах присутствует шум, нарастанием которого при вычислениях нужно грамотно управлять для того, чтоб получить корректное вычисление с минимальной сложностью. Нужно изначально уметь выбрать подходящие параметры схемы ВГШ, чтобы она поддерживала необходимую схемную сложность. В

процессе может потребоваться перестройка арифметической схемы из функциональных элементов (АСФЭ) для вычислений и введение дополнительных операций обработки шифртекстов для снижения шума и улучшения производительности. Все это делает разработку приложения, использующего ГШ сложной задачей.

В настоящее время отсутствует полноценный инструментарий для разработчиков, не обладающих знаниями в области криптографии, для написания кода без понимания устройства схем ВГШ. Хотя уже появились некоторые инструменты (библиотеки ПГШ и компиляторы), переводящие программы, написанные на языках высокого уровня, в арифметические схемы, которые уже можно вычислять с помощью ГШ. Однако получаемые в результате схемы могут быть неоптимальны с точки зрения количества потребляемых мультипликативных уровней, скорости роста шума и производительности. Требуются дополнительные инструменты, позволяющие разработчику осуществлять оптимизацию в автоматическом режиме.

Цели и задачи работы. В существующих работах используют один из двух подходов к управлению ростом шума. Первый использует эвристические оценки роста шума [10], чтобы оценить оптимальные параметры ВГШ для вычисления заданной АСФЭ. Но эти оценки слишком консервативны и не дают оптимальных результатов по производительности. Второй подход [12] пытается автоматически переупорядочить или переписать схему вычисления для достижения лучших характеристик роста шума. Но здесь от разработчика требуется ручной выбор параметров, либо используют упрощенные методы, что приводит к неэффективному выбору. Данная работа предлагает подход к оптимизации гомоморфного вычисления (ГВ) за счет объединения этих подходов в одно целостное решение. Мы используем эвристические оценки величины шума для выявления областей АСФЭ, ответственных за наиболее значительный роста шума. Тем самым выявляем части АСФЭ, которые имеет смысл переписать. И далее уже модифицируем эти части АСФЭ так, чтоб минимизировать рост шума. Минимизация нарастания шума позволяет выбирать меньшие параметры ВГШ, что может повысить производительность.

В данной работе в качестве основы мы используем ВГШ FV [4], реализованную в библиотеке Microsoft SEAL [11]. Предлагаемый метод модификации АСФЭ основан на добавлении вспомогательных операций переключения модулей (ПМ, modulus switching) после некоторых гейтов.

Основные задачи исследования.

1) Создание общей методологии оптимизации гомоморфных вычислений по времени и памяти, объединяющей эвристики оценки роста шума для данной АСФЭ и различные методы переписывания АСФЭ на основе этих эвристик. Результатом переписывания АСФЭ является семантически эквивалентная схема, которую можно вычислить с большей эффективностью
2) Проработка метода модификации АСФЭ для ВГШ FV, основанного на добавлении вспомогательных ПМ операций. Апробация данного метода на эталонном наборе схем и выделение класса АСФЭ, для которого он работает наиболее эффективно.
3) Создание программного модуля, реализующего данную методологию, и его интеграция с библиотекой Microsoft SEAL. Этот модуль будет предоставлять разработчикам возможность, подав на вход описание АСФЭ, получить оценку подходящих параметров ВГШ и модифицированный вариант АСФЭ, сложность вычисления которого будет более оптимальна, чем для исходной схемы.

Теоретическая и практическая значимость работы. На данный момент оптимизация гомоморфного вычисления АСФЭ с помощью ВГШ является трудной задачей. Библиотеки ГШ, такие как SEAL, предоставляют API, дающее основные функции, такие как генерация ключей, шифрование, дешифрование, а также гомоморфные базовые арифметические операции. Однако они по-прежнему остаются низкоуровневыми и оставляют вопросы управления шумом и проектирования АСФЭ на усмотрение пользователя Наша цель предоставить неопытным разработчикам инструменты для автоматической (или хотя бы полуавтоматической) оптимизации АСФЭ для ГВ. Наличие таких инструментов поможет сделать написание ПО, использующего ВГШ, более доступным и простым для начинающих разработчиков.

Степень разработанности темы. На данный момент в литературе наиболее проработан метод модификации АСФЭ для оптимизации ГВ, основанный на переписывании конуса (cone rewriting). Основная цель – уменьшения мультипликативной глубины (МГ) АСФЭ. Это может помочь уменьшить рост шума, позволяя использовать меньшие параметры для ВГШ и, как следствие, ускорить вычисления. АСФЭ интерпретируется как граф, в котором рассматривается множество всевозможных путей от входных вершин к выходным. Выделяется подмножество критических путей, т.е. таких, что

МГ пути равна МГ всей АСФЭ. Далее нужно перестроить каждый критический путь так, чтоб уменьшить его МГ. Тогда МГ всей АСФЭ будет уменьшена. В [7] были предложены два базовых оператора переписывания путей, основанных на перестройке их подпутей. Первый оператор умеет переписывать подпути в графе АСФЭ, состоящие только из гейтов умножения. А именно, подпуть длины 2 можно переписать на основе свойства ассоциативности $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. Если подсхема имеет вид $(x \cdot y) \cdot z$, то замена ее $x \cdot (y \cdot z)$ уменьшит МГ критического пути в случае, если МГ узлов y и z меньше МГ x. Если это так, то МГ уменьшается на единицу. Второй оператор позволяет получить подпуть, состоящий только из 2-х гейтов умножения из любого подпути с МГ = 2 (т.е. подпути с любым количеством внутренних гейтов сложения). Он использует свойство дистрибутивности $(x + y) \cdot z = x \cdot z + y \cdot z$. В [2] эти два оператора объединены в один оператор модификации подпутей в АСФЭ с МГ = 2. Полученный оператор называется оператором минимизации конусов. В [2] представлена эвристика, направленная на минимизацию МГ АСФЭ за один проход: на каждой итерации вычисляется набор конусов Δ_{min}. Если Δ_{min} не пусто, то конусы из этого множества переписываются и впоследствии обновляются МГ узлов схемы. Если МГ новой АСФЭ меньше, она обновляется. В противном случае определяется новый Δ_{min} и применяется алгоритм перезаписи. Алгоритм окончательно завершается, когда Δ_{min} становится пустым.

Описанное преобразование АСФЭ в конечном итоге может уменьшить МГ схемы. Однако при этом может увеличиться общее число гейтов в АСФЭ, в некоторых случаях значительно. Поэтому для некоторых АСФЭ этот метод привести к ухудшению производительности.

В [2] изучалось влияние минимизации МГ схем на ГВ. Ясно, что минимизация МГ выгодна только в случае, если количество гейтов, добавленных к АСФЭ, ниже порогового значения.

Модификация АСФЭ, нацеленная на уменьшение МГ, не берет в расчет участки АСФЭ, на которых происходит реальный прирост шума. Если наиболее существенное увеличение шума происходит на пути АСФЭ, который не подвергается операции переписывания конуса, как, например, большое количество последовательных сложений, описанный способ практически не влияют на оптимизацию схемы. Успех применения данного метода существенно зависит от конкретной АСФЭ.

На данный момент в литературе не предложено методов модификации АСФЭ для улучшения производительности ГВ, основанных на эвристике шума и выделении участков АСФЭ, дающих наиболее существенный прирост шума. Здесь мы восполним этот пробел и опишем такой метод.

Научная новизна. Ранее в литературе не предлагалось метода модификации АСФЭ для ГВ, основанного на применении эвристических оценок роста шума.

Основные положения, выносимые на защиту.

1) Предложен метод оптимизации производительности ГВ для ВГШ FV, основанный на переписывании вычисляемой АСФЭ исходя из эвристических оценок нарастания шума. При этом модификация АСФЭ осуществляется за счет добавления вспомогательных операций переключения модулей после некоторых гейтов умножения.
2) Получено описание класса АСФЭ, для которого данная методология работает наиболее эффективно.
3) Реализован программный комплекс для автоматической оптимизации АСФЭ, реализующий разработанную методологию.

Краткое содержание диссертации.

1. Описание ВГШ FV.

Пусть есть $q, t \in \mathbb{Z}, q \gg t, t > 1$, $\Delta := q/t$, $q = \prod_i q_i$, q_i – простое число. Пусть также есть вероятностное распределения с χ с небольшой дисперсией над $\mathbb{Z}_q$, кольца $R_q = \mathbb{Z}_q[x]/(f(x))$ и $R_t = \mathbb{Z}_q[x]/(f(x))$, где $f(x) = x^d + 1$, $d = 2^n$.

Генерация секретного ключа: $s \leftarrow \chi$, выдать $sk = s$.

Генерация открытого ключа: $a \leftarrow R_q$, $e \leftarrow \chi$ и вернуть $pk = ([-(a \cdot s + e)]_q, a)$, где $[b]_q$ означает покоэффициентное приведение b по модулю q.

Шифрование: Получает на вход открытый текст $m \in R_t$ и $pk = (p_0, p_1)$. Генерирует u, e_1, $e_2 \leftarrow \chi$ и выдает $ct = ([p_0 \cdot u + e_1 + \Delta \cdot m]_q, [p_1 \cdot u + e_2]_q)$.

Расшифрование: Получает на вход sk и шифртекст $ct = (c_0, c_1)$ и вычисляет: $\left[\left\lfloor \frac{t \cdot [c_0 + c_1 \cdot s]_q}{q} \right\rceil\right]_t$.

Слагаемое $v = \Delta \cdot m + e \cdot u + e_1 + e_2 \cdot s$ называется шумом, содержащимся в шифртексте. Бюджет шума шифртекста – это величина равная $\sigma = -\log_2(\|v\|)$. По мере гомоморфных вычислений она уменьшается, особенно быстро при умножении. Корректное расшифрование возможно, пока $\sigma > 0$.

Суммирование шифртекстов осуществляется покоординатно. Умножение двух шифртекстов вводит нелинейный член, в результате чего шифртекст будет состоять уже из трех элементов, т.е. $ct_{mul} = [c_0, c_1, c_2]$. Эта проблема решается релинеаризацией, вычисляющей шифртекст $ct' = [c_0', c_1']$, который будет шифровать тот же открытый текст.

Определение (Переключение модуля) Пусть есть $ct = (c_0, c_1) \in R_q^2$, p и q – взаимно простые. Операция ПМ выдает шифровку $(c_0', c_1') = (\left[\left\lfloor \frac{p}{q} \cdot c_0 \right\rceil\right]_p, \left[\left\lfloor \frac{p}{q} \cdot c_1 \right\rceil\right]_p)$.

ПМ увеличивает шум, поэтому использование ПМ для BFV ограничивается отбрасыванием сомножителей q_i по очереди из q, тем самым создавая лестницу $\mathfrak{J}$ модулей длины β. ПМ меняет параметры ct вниз по цепочке модулей. Размер ct линейно зависит от β. Если не надо выполнять дальше вычисления с ct, то целесообразно выполнить ПМ операцию перед расшифрованием до минимального модуля в $\mathfrak{J}$. Выполнение ПМ уменьшает глубину АСФЭ, которую может корректно вычислить FV. Но ПМ можно применить, если основная часть затратных в плане шума вычислений выполнена и остаток вычислений можно провести с меньшим q, сохраняя корректность расширофвания. Это улучшит производительность.

2. Выделение подсхем АСФЭ, ответственных за наиболее значительный рост шума.

Полезно определить области АСФЭ, которые являются источником основного роста шума, чтобы увидеть, где есть потенциал для изменения АСФЭ. Мы рассматриваем АСФЭ как ориентированный ациклический граф (ОАГ) $C = (V, E)$, где каждый узел представляет значение, доступное во время ГВ. Узлы, имеющие входящие ребра называются инструкциями (гейтами). Инструкции могут быть следующие: +, -, * и ПМ операция. Мы используем эвристические оценки бюджета шума и спад относительного бюджета шума, чтобы идентифицировать интересующие нас области АСФЭ. Здесь спад относительного бюджета шума определяется как $(min\{E1, E2\} - E)/min\{E1, E2\}$, где $E1$ и $E2$ – бюджеты шума операндов, а E – бюджет шума после ГВ бинарной операции. Однако сами по себе эти величины не могут быть использованы для выявления областей роста шума: бюджет шума всегда будет наименьшим в самом конце вычисления, поскольку гомоморфные операции в ВГШ наращивают шум, но никогда не уменьшают.

Мы предлагаем алгоритм, который, начиная с корневого узла (результата вычислений), проходит ОАГ, рекурсивно посещая дочерние элементы с наименьшим бюджетом шума. Если все потомки имеют одинаковый бюджет шума, то все потомки посещаются. Алгоритм завершает работу, возвращая один или несколько конечных узлов, указывающих пути, которые являются источником значительного роста шума. Алгоритм 1 использует функции $GetNoiseBudget(node\ v)$, которые возвращают эвристику шума заданного входного узла (шифртекста), а также функцию $CalculateEncryptionNoiseHeuristics\ (v)$, которая возвращает эвристику шума для «свежего» шифртекста.

Лемма. Алгоритм 1 всегда завершает работу и возвращает узел.

Доказательство. Проведем по индукции: для деревьев единичного размера алгоритм возвращает один узел. Предположим, что алгоритм завершает работу и возвращает узел для дерева размера $n - 1$. Для дерева размера n, на первом шаге алгоритм посещает дерево размера $\leq n - 1$. По индукции, алгоритм завершает работу и возвращает узел.

Алгоритм 1 выявляет один или несколько путей, которые потенциально могут быть переписаны, чтобы ограничить рост шума во время ГВ, что позволяет выбрать более оптимальные параметры и повысить эффективность вычислений. Важно отметить, что возвращаемый путь не обязательно является областью АСФЭ, где существует потенциал для оптимизации. Может быть, что алгоритм вернет уже полностью оптимизированный путь. Поэтому он просто служит основой для стратегий улучшения АСФЭ.

Алгоритм 1 Обход вершин АС

Вход: вершина АС, с которой начинается обход
Выход: вершина, в которой оканчивается обход ОАГ

```
1: procedure Visit(node n)
2:     left := GetNoiseBudget(leftChild(n))
3:     right := GetNoiseBudget(rightChild(n))
4:     initial := CalculateEncryptionNoiseHeuristics(n)
5:     if (right == left) ∧ ((right == initial) ∨ (right == NULL)) then
6:         return n
```

```
7:     else if (left ⩽ right) then
8:       Visit(left)
9:     else if (left > right) then
10:      Visit(right)
11:    else
12:      Visit(left)
13:     Visit(right)
14:   end if
15: end procedure
```

3. Модификация АС посредство вставки ПМ операций.

Для любой функции можно разработать большое количество АСФЭ, вычисляющих ее. Для ГВ большое значение имеет именно АСФЭ – некоторые АСФЭ индуцируют больший рост шума в шифртекстах, чем другие. Это вызвано различными факторами: число последовательно выполняемых умножений или добавление дополнительных операций по обслуживания шифртекста, таких как релинеаризация или ПМ. Здесь представим пару алгоритмов, использующих эвристику шума, на основании которой в АСФЭ будут добавляться дополнительные операции ПМ в соответствующих точках. Это уменьшит битовую длину модуля q шифртекста и ускорит ГВ оставшейся части схемы. Это может дать значительный эффект, поскольку в FV q это очень большое число (битовой длины в несколько тысяч) и шифртексты являются полиномами большой степени. Поэтому уменьшение q в результате ПМ может улучшит скорость ГВ.

Как уже отмечалось, в FV выполняется $q = \prod_{i=1}^{\beta} q_i$. ПМ здесь работает так, что просто отбрасывается часть сомножителей, чтобы уменьшить битовую длину q с помощью переключения модуля (ModSwitch). Предлагаемый Алгоритм 2 анализирует операнды каждого мультипликативного гейта в АСФЭ и вычисляет бюджет шума, затраченный при вычислениия, для автоматического применения ПМ операции к операндам, если количество битов в шифртексте, занятых шумом, превышает битовую длину последнего простого числа в цепочке $q_1, \dots, q_\beta$. В этом случае алгоритм применяет к операндам ПМ операцию.

Поскольку операция ПМ изменяет модуль шифртекста, то при вставке ПМ гейтов в АСФЭ для корректной работы ВГШ, должно обеспечить, чтобы операнды любого гейта в результате имели одинаковый модуль q шифртекста. Мы уже отмечали, что после выполнения достаточного количества вычислений разумно выполнить ПМ операцию, но мы должны гарантировать, что для обоих операндов гейта битовая длина шумового члена больше, чем битовая длина последнего простого числа q_β в цепочке $q_1, \dots, q_\beta$.

Алгоритм 2 использует оценку уровня шума в шифртексте, чтобы решить, возможно ли включение операции ПМ в АСФЭ без ущерба для вычислений. Эвристическая оценка шума, рассчитывается для каждого узла АСФЭ. Мы рассматриваем разницу между бюджетом шума «свежего» шифртекста (только что вышедшего из шифратора) и бюджетом шума шифртекста, являющегося результатом вычисления узла в ОАГ. Эту разницу будем называть *израсходованным бюджетом шума*. Для каждого гейта израсходованные бюджеты шума операндов сравниваются с битовыми длинами последних простых множителей в лестнице модулей $\mathfrak{J}$. Если их разность превышает q_β и гейт является мультипликативным, то операция ПМ возможна и вставляется в схему с помощью функции $insertModSwitch(operand)$. Эта функция принимает шифртекст операнда в качестве входных данных. На этом шаге алгоритма гарантируется, что в рассматриваемой бинарной операции не возникнет рассогласования параметров, т. е. оба операнда имеют одинаковый модуль. Затем пересчитываются шумовые эвристики новой схемы. Если бюджет шума в корневом узле ОАГ остается больше нуля, изменения принимаются и АСФЭ обновляется.

Алгоритм 2 использует набор вспомогательных функций. Функции $getLeftOperand(op)$ и $getRightOperand(op)$ принимают двоичную операцию op и возвращают левый или, соответственно, правый операнд. Функция $getLastPrimeIndex(v)$ принимает шифртекст и возвращает индекс последнего простого числа в цепочке $\mathfrak{J}$. Для вычисления битовой длины простых чисел в модуле шифртекстов q была определена функция $bitLen(q_i)$. Наконец, функция $spentNoiseBudget(node)$ принимает в качестве входных данных шифртекст и возвращает израсходованный бюджет шума.

Мы должны гарантировать, что модули коэффициентов шифротекстов, участвующих в бинарных операциях, всегда совпадают. Поэтому необходимо выполнить второй проход по схеме,

чтобы гарантировать, что новая схема удовлетворяет этому требованию. Алгоритм 3, начинается с корня ОАГ и посещает все бинарные гейты в порядке возрастания и сравнивает модули шифртекстов входных узлов текущего гейта. Если есть несоответствие, то операции ПМ над операндом с бОльшим модулем шифртекста выполняются до тех пор, пока модули операндов не сравняются. Это можно сделать, поскольку результирующий израсходованный бюджет шума после любой бинарной операции будет превышать размер отброшенных простых чисел.

Лемма. Алгоритмы 2 и 3 завершают работу и создают корректную АСФЭ.

Доказательство. Основной цикл алгоритма 2 завершается, так как в дереве конечное число двоичных инструкций. Кроме того, алгоритм 3 возвращает правильное дерево, поскольку он гарантирует, что число простых чисел в модулях одинаково для операндов в каждом двоичном выражении.

Алгоритм 2 Rewrite (circuit)

Вход: СФЭ circuit.

Выход: оптимизированная СФЭ, семантически эквивалентная circuit

```
1:  for каждой бинарной операции op схемы circuit do
2:    if op – это умножение then
3:      tempCircuit := circuit
4:      left := GetLeftOperand(op)
5:      right := GetRightOperand(op)
6:      leftIndex := GetLastPrimeIndex(left)
7:      rightIndex := GetLastPrimeIndex(right)
8:      diff := leftIndex - rightIndex
9:      if (diff > 0) then
10:       sum := 0
11:       for i:=leftIndex downto leftIndex – ( |diff| + 1)
12:         sum:= sum + bitLen(coeffModulus[i])
13:       end for
14:       if ( sum < spentNoizeBudget(left) ) ∧
              ( spentNoizeBudget(right) > bitLen(coeffModulus[rightIndex]) ) then
15:         tempCircuit.insertModSwitch(right)
16:         for j:=0 to |diff|-1 do
17:           tempCircuit.insertModswitch(left)
18:         end for
19:       end if
20:       if (tempCircuit.getNoizeBudget(root) > 0) then
21:         circuit := tempCircuit
22:       end if
23:     else if (diff < 0) then
24:       sum := 0
25:       for i:=rightIndex downto rightIindex – (|diff|+1) do
26:         sum := sum + bitLen(coeffModulus[i])
27:       end for
28:       if ( sum < spentNoizeBudget(right) ) ∧
              ( spentNoizeBudget(left)> bitLen(coeffModulus[leftIndex]) ) then
29:         tempCircuit.insertModSwitch(left)
30:         for j:=0 to |diff|-1 do
31:           tempCircuit.insertModSwitch(right)
32:         end for
33:       end if
34:       if (tempCircuit.getNoizeBudget(root) > 0) then
35:         circuit := tempCircuit
36:       end if
37:     else
38:       if ( bitLen(coeffModulus[leftIndex]) > SpentNoizeBudget(left) ∧
              ( bitLen(coeffModulus[rightIndex]) > SpentNoizeBudget(right)) ) then
39:         tempCircuit.insertModSwitch(left)
```

```
            tempCircuit.insertModSwitch(right)
            if (tempCircuit.getNoizeBudget(root) > 0) then
              circuit := tempCircuit
            end if
          end if
        end if
      end if
    end for
  return circuit
```

Алгоритм 3 Обход и обработка вершин графа СФЭ

Вход: корневая вершина графа СФЭ.
Выход: обработанный граф СФЭ

```
procedure Visit(node n)
  if n – бинарное выражение then
    if HasChild(GetLeft(n)) ∧ (Visited(GetLeft(n)) == false) then
      Visit(GetLeft(n))
    end if
    if HasChild(GetRight(n)) ∧ (Visited(GetRight(n)) == false) then
      Visit(GetRight(n))
    else if GetLastPrimeIndex(GetLeft(n)) ≠ GetLastPrimeIndex(GetRight(n)) then
      вставить ModSwitch перед n
    end if
  end if
end procedure
```

Ниже мы увидим, что при оценке влияния переписывания АСФЭ с использованием предложенных алгоритмов, есть существенная разница, вставляется ли ПМ операция перед гейтом сложения или умножения. Гомоморфное сложение выполняется значительно быстрее, чем ПМ операция и гомоморфное умножение. Это может негативно повлиять на производительность АСФЭ, если алгоритмы добавит ПМ операции перед сложением. Кроме того, поскольку эвристические оценки шума обычно переоценивает израсходованный шумовой бюджет шифртекста, положение вставленных ПМ операций не обязательно соответствует месту вставки, полученному из расчетов реального шума. Однако, поскольку Алгоритм 2 пересчитывает шумовую эвристику всей схемы после каждой вставки ПМ, корректность схемы всегда гарантируется.

4. Результаты вычислительного эксперимента и их анализ.

Описанные алгоритмы были реализованы на языке C++ как вспомогательные модули к библиотеке Microsoft SEAL. Для тестирования реализации использовалась рабочая станция Apple M1 CPU (3.2 GHz), 8 GB RAM. Чтобы проанализировать влияние разработанных инструментов оптимизации схем на время ГВ, для экспериментов была использована выборка АСФЭ из набора комбинаторных тестов EPFL. Был реализован синтаксический анализатор, переводящий схемы из пакета EPFL, представленные в формате Verilog, в специфичное для предметной области представление в виде АСФЭ. Схемы, выбранные для экспериментов, были частично усечены в плане глубины и сложности, чтобы обеспечить возможность их корректного гомоморфного вычисления с помощью SEAL.

Здесь мы оценим эффект применения алгоритмов 2 и 3 к различным АСФЭ. Мы увидим, что применение указанных алгоритмов может по-разному влиять на время ГВ в зависимости от характера АСФЭ. Сначала оценим время выполнения одиночных гомоморфных бинарных операций и ПМ операции, чтобы показать влияние вставки ПМ на отдельные операции.

Таблица 1: Тайминги бинарных операций и ПМ операции для FV, полученные, с использованием SEAL, для $d = 16384$ и $d = 32768$. Результаты показаны в мксек, а стандартные отклонения указаны в скобках

	$d = 16384$			$d = 32768$		
	Mult	Add	ModSwitch	Mult	Add	ModSwitch
Уровень 1	30189 (31)	220 (1)	1167 (2)	149681 (191)	844 (4)	4375 (7)
Уровень 2	25733 (11)	208 (2)	1036 (2)	135788 (87)	740 (1)	4038 (4)

Уровень 3	21786 (12)	191 (2)	856 (1)	124121 (89)	699 (1)	3747 (3)
Уровень 4	18030 (4)	143 (1)	855 (1)	110709 (50)	648 (1)	3774 (2)

Видно, что среднее время выполнения ПМ превышает время сложения. Из этого видно, что возможно неблагоприятное влияние на производительность, если алгоритмы 2 и 3 вставят инструкции ПМ перед гейтами сложения. Однако добавление ПМ для обоих операндов перед мультипликативным гейтом может, напротив, дать повышение производительность.

Мы анализируем влияние описанного метода модификации АСФЭ, чтобы представить наилучший и наихудший сценарии и показать, что метод может иметь разное влияние на схемы различной природы.. АСФЭ выбирались так, чтобы продемонстрировать в том числе влияние количества аддитивных гейтов в схеме на эффективность введенных оптимизаций. Общее влияние на время ГВ после применения алгоритмов 2 и 3 относительно невелико, обычно в диапазоне 15 процентов. В таблице 3 показаны отношения средних значений времени ГВ для исходных АСФЭ и времени выполнения, измеренного после преобразования с помощью алгоритмов 2 и 3. Из таблицы 2 видно, что переписывание схемы на основе ПМ операции не всегда положительно влияет на производительность.

Таблица 2: Средние коэффициенты ускорения для оценки выбранных АСФЭ.

Схема	$d = 8192$	$d = 16384$	$d = 32768$
$(x^4 + y) \cdot z^4$	1,15	1,15	1,12
$(x^4 + y) \cdot z^4 + \sum_{i=1}^{12} a_i$	0,93	0,98	0,98
Сумматор	-	1.00	0,97
«Сдвиговый регистр»	-	1,02	1,09
«Максимум»	-	1,12	1,03

Рассмотрим схему, представляющую вычисление полинома $f(x, y, z) = (x^4 + y) \cdot z^4$. По построению алгоритмы применяют операцию ПМ к каждому из операндов $(x^4 + y)$ и z^4, а также перед вычислением конечного результата $(x^4 + y) \cdot z^4$. В таблице 4 мы показываем сравнение среднего значения времени ГВ модифицированной и исходной АС для $d \in \{8192, 16384, 32768\}$. Таблица 3 показывает, что здесь коэффициент ускорения > 1 при использовании описанного метода.

Таблица 3: Среднее время выполнения в мс для вычисления f с использованием SEAL с ПМ операцией и без нее.

d	С ПМ	Без ПМ
Для $f = (x^4 + y) \cdot z^4$		
8192	60	76
16384	315	338
32767	1570	1624
Для $f = (x^4 + y) \cdot z^4 + \sum_{i=1}^{12} a_i$		
8192	86	76
16384	350	333
32767	1680	1628

Это связано с характером схемы, поскольку в схеме аддивтных гейтов, чьи операнды которых должны подвергаться ПМ операции после трансформации АС.

Рассмотрим другой пример $f = (x^4 + y) \cdot z^4 + \sum_{i=1\ldots12} a_i$. Как и в предыдущем примере, алгоритм 2 вставляет ПМ перед умножением $(x4 + y) \cdot z4$. Чтобы компенсировать несовпадение параметров при последовательных сложениях, алгоритм 3 применяет ПМ и к слагаемым a_i. Это оказывает негативное влияние на время ГВ, как видно из таблиц 4.2 и 4.3.

Для дальнейшего изучения предложенной методики мы дополнительно выполнили бенчмаркинг на подмножестве АСФЭ из набора комбинаторных тестов EPFL. Набор АСФЭ, выбранных для тестирования, состоит из схем: Adder (Сумматор), Сдвиговый регистр («Сдвиг») и Максимум (Макс). АС были усечены для обеспечения корректности ГВ. Оценка времени работы

представлена в таблице 4.4 для d = 16384 и d = 32768 соответственно. Коэффициенты ускорения представлены в таблице 3. Время вычисления схемы сумматора фактически увеличивается при вставке ПМ алгоритмами, что вязано большим количеством сложений в АСФЭ. Для двух других схем мы наблюдаем улучшение времени работы. Эти результаты показывают, что мы не можем предсказать значительное улучшение производительности в общем случае. Время выполнения предлагаемых алгоритмов перезаписи сильно зависит от количества выполняемых АСФЭ сложений.

Таблица 4: Среднее время выполнения в мс для АС из EPFL набора.

АС	С ПМ	Без ПМ
Для $d = 16384$		
Adder	4902	4800
Bar	2400	2440
Max	8700	8900
Для $d = 32768$		
Adder	26330	26012
Bar	12881	13100
Max	53004	53500

Заключение.

В работе исследованы существующие методы модификации АСФЭ для оптимизации времени ГВ, основанные на минимизации мультипликативной глубины. А также предложен новый алгоритм модификации АС. Основная его идея состоит в том, что эвристические оценки величины шума используются для выделения самых проблемных областей АСФЭ, в которых шум нарастает наиболее интенсивно при ГВ. В основе нашей реализации лежит ВГШ FV. Мы использовали методики эвристической оценки шума в процессе ГВ, представленные для FV в [10]. Эвристические оценки зачастую переоценивают степень нарастания шума, однако тем не менее они дают некоторую полезную верхнюю оценку. И вычислить эти оценки можно очень быстро по сравнению с проведением ГВ.

После получения оценок на бюджет шума в каждом узле схемы, к критическим областям можно применить различные модификации. Здесь мы предлагаем модификацию АСФЭ на основе добавления дополнительных операций переключения модуля, что позволяет для определенного подмножества АСФЭ улучшить производительность вычисления.

Как показывают вычислительные эксперименты наиболее целесообразно ынедрять ПМ операции перед мультипликативными гейтами. Так как гомоморфное умножение имеет горазд бОльшую вычислительную сложность, чем ПМ. Однако для сохранения корректности ГВ для некоторых АСФЭ возникает необходимость добавить ПМ операции и перед аддитивными гейтами. Это может вызвать обратный эффект в плане производительности, поскольку сложение шифртекстов более легковесно, чем ПМ операция. И время вычсиления может увеличиться.

Возможная оптимизации предложенного алгоритма возможны в том ключе, что можно отказаться добавлять ПМ операции в случае, если в подсхеме есть аддитивный гейт с большим количеством операндов.

СПИСОК ЛИТЕРАТУРЫ

1. Бабенко, Л.К. Полностью гомоморфное шифрование (Обзор) / Л.К. Бабенко, Ф.Б. Буртыка, О.Б. Макаревич, А.В. Трепачева // Вопросы защиты информации. — 2015. — № 3. — С. 3-26.
2. Chilotti, I. TFHE: Fast Fully Homomorphic Encryption over the Torus / I. Chilotti, N. Gama, M. Georgieva, M. Izabachene // Journal of Cryptology. — 2020. — № 1. — Стр. 34-91.
3. Brakerski, Z. (Leveled) Fully Homomorphic Encryption without Bootstrapping. / Z. Brakerski, G. Craig, V. Vaikuntanathan // ACM Transactions on Computation Theory. — 2014. — № 3. — Стр. 1-36.
4. Fan, J. Somewhat Practical Fully Homomorphic Encryption / J. Fan, F. Vercauteren // Cryptology ePrint Archive, Report 2012/144. — 2012. — № 144. — https://eprint.iacr.org/2012/144.
5. Gorantala, S. A General Purpose Transpiler for Fully Homomorphic Encryption / S. Gorantala и др. // arXiv preprint arXiv:2106.07893. — 2021.
6. Viand, A. SoK: Fully Homomorphic Encryption Compilers / A. Viand, P. Jattke, A. Hithnawi // Proceedings of Symposium on Security and Privacy. IEEE. — 2021.

7. Бабенко, Л.К. Обобщенная модель системы криптографически защищенных вычислений / Л.К. Бабенко, Ф.Б. Буртыка, О.Б. Макаревич, А.В. Трепачева // Известия ЮФУ. Технические науки. — 2015. — № 5. — С. 77-86.
8. Boura, C. CHIMERA: Combining Ring-LWE-based Fully Homomorphic Encryption Schemes / C. Boura, N. Gama, M. Georgieva, D. Jetchev // Journal of Mathematical Cryptology. — 2020. — № 1, Vol. 14. — С. 316-338.
9. Штейнберг, Б.Я. Особенности реализации распараллеливающих преобразований программ в системе ДВОР / Б.Я. Штейнберг и др. // Известия высших учебных заведений. Приборостроение. — 2011. — № 10. — С. 87-89.
10. Costache, A. Evaluating the effectiveness of heuristic worst-case noise analysis in FHE / A. Costache, K. Laine, R. Player // European Symposium on Research in Computer Security 2020. — С. 546-565.
11. K. Laine. Simple Encrypted Arithmetic Library 2.3.1. Microsoft Research.
12. P. Aubry, S, Carpov, R. Sirdey. Faster homomorphic encryption is not enough: improved heuristic for multiplicative depth minimization of Boolean circuits // Cryptographers' Track at the RSA Conference 2020. — С. 345-363.

Гельфанд А.М.,
Санкт-Петербургский Государственный Университет имени Профессора Михаила Александровича Бонч-Бруевича (СПбГУТ им. Проф. М.А. Бонч-Бруевича.).
Старший преподаватель кафедры Защищенных Систем Связи (ЗСС),
amgelfand@mail.ru

РАЗРАБОТКА МЕТОДИКИ АНАЛИЗА БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация:в работе выполняется исследование подсистем обеспечения безопасности объектов критической информационной инфраструктуры для разработки методики анализа уровня защищенности объектов критической информационной инфраструктуры. В работе разрабатывается типовая модель угроз на основе базовой модели согласно документации ФСТЭК. В работе исследуются модели и методы принятия решений в ходе создания и эксплуатации подсистем безопасности объектов критической информационной инфраструктуры
Ключевые слова: критические информационные инфраструктуры (КИИ), объект КИИ, субъект КИИ, риск, угроза, информационная безопасность, несанкционированный доступ**.**

Актуальность

Вопрос регулирования безопасности информационных ресурсов является крайне важным в настоящее время. Информационные технологии (ИТ) применяются практически в каждой отрасли. Следовательно, каждый день увеличивается количество атак на информационные ресурсы (ИР) и информационные системы (ИС) . Атаки на разные системы вызывают разные последствия. Атаки, направленные на кражу персональных данных конечных пользователей не представляют угрозу в глобальном смысле. Такие атаки можно профилактировать и предотвращать следуя указаниям специалистов в области информационной безопасности – устанавливать надежные пароли, не открывать неизвестные ссылки, не скачивать подозрительные вложения из электронных писем. Такие атаки нанесут вред финансовому благополучию конкретных граждан. Но существуют другие атаки, успешное проведение которых вызовет ряд проблем, связанных с национальной безопасностью. Удаленный вывод из строя оборудования на атомной электростанции или в городской больнице может понести непоправимые последствия, а также угрожать жизни людей.

В связи с этим был издан Федеральный Закон (ФЗ) о безопасности критической информационной инфраструктуры (КИИ) РФ. Закон регулирует обеспечение безопасности критически важных объектов. Закон излагает основы обеспечения безопасности объектов КИИ. Закон о КИИ охватывает различные сферы, а также определяет субъекты и объекты КИИ:

Субъект КИИ – гос. учреждение, гос. орган, индивидуальный предприниматель (ИП) или юридическое лицо, которому на законном основании принадлежат информационно-телекоммуникационные сети (ИТКС), информационные системы (ИС), автоматизированные системы управления (АСУ). АСУ, ИС и ИКТС функционируют энергетической, научной, транспортной сферах, , банковской сфере и сфере здравоохранения , а также сфере связи, в сферах финансового рынка, в области атомной энергии, топливно-энергетического комплекса (ТЭК), оборонной, ракетнокосмической, горнодобывающей, химической, металлургической промышленностей, юридические лица или индивидуальные предприниматели, ответственных за взаимодействие данных систем.

Актуальность темы обуславливается необходимостью обеспечить защиту каждой из перечисленных сфер. Халатность в обеспечении безопасности может повлечь за собой финансовые потери и человеческие жертвы. Каждая из областей требует детальной проработки. Но в рамках данного доклада рассматривается область информационно-телекоммуникационные сети (ИКТС) и непосредственно сети и информационные системы как объект КИИ.

Существуют нормативно-правовые акты, регулирующие безопасность, но они не затрагивают безопасность полностью. Необходимо провести исследование на предмет выявления рисков и оценку возможного ущерба. Для обеспечения безопасности необходимо определить нарушителя, угрозы, рассмотреть вектора атак, а также оценить риски и последствия от угроз.

Степень изученности темы

На данный момент тема является изучаемой. В данной сфере публикуются работы учеными-исследователями и федеральными органами, такие как МИНЦИФРЫ, ФСТЭК и ФСБ РФ.

В данном направлении работают такие известные ученые как

Цыгичко В.Н.,
Черешкин Д.С.,
Смолян Г.Л.

Объект исследования

подсистемы безопасности объектов КИИ

Предмет исследования

Модели и методы принятия решений в ходе создания и эксплуатации подсистем безопасности объектов критической информационной инфраструктуры

Цель работы

В качестве цели работы можно обозначить разработку методики отнесения организации к критическим информационным инфраструктурам в целом. В данную методику будут входить следующие аспекты а также определению критерия значимости.

Задачи работы

- Разработать типовую модель нарушителя;
- определить интерфейсы взаимодействия между объектом и нарушителем;
- исследовать способы выявления угроз нарушения информационной безопасности;
- разработать метод принятия решений на основе математического аппарата;
- оценить эффективность и экономическую целесообразность разработанных методов;
- разработать методику улучшения «Перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения». Для этого разработать формулу оценки ущерба;
- выполнить оценку защищенности объекта КИИ.

Структура работы

1. Разработка типовой модели угроз.

Актуальность

На данный момент существующие модели угроз информационной безопасности системы имеют весьма условный характер, этому характерно отсутствие единого принципа построения таких моделей. Существующим подходам присущи такие недостатки как: отсутствие однозначного определения модели угроз, существенная разница структур и принципов работы моделей, а также вариантов применения этой модели,. Наличие данных недостатков в имеющихся подходах отрицательно сказывается на качестве работы с самой моделью, а также на итоговом результате работы. Это обуславливается отсутствием итоговых стандартизованных оценок одной модели относительно другой модели угроз.

Суть

На основе базовой модели ФСТЭК и анализа процессов в построена типовая модель ОКИИ характерная для организаций, работающих в области телекоммуникаций.

Предложен методы ее адаптации к конкретным объектам.

Новизна

Типовая модель для данной области была разработана впервые.

Теоретическая значимость:

Типовая модель систематизирует виды и категории актуальных нарушителей и последовательности техник и тактик, применение которых может привести к реализации угрозы безопасности информации.

Практическая значимость

Типовая модель ОКИИ, позволяет определить границу оценки угроз безопасности информации и необходимые исходные данные, используемые в ходе выявления критических процессов и объектов, подлежащих категорированию

Типовая модель угроз безопасности в сфере телекоммуникаций и телекоммуникационных сетей.

Внутренние угрозы

- различные угрозы утечки по техническим каналам связи;
- угрозы несанкционированного доступа (НСД) по телекоммуникационным каналам (атака человек-по-середине).
- Угрозы НСД связанные с доступом к оборудованию в телекоммуникационных сетях (ТС) вызванные действиями нарушителя, имеющего доступ к телекоммуникационной сети, в том числе учитывая пользователей ТС, выполняющих угрозы непосредственно в самой ТС;

Угрозы из внешних сетей:

- Анализ сетевого трафика, перехват передаваемой информации во внешние сети и принимаемой информации из внешних сетей;
- перехват паролей для администрирования сетевых устройств и захват контроля;
- получение НСД (подмена доверенного объекта);
- Отказ в обслуживании;
- внедрение вредоносных программ по сети.

Построение модели угроз основано на элементарных информационных потоках (ЭИП) . Поток представлен на рис. 1

Рисунок 1 Графическое представление информационного потока

Где $ВП_i$ и $ВП_j$–множества носителей информации (вершины потока);
$КПИ_z$– множестваканалов передачи информации

Информационный поток описывается следующим образом (1)

$$эип = \{ВП_i, КПИ_z, ВП_j\} \quad (1)$$

Определение несанкционированного доступа (НСД) подразумевает появление нового элементав системе. Используя обозначенное ранее, дополним модель (рис. 2):

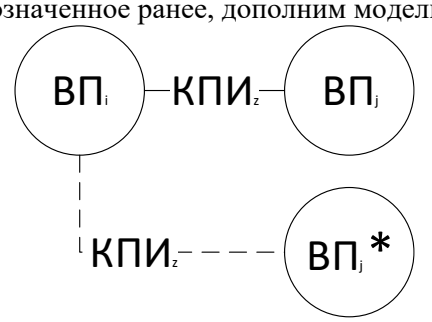


Рисунок 2 Появление элемента множества $ВП_j$*, который получает информацию незаконно из элемента $ВП_i$

Несанкционированный доступ ставит под угрозу целостность, конфиденциальность и доступность информации. В работе подробно рассматривается каждая из данных угроз, а также ее последствия.

2. Методика анализа рисков от происшествий различных категорий приметитесь для критериев значимости

Суть

На основе анализа критических процессов были оценённые риски и последствия от угроз. Был применен математический аппарат, проведено сравнение различных алгоритмов согласно теории рисков и выбран оптимальный алгоритм для поставленных задач.

Новизна:

Разработанная методика позволяет автоматизировать оценку ущерба на основании перечня ФСТЭК

Теоретическая значимость:

Методика устанавливает зависимость объектов и видов воздействия от нежелательных последствий, которые могут возникнуть при исполнении угроз безопасности информации.

Практическая значимость:

Разработанный позволяет ускорить процесс оценки ущерба от происшествий с различными параметрами за счет автоматизации.

Выбор оптимальной альтернативы по критериям

Если во всем множестве возможных решений есть одна альтернатива, которая абсолютно или по состояниям доминирует над всеми остальными, то она является оптимальной, и задача выбора решена.

Если среди множества возможных решений есть альтернатива, которая доминирует абсолютно или по состояниям хотя бы одной другой альтернативой, то доминируемую альтернативу можно исключить из рассмотрения, поскольку она точно не будут оптимальной.

Если после применения принципов доминирования осталось несколько эффективных альтернатив, значит оптимальное решение еще не найдено, и для его поиска требуется применять критерии выбора.

Для поиска оптимального решения по критериям необходимо:

1. отобрать критерии, для выполнения выборки;
2. произвести расчет значения выбранного критерия;
3. сравнить для всех альтернатив полученные значения критерия. Сравнение проводится между полученными результатами.

Оптимальной является альтернатива, которая имеет наилучшее значение критерия. Минимальное или максимальное значение будет считаться «Наилучшим» значение критерия и зависеть от следующих условий:

- вид критерия (максимальное или минимальное значение).
- исходы альтернатив (выигрыш, расходы, прибыл, убытки).

Для оценки риска успешного проведения атаки были выбраны 6 основных критериев:

- Вальда;
- «максимакс»;
- Лапласа;
- Сэвиджа;
- простой критерий Гурвица;
- критерий Гурвица обобщенный.

Данные критерии были применены к Перечню Постановления правительства Российской Федерации от 8 февраля 2018 г. N 127 "об утверждении правил категорирования объектов критической информационной инфраструктуры российской федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений" для автоматизации принятия решений.

Были смоделированы происшествия, повлекшие последствия социальной значимости (табл. 1).

Задача: автоматизировать принятие решений о выборе происшествия с самым негативным и самым не негативным исходом

Табл. 1. Происшествия.

Альтернативы (X_i)	**Состояние срреды (Y_j) Значение показателя**				
	Ущерб жизни и\или здоровью людей (измеряется в количестве человек)	Полное прекращение или частичное нарушение функционирования объектов обеспечения жизнедеятельности населения. Оценивается по численному количеству людей, а также по возможным нарушениям обычной жизнедеятельности людей (измеряется в количестве человек)	Полное прекращение или частичное нарушение функционирования инфраструктуры сферы транспорта. Оценивается по численному количеству людей, которым может быть отказано в доступе к транспортным услугам. (измеряется в количестве человек)	Полное прекращение или частичное нарушение функционирования сетей связи. Оценивается по количеству людей, которым может быть не предоставлен доступ к услугам связи. (измеряется в количестве человек)	Отсутствие доступа к государственной услуге. Оценивается в максимально допустимом промежутке времени, в течение которого государственная услуга может быть недоступна (измеряется в количестве часов)

1 X_A	**20**	**2000**	**3570**	**89**	**12**
2 **X_B**	**550**	**30000**	**9850**	**2550**	**5**
3 **X_C**	**100**	**2000**	**11420**	**30**	**23**
4X_D	**1000**	**6500**	**2575**	**25**	**14**
5 X_E	**63**	**6570**	**6972**	**685**	**7**

Среди данных происшествий нет доминирующих. Невозможно однозначно определить какое происшествие более серьезное. Поэтому решение придется принимать по критериям.

Рассмотрим данную задачу применив отобранные критерии.

Критерий Вальда

Оптимальная альтернатива обеспечивает наилучший исход из всех возможных альтернатив при самых негативных последствиях.

Порядок действий:

1) Находим для каждой альтернативы минимальные исходы - значение критерия Вальда
2) Сравниваем полученные значения критерия Вальда и находим максимальную величину.

Вариант с максимальным значением критерия является оптимальным. Лицо, принимающее решение, т.е. лицо осуществляющее выбор по данному критерию, гарантирует, что при самом плохом стечении обстоятельств исход не будет меньше, чем значение критерия.

Находим минимальные исходы для каждой альтернативы (табл 2).

Табл. 2. Расчёты по критерию Вальда

$W_A= \min(x_{1j}),j=1..5$	$W_A= \min(20,2000,3570,89,12)=12$
$W_B= \min(x_{2j}),j=1..5$	$W_B = \min(550,30000,9850,2550,5)=5$
$W_C= \min(x_{3j}),j=1..5$	$W_C= \min(100,2000,11420,30,23)=23$
$W_D= \min(x_{4j}),j=1..5$	$W_D= \min(1000,6500,2575,25,14)=14$
$W_E= \min(x_{5j}),j=1..5$	$W_E= \min(63,6570,6972,685,7)=7$

Сравниваем значения критерия Вальда и находим наибольшую величину. Искомая альтернатива - альтернатива с максимальным значением критерия.

$W_C>W_D>W_A>W_E>W_B=>X^*=X_C$

Согласно критерию Вальда значение X_C, т.е. происшествие 3 является искомым. Критерий учитывает количественный показатель, не основываясь на значимости показателей.

Вывод

Для оценки ущерба от происшествия на предприятии, относящемся к КИИ, при учете различным показателей критерий Вальда не подходит.

При оценке полученного результата невозможно однозначно утверждать, что данный исход является искомым, т.е. с минимальными последствиями от происшествия. Критерий не учитывает значимость показателей. Критерий учитывает лишь количественные показатели.

Критерий подходит для оценки ущерба в рамках одного показателя т.е. при оценке ущерба в рамках одного столбца

Критерий "Максимакс"

альтернатива с максимальным наибольшим исходом считается оптимальной.

Алгоритм действий:

1) Находим значение критерия «максимакс», т.е. максимальные исходы для каждой альтернативы.
2) Сравниваем найденные значения и расчитываем альтернативу с максимальной величиной критерия.

Получаем максимальные исходы для каждой альтернативы (табл. 3).

Табл. 3 Расчёты по критерию Максимакс

$W_A= \max(x_{1j}),j=1..5$	$W_A= \max(20,2000,3570,89,12)=3570$
$W_B= \max(x_{2j}),j=1..5$	$W_B = \max(550,30000,9850,2550,5)=30000$
$W_C= \max(x_{3j}),j=1..5$	$W_C= \max(100,2000,11420,30,23)= 11420$
$W_D= \max(x_{4j}),j=1..5$	$W_D= \max(1000,6500,2575,25,14)= 6500$
$W_E= \max(x_{5j}),j=1..5$	$W_E= \max(63,6570,6972,685,7)=6972$

Сравниваем найденные значения и определяем альтернативу с максимальной величиной критерия:

$M_B > M_C > M_E > M_D > M_A => X^* = X_B$

Согласно критерию Максимакс значение X_B, т.е. происшествие 2 является искомым. Критерий учитывает количественный показатель, не основываясь на значимости показателей.

Вывод

Для оценки ущерба от происшествия на предприятии области КИИ, при учете различных показателей, критерий Максимакс не подходит.

При оценке полученного результата невозможно однозначно утверждать, что данный исход является самым негативным, т.е. ущерб максимален. Критерий не учитывает значимость показателей. Критерий учитывает лишь количественные показатели.

Критерий подходит для оценки ущерба в рамках одного показателя т.е. при оценке ущерба в рамках одного столбца

Критерий Лапласа

Для оценки альтернатив используем среднее арифметическое значение. Оптимальной считаем альтернативу где среднее значение максимально.

Порядок действий:

1. Рассчитываем значение критерия Лапласа вычисляя среднее арифметическое исходов для каждого происшествия;
2. ищем альтернативу с максимальным значением. сравнивая рассчитанные величины между собой.

Находим среднее арифметическое значение исходов по каждому событию.

LA=(x11+x12+x13+x14+x15)/5=(20+2000+3570+89+12)/5=1138,2

LB=(x21+x22+x23+x24+x25)/5=(550+30000+9850+2550+5)/5=8591

LC=(x31+x32+x33+x34+x35)/5=(100+2000+11420+30+23)/5=2714,6

LD=(x41+x42+x43+x44+x45)/5=(1000+6500+2575+25+14)/5=2022,8

LE=(x51+x52+x53+x54+x55)/5=(63+6570+6972+685+7)/5=2859,4

LB> LE > LC> LD > LA => X*= LB

Критерий подходит для оценки ущерба в рамках одного показателя т.е. при оценке ущерба

Критерий Сэвиджа

Оценка альтернатив производится по «матрице рисков». Величина «риска» равна разнице между тем, что обеспечивает данная альтернатива, и максимальным значением при данном состоянии.

Значение критерия Сэвиджа для альтернативы соответствует ее наибольшему «риску» («сожалению»).Риск (сожаление) показывает величину, теряемую при принятии неверного решения.

Альтернатива с минимальным наибольшим «риском» оптимальна.

Порядок действий:

1) определяем максимальное значение для каждого столбца матрицы при данном сценарии;
2) ищем разницу между максимальным (при данном сценарии) и для каждой клетки исходной матрицы исходом в рассматриваемой ячейке;
3) составляем матрицу рисков из полученных значений;
4) Выполняем оценку данной альтернативы по критерию Сэвиджа, т.е. определяем максимальный риск для каждой альтернативы в новой матрице найти наибольший возможный вариант;
5) Сравниваем полученные величины и выбираем альтернативу с минимальным риском.

В данном случае рассчитываем оценку ущерба от происшествия. Ищем происшествие с максимально неблагоприятным исходом. т.е. в нашем случае "выигрышное" состояние будет максимально неблагополучным и отрицательным.

Рассчитываем наибольшую величину для каждого исхода

Y1=max(x11, x21, x31, x41, x51) = max (20,550,100,1000,63)=1000

Y2=max(x12, x22, x32, x42, x52) = max(2000, 30000,2000,6500,6570)=30000

Y3=max(x13, x23, x33, x43, x53) = max(3570,9850,11420,2575,6972)=11420

Y4=max(x14, x24, x34, x44, x54) = max(89,2550,30,25,685)=2550

Y5=max(x15, x25, x35, x45, x55) = max(12,5,23,14,7)=23

Рассчитываем значения «риска» («сожаления») для каждого происшествия при каждом сценарии.

Для происшествия 1 (X_A)

r11=y1-x11=980
r12=y2-x12=29450
r13=y3-x13=11320
r14=y4-x14=1550
r15=y5-x15=-40
Для происшествия 2 (X_B)
r21=y1-x21=-1000
r22=y2-x22=0
r23=y3-x23=9420
r24=y4-x24=-3950
r25=y5-x25=23-14=9
Для происшествия 3 (X_C)
R31=y1-x31=-2570
r32=y2-x32=20150
r33=y3-x33=0
r34=y4-x34=-25
r35=y5-x35=-6949

Для происшествия 4 (X_D)
r41=y1-x41=911
r42=y2-x42=27450
r43=y3-x43=11390
r44=y4-x44=2525
r45=y5-x45=-662

Для происшествия 5 (X_E)
r51=y1-x51=988
r52=y2-x52=29995
r53=y3-x53=11397
r54=y4-x54=2536
r45=y5-x45=16
Составляем из полученных значений «матрицу рисков» (табл.4)

Максимальный показатель y_j при j-сценарии	1000	30000	11420	2550	23
1 X_A	980	29450	11320	1550	-40	29450
2 X_B	-1000	0	9420	-3950	-6547	9420
3 X_C	-2570	20150	0	-25	-6949	20150
4 X_D	911	27450	11397	2525	-662	27450
5 X_E	988	29995	11397	2536	16	29995

Табл. 4 Матрица рисков.

Альтернативы (X_i)	**Состояние среды (Y_j)** **Значение показателя**					**Максимальный риск Si**
	Ущерб жизни и\или здоровью людей (измеряется в количестве человек)	Полное прекращение или частичное нарушение функционирования объектов обеспечения жизнедеятельности населения. Оценивается по численному количеству людей, а также по возможным нарушениям обычной жизнедеятельности людей (измеряется в количестве человек)	Полное прекращение или частичное нарушение функционирования инфраструктуры сферы транспорта. Оценивается по численному количеству людей, которым может быть отказано в доступе к транспортным услугам. (измеряется в количестве человек)	Полное прекращение или частичное нарушение функционирования сетей связи. Оценивается по количеству людей, которым может быть не предоставлен доступ к услугам связи. (измеряется в количестве человек)	Отсутствие доступа к государственной услуге. Оценивается в максимально допустимом промежутке времени, в течение которого государственная услуга может быть недоступна (измеряется в количестве часов)	
Максимальный показатель yj при j-сценарии	1000	**30000**	11420	2550	23	
1 X_A	**980**	**29450**	**11320**	**1550**	**-40**	**29450**
2 **X_B**	**-1000**	**0**	**9420**	**-3950**	**-6547**	**9420**
3 **X_C**	**-2570**	**20150**	**0**	**-25**	**-6949**	**20150**
4 **X_D**	**911**	**27450**	**11397**	**2525**	**-662**	**27450**
5 X_E	**988**	**29995**	**11397**	**2536**	**16**	**29995**

В новой матрице по каждой строке находим наибольшую величину «риска» для каждого происшествия. Это значение - оценка данной альтернативы по критерию Сэвиджа.

S_A=30000
S_B=29450
S_C=20150
S_D=27450

S_E=29995

Сравним полученные значения и находим проект с минимальным значением критерия

$S_B > S_C > S_A > S_E$

$X^* = X_E$

Согласно критерию Сэвиджа происшествие X_E будет являться происшествием с минимальными потерями.

Вывод

Критерий Сэвиджа удовлетворяет требованиям поставленной задачи. Происшествие с данными параметрами действительно считается самым благоприятным.

Достоинства критерия Сэвиджа: оценка показателей в рамках происшествия. Задачей стояло выявить происшествие с минимальным ущербом.

Недостаток: критерий не учитывает важность отдельно взятых параметров. Требуется доработать и прийти к усредненным показателям. рамках одного столбца

Критерий Гурвица

В обобщенном критерии Гурвица, в отличие от обычного, учитываются не только крайние а все возможные исходы. «удельный вес» присваивается всем исходам. Пессимисту присущ принцип чем хуже исход, тем больше вес, оптимист руководствуется противоположным значением. Сумма исходов является значением обобщенного критерия Гурвица. Расчет выполняется по удельным весам.

Расчет обобщенного критерия для i-й альтернативы выполняется следующим образом (2):

$$H_i' = \sum_{q=1}^{M} \lambda_q x_{iq} \quad (2)$$

где λ_q – коэффициент для q-го значения i-й альтернативы,

Необходимо соблюдать следующие условия при назначении коэффициентов:

а) величины коэффициентов должны отражать отношение лица, принимающего решения, к риску:

• «оптимист» ищет лучшие исходы. Исходы должны иметь больший «вес». Чем лучше исход, тем больше «вес»;

• «пессимист» ищет больший «вес» у худших исходов. Чем хуже исход – тем больше «вес».

При этом каждый коэффициент должен быть не больше единицы и больше нуля:

б) итоговая сумма есовых коэффициентов равняется единице (3):

$$\sum_{q=1}^{M} \lambda_q = 1 \quad (3)$$

Другими словами $\lambda_1 + ... + \lambda_q + ... + \lambda_M = 1$

Порядок действий:

1. Отсортировать матрицу таким образом, чтобы исходы каждой альтернативы находились в порядке возрастания.
2. Вычислить суммы исходов по каждой колонке «новой» матрицы Y(4):

$$y_q = \sum_{i=1}^{N} y_{iq} \quad (4)$$

3. Вычисляем сумму всех исходов матрицы (5):

$$y = \sum_{i=1}^{N} \quad \sum_{q=1}^{M} y_{iq} = \sum_{q=1}^{M} y_q \quad (5)$$

4. Выбираем в зависимости от отношения к неопределенности лица, принимающего решение, коэффициенты λ_q.

- а) для «Оптимиста» по формуле определяем коэффициент λ_q для любой q-й коллонки (6):

$$\lambda_q = \frac{y_q}{y} \quad (6)$$

- б) для «Пессимиста» зеркально меняем местами коэффициенты, вычисленные для «оптимиста»:

5. Рассчитываем величину обобщенного критерия Гурвица для каждой i-й альтернативы(7):

$$H_i' = \sum_{q=1}^{M} \lambda_q x_{iq} = \lambda_1 y_{i1} + \lambda_{21} y_{i2} + .. + \lambda_M y_{iM} \quad (7)$$

Стратегия, у которой значение обобщенного критерия Гурвица наибольшее, является оптимальной.

Выбранный критерий:Критерий Гурвица. Благодаря возможности использования λ коэффициентов можно подобрать такие коэффициенты, которые уравнивают показатели значимости между собой. То есть не будет возникать ошибка несоответствия. При правильном выборе коэфффициентов можно уравнять показатели значимости между собой.

3. Методика распределения ресурсов подсистем безопасности

4. Методика оценки эффективности принятых организационных и технических мер ОКИИ

Суть:

Разработка методики оценки эффективности принятых мер по обеспечению безопасности ОКИИ

Новизна:

В отличие от известных методик конкретизированы критерии оценки эффективности защиты информации.

Апробация

1. Свидетельство о государственной регистрации программы для ЭВМ № 2022613440 Российская Федерация. Программное обеспечение по реализации стеганографических методов при передаче сообщения : № 2022612582 : заявл. 24.02.2022 : опубл. 14.03.2022 / А. В. Красов, А. М. Гельфанд, П. И. Шариков, А. И. Катасонов ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича». – EDN MLCKWP.

2. Свидетельство о государственной регистрации программы для ЭВМ № 2021669969 Российская Федерация. Система электронного документооборота : № 2021669214 : заявл. 26.11.2021 : опубл. 06.12.2021 / А. М. Гельфанд, А. И. Пешков, И. И. Фадеев, Н. Н. Лансере ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича». – EDN JOWFST.

3. Гельфанд, А. М. Краткий анализ российских и зарубежных банков уязвимостей / А. М. Гельфанд, А. А. Ложкина // Технологии информационного общества : Сборник трудов XV Международной отраслевой научно-технической конференции «Технологии информационного общества», Москва, 03–04 марта 2021 года. – Москва: ООО "Издательский дом Медиа паблишер", 2021. – С. 153-155. – EDN LZQTVF.

4. Интернет вещей (IoT): угрозы безопасности и конфиденциальности / А. М. Гельфанд, А. А. Казанцев, А. В. Красов, В. Р. Уляшева // Актуальные проблемы инфотелекоммуникаций в науке и образовании : сборник научных статей: в 4х томах, Санкт-Петербург, 24–25 февраля 2021 года / Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2021. – С. 215-220. – EDN TFJJHA.

5. Свидетельство о государственной регистрации программы для ЭВМ № 2020617705 Российская Федерация. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры : № 2020616731 : заявл. 29.06.2020 : опубл. 10.07.2020 / А. В. Красов, А. М. Гельфанд, И. И. Фадеев, А. А. Казанцев ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ). – EDN NKWPHE.

6. Оценка рисков и угроз безопасности в среде "умный дом" / А. М. Гельфанд, А. А. Казанцев, А. В. Красов, Г. А. Орлов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020) : IX Международная научно-техническая и научно-методическая конференция : сборник научных статей, Санкт-Петербург, 26–27 февраля 2020 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2020. – С. 316-321. – EDN HIGZYQ.

7. Исследование распределенного механизма безопасности для устройств Интернета вещей с ограниченными ресурсами / А. М. Гельфанд, А. А. Казанцев, А. В. Красов, Г. А. Орлов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020) : IX Международная научно-техническая и научно-методическая конференция : сборник научных статей, Санкт-Петербург, 26–27 февраля 2020 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2020. – С. 321-326. – EDN GYBXPT.

8. Орлов, Г. А. Применение BigData при анализе больших данных в компьютерных сетях / Г. А. Орлов, А. В. Красов, А. М. Гельфанд // Наукоемкие технологии в космических

исследованиях Земли. – 2020. – Т. 12. – № 4. – С. 76-84. – DOI 10.36724/2409-5419-2020-12-4-76-84. – EDN RQQTOQ.

9. Организация концептуальной модели критической информационной инфраструктуры / А. М. Гельфанд, Н. Н. Лансере, А. А. Ложкина, И. И. Фадеев // Методы и технические средства обеспечения безопасности информации. – 2020. – № 29. – С. 39-40. – EDN PYPOHZ.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 26 июля 2017 г. N 187-ФЗ"О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ (последняя редакция)
2. Федеральный закон от 26 мая 2021 г. N 141-ФЗ «О внесении изменений в кодекс российской федерацииоб административных правонарушениях»
3. Федеральный закон от 26 июля 2017 г. N 193-ФЗО внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием федерального закона «О безопасности критической информационной инфраструктурыРоссийской Федерации»
4. Указ президента Российской Федерации О внесении изменения в перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203
5. Указ президента Российской Федерации о внесении изменений в положение о федеральной службе по техническому и экспортному контролю, утвержденное указом президента российской федерации от 16 августа 2004 г. N 1085
6. Постановление правительства Российской Федерацииот 24 декабря 2021 г. № 2431 «О внесении изменений в Правила категорирования объектов критической информационной инфраструктурыРоссийской Федерации»
7. Постановление правительства Российской Федерации от 24 декабря 2021 г. № 2431 «О внесении изменений в Правила категорирования объектовкритической информационной инфраструктурыРоссийской Федерации»
8. Цыгичко, В. Н. Безопасность критических инфраструктур / В. Н. Цыгичко, Д. С. Черешкин, Г. Л. Смолян. – Москва : КРАСАНД, 2018. – 200 с. – EDN YMIPAT.
9. Цыгичко, В. Н. Оценка рисков нарушения безопасности критически важных объектов и критических инфраструктур / В. Н. Цыгичко // Проблемы анализа риска. – 2016. – Т. 13. – № 5. – С. 6-10. – EDN WZJMFV.
10. Николаев, Н. С. Управление информационной безопасностью : Учебник / Н. С. Николаев. – Москва : Общество с ограниченной ответственностью "Издательство "КноРус", 2021. – 190 с. – (Бакалавриат). – ISBN 978-5-406-07325-4. – EDN EWDCBL.
11. Прикладные цифровые технологии и системы XXI века: экономика, менеджмент, управление персоналом, информационная безопасность, право : Материалы региональной научно-практической конференции, Владимир, 17 декабря 2021 года. – Владимир: Владимирский филиал федерального государственного бюджетного образовательного учреждения высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации", 2022. – 194 с. – ISBN 978-5-907389-41-0. – EDN QOWYOG.
12. Фомин, Д. В. Информационная безопасность : Учебное пособие для СПО / Д. В. Фомин. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. – 218 с. – ISBN 978-5-4488-1351-1. – EDN MIRNCC.
13. Келдыш, Н. В. Информационная безопасность. Защита информации на объектах информатизации / Н. В. Келдыш. – Москва : Общество с ограниченной ответственностью "Издательство "Мир науки", 2022. – 260 с. – ISBN 978-5-907603-01-1. – EDN OMREPL.
14. Информационная безопасность как элемент национальной безопасности, Нижний Новгород, 25 апреля 2022 года. – Нижний Новгород: Нижегородская академия Министерства внутренних дел Российской Федерации, 2022. – 107 с. – EDN UWPKWM.
15. Информационная безопасность и защита персональных данных. Проблемы и пути их решения : Материалы XIII Межрегиональной научно-практической конференции, Брянск, 30 апреля 2021 года. – Брянск: Брянский государственный технический университет, 2021. – 300 с. – ISBN 978-5-907570-12-2. – EDN GSNHQB.
16. Информационная безопасность: влияние пандемии COVID-19, Москва, 20 мая 2021 года. – Москва: Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, 2021. – 340 с. – ISBN 978-5-9228-2468-2. – EDN KDVQAY.

Дорофеев К.А.
ФГБОУ ВО «ЧелГУ», старший преподаватель
кафедры компьютерной безопасности
и прикладной алгебры ЧелГУ,
Kostuan1989@mail.ru

МЕТОДЫ И АЛГОРИТМЫ АУТЕНТИФИКАЦИИ ПО ТРЁХМЕРНЫМ МОДЕЛЯМ ЛИЦ НА ОСНОВЕ ГЛУБОКИХ НЕЙРОННЫХ СЕТЕЙ

Аннотация: Аутентификация человека по трёхмерной модели лица – одна из наиболее важных и перспективных задач компьютерного зрения, как с теоретической, так и с практической точки зрения. В настоящее время существуют системы распознавания человека по лицу, однако они имеют недопустимо большую ошибку в неконтролируемых условиях. Цель данного проекта – разработка надёжной системы биометрической аутентификации по трёхмерной модели лица, заданной облаком точек в трёхмерном пространстве, с помощью глубоких нейронных сетей с учётом сложных внешних факторов, искажений, шума. В рамках проекта будут исследованы особенности биометрических систем аутентификации, а также подходы к их улучшению, предобработки данных, будут разработаны и реализованы новые методы и алгоритмы выбора признаков с использованием глубокой нейронной сети. Запланированные результаты будут соответствовать мировому уровню исследований. Результаты проведенных исследований могут быть использованы в различных существующих, а также вновь создаваемых системах аутентификации, в социальных, научных и инженерных приложениях, где требуется автоматическая обработка биометрических данных. Потребителями созданного интеллектуального продукта могут стать:

- Государственные органы, заинтересованные в обеспечении безопасности на основе биометрических технологий.
- Частные компании и предприниматели, использующие биометрические технологии.

Ключевые слова: информационная безопасность, биометрия, нейронные сети, распознавание лиц, глубокое обучение, аутентификация.

Актуальность исследования.

Одной из крайне актуальных задач информационной безопасности является разработка систем биометрической аутентификации. Интерес к ее решению обусловлен высокими финансовыми потерями от угрозы несанкционированного доступа, а также от действий киберпреступников по всему миру.

Аутентификация человека по лицу – одна из наиболее важных современных задач компьютерного зрения и робототехники, как с теоретической, так и с практической точек зрения. Существующие в настоящее время системы некооперативного и автоматического распознавания человека по лицу в неконтролируемых условиях имеют недопустимо большую ошибку.

Проект посвящен решению проблемы повышения надежности биометрической аутентификации по трехмерному лицу с помощью глубоких нейронных сетей в зависимости от таких факторов, как возрастные изменения человека, мимические экспрессии, изменения в обучающей выборке, существенное изменение масштаба изображений, неравномерное освещение, частичное перекрытие человека посторонними предметами.

Анализ современного состояния исследований (степень разработанности темы).

За последние годы достигнуты значительные успехи в решении задачи распознавания человека по двумерному и трехмерному изображению лица благодаря применению нейронных сетей глубокого обучения с тремя и более слоями [1-9], которые объединяют в себе как выбор и расчет признаков, так и классификацию. Точность методов глубокого обучения при большом количестве слоев (от 10 до 22) и при очень большой обучающей выборке (миллионы образцов) на некоторых известных базах данных, таких как Labelled Faces in the Wild [10] (LFW) превысила точность распознавания человеком и достигла 99.6% [6-8]. В рамках проекта были проведены предварительные исследования по распознаванию лиц по двумерным изображениям с помощью трехслойной сверточной нейронной сети [11], однако для достижения высокого качества распознавания необходимо существенное увеличение обучающей выборки и вычислительных затрат. Для реальных приложений качественное распознавание субъекта с помощью сверточных нейронных сетей глубокого обучения затруднительно из-за ограниченности времени для обучения системы, а также из-за отсутствия больших обучающих выборок.

Для достижения высокой точности и надежности идентификации человека на динамических сценах в реальных условиях использование алгоритмов трехмерного распознавания лиц является перспективным, так как алгоритмы являются инвариантными к изменению освещения, а идентификация личности может быть проведена с разных углов обзора. Алгоритмы трехмерного распознавания используют информацию о форме лица для идентификации отличительных признаков, таких как контур глазниц, носа и подбородка. Однако деформации формы лица при мимических экспрессиях ухудшают качество распознавания [12]. Трехмерное изображение человеческого лица является гораздо более информативным, чем соответствующая двумерная проекция. Из-за сложной топологии формы лица при его динамическом трехмерном описании часто используется деформируемая модель лица [13-16]. С помощью данной модели можно параметрически описать мимические экспрессии человека, и, как следствие, улучшить качество идентификации человека.

Качество алгоритмов трехмерного распознавания напрямую зависят от точности построения трехмерной модели формы лица человека с помощью регистрации в трехмерном пространстве облаков точек, получаемых от датчиков глубины [17, 18]. Традиционный алгоритм регистрации решает вариационную задачу поиска оптимального геометрического (ортогонального или аффинного) преобразования, который наилучшим образом совмещает два облака точек с заданным соответствием между точками [19]. Выбор вида функционала в задаче оптимизации приводит к различным методам регистрации облаков точек. Наиболее используемыми являются поиск соответствия между парой облаков - точка-точка (point-to-point) и поиск соответствия – точка-плоскость (point-to-plane). Для класса ортогональных преобразований для задачи точка-точка решение в явном виде представлено в классических работах Хорна [20, 21]. Точное решение задачи точка-точка для случая произвольного аффинного преобразования приведено в работе [22]. Вариационная задача точка-плоскость в классе ортогональных преобразований решается с применением итерационного алгоритма Левенберга-Марквардта или методом линеаризации для малых углов [23]. Для вариационной задачи точка-плоскость в классе аффинных преобразований участниками проекта найдено точное решение [24]. В работе [25] получено приближенное решение задачи точка-плоскость в классе ортогональных преобразований.

Отметим, что метод точка-плоскость является более робастным к шуму датчиков, но для этого метода для класса ортогональных преобразований решение задачи в явном виде пока не найдено. Это усложняет применение метода в задачах, где требуется производить регистрацию в масштабе реального времени. В работе [26] представлен алгоритм динамической регистрации облаков точек, используемый для поиска соответствия между деформируемыми поверхностями. Метод предусматривает разбиение поверхностей на участки, каждый из которых обрабатывается отдельно, а способ объединения результатов регистрации основан на минимизации функционала.

Как показали предварительные результаты исследований в рамках данного проекта, использование трехмерной карты окружающего пространства [27,28] существенно улучшает качество распознавания и локализации субъектов на динамических, контекстуально сложных сценах, особенно при частичном или полном закрытии субъектов посторонними предметами. Несмотря на то, что качество карты глубины, получаемое от Kinect-камеры, в целом хорошее, существуют проблемы с выходной информацией. Так в выходных данных образуются области неопределенности из-за того, что структурированный свет излучения после отражения не попадает на камеру, разрешающая способность измерения глубины сцены падает по квадратичному закону с увеличением глубины сцены [29], а также из-за того, что быстрое движение камеры приводит к потере данных.

Для повышения точности распознавания лиц с использованием векторов признаков (дескрипторов) для предварительного обучения сверточных нейронных сетей на внешних наборах данных применяются различные методы регуляризации. Например, для того, чтобы дескрипторы каждого класса образовывали гиперсферу в многомерном пространстве, был предложен метод center loss [30]. Дескрипторы FaceNet [31] обучаются с помощью минимизации специальной функции потерь (triplet loss), которая приводит к тому, что расстояния между дескрипторами одного человека становятся меньше расстояний между дескрипторами различных людей. Кроме того, в последнее время появились функции потерь, основанные на максимизации зазора между углами, образованными извлекаемыми векторами признаками различных классов, такие как ArcFace [32]. В то же время на практике замечено, что наиболее точные результаты распознавания лиц получаются с помощью дескрипторов СНС, обученных с помощью оптимизации традиционной функции потерь (softmax loss), если использовать высококачественную большую внешнюю базу данных лиц, такую как VGGFace-2 [33].

Была произведена количественная оценка точности модели, устойчивости к внешним искажающим факторам, таким как неравномерное и слабое освещение, а также к подвижности человека [34,35]. Для нежесткой математической модели лица, то есть когда лицо подвижно, и его форма может деформироваться, предложен метод построения плотной трехмерной математической модели формы лица по набору изображений и карт глубины, снятых с помощью трех Kinect-камер. Реализована система объединения данных с Kinect-камер с использованием модифицированного алгоритма совмещения ICP по динамическому набору облаков точек [36].

Была проанализирована точность реконструкции трехмерного объекта при прямой фильтрации облаков точек [37]. Были сравнены различные алгоритмы фильтрации облаков точек с точки зрения точности восстановления трехмерных объектов с использованием реальных данных от камер глубины. Был предложен алгоритм каскадной фильтрации облаков точек, который дает лучший результат с точки зрения ошибки восстановления по сравнению с известными алгоритмами фильтрации облаков точек [37].

Цели и задачи работы.

Главной целью проекта является разработка и реализация надежной системы биометрической аутентификации по трехмерному лицу с помощью глубоких нейронных сетей.

Задачи научного исследования:

1.Построение трехмерной модели формы лица с использованием алгоритмов регистрации в трехмерном пространстве облаков точек, получаемых от датчиков глубины.

2.Реализация алгоритмов, учитывающих трехмерную карту окружающего пространства, для сегментирования и локализации лица.

3.Разработка и реализация методов предобработки данных для устранения шума и восстановления данных с использованием двумерного и трехмерного подхода.

4.Разработка и реализация алгоритмов для надежного распознавания лица с использованием трехмерной модели формы лица на основе глубокой нейронной сети.

Научная новизна.

Новизна научного исследования состоит в решении перспективных задач исследования:

1.Реализация алгоритмов построения трехмерной модели формы лица.

2.Реализация алгоритмов сегментирования и локализации лица.

3.Разработка и реализация новых алгоритмов для устранения шума и восстановления двумерных и трёхмерных данных.

4.Разработка и реализация новых эффективных алгоритмов надежного распознавания лиц на основе двумерных, трёхмерных данных, а также на основе гибридного подхода.

Теоретическая и практическая значимость работы.

Запланированные результаты проекта будут соответствовать мировому уровню исследований, поэтому предполагается регулярная презентация и обсуждение результатов на международных конференциях по биометрической аутентификации и обработке изображений. Результаты также будут опубликованы в соответствующих тематических журналах, включённых в список Web of Science и SCOPUS.

1.Будет реализован алгоритм построения трехмерной модели формы лица.

2.Будут разработаны и реализованы новые алгоритмы выбора признаков с использованием глубокой нейронной сети для обеспечения высокой информативности с низкой внутриклассовой и высокой межклассовой вариативностью.

3.Будут разработаны и реализованы новые методы устранения шума и восстановления двумерных и трёхмерных данных. Будет проведен сравнительный анализ по качеству восстановления исходной функции с известными методами.

4.Будут разработаны и реализованы новые методы распознавания человека с сильными мимическими экспрессиями на динамических сценах с использованием трёхмерных моделей лица.

Конечные результаты проекта могут быть использованы в таких социальных, научных и инженерных приложениях, где требуется автоматическая обработка биометрических данных в реальном времени, например, при создании роботизированных систем безопасности и спасения людей на основе методов распознавания личности на расстоянии в реальных погодных условиях. Также потенциальными потребителями проекта могут стать государственные органы и частные компании, использующие биометрические технологии.

Методология и методы исследования.

Для разработки системы аутентификации по трёхмерному лицу с применением глубоких нейронных сетей с качеством распознавания близким к возможностям человека будут разработаны новые математические модели и алгоритмы, включающие в себя предобработку изображений и облаков точек, выбор признаков и классификацию. Выбор признаков будет проводиться автоматически.

Первая проблема, которую необходимо решить – это использование глубокого обучения при относительно небольшом объеме данных. Предполагается увеличить объём данных с использованием генеративных состязательных сетей (Generative Adversarial Networks) для синтеза новых изображений на основе уже существующих базы данных. Кроме того, геометрические преобразования над существующими изображениями также помогут искусственно увеличить обучающую выборку.

Кроме того, нужно решить следующие подзадачи:

1.Разработка алгоритма нормализации изображений.

2.Разработка новых методов и алгоритмов выбора признаков, используя методы глубокого обучения, например, автокодировщики, для обеспечения высокой информативности с низкой внутриклассовой и высокой межклассовой вариативностью.

3.Разработка алгоритмов поиска соответствия изображений и архитектуры глубоких сверточных нейронных сетей для классификации изображений. Ожидается, что разрабатываемая система обработки, анализа и классификации лиц, обеспечит качество распознавания близкое к возможностям человека.

Для решения задачи построения трёхмерной модели формы лица при небольших изменениях формы будут использоваться специальные методы. Регистрация облаков точек на сетке поверхности может быть выполнена с помощью множества алгоритмов регистрации по отдельным участкам, а объединение результатов регистрации произведено путем минимизации функционала ошибки, который учитывает геометрические ошибки регистрации на сетке поверхности.

Ожидается, что на основе трёхмерной модели лица будут разработаны эффективные алгоритмы для надежного распознавания с небольшими изменениями формы лица вследствие мимических экспрессий на динамических сценах, искаженных реальными помехами различной природы.

Для реализации метода построения точной трёхмерной карты окружающего пространства с использованием последовательностей разреженных облаков точек, получаемых от датчиков глубины, для динамичных, контекстуально-сложных и крупномасштабных сцен будет разработан алгоритм регистрации облаков точек с произвольным пространственным разрешением и масштабом относительно друг друга.

В качестве предобработки данных предполагается разработать принципиально новые методы устранения шума и восстановления двухмерных и трёхмерных данных, в частности с помощью применения морфологических фильтров (2D) и фильтров обработки облаков точек (3D).

Положения, выносимые на защиту.

Основные результаты по части предобработки данных:

- Разработан и реализован новый переключающийся морфологический алгоритм фильтрации данных глубины (depth map). Также реализованы многочисленные известные алгоритмы фильтрации данных глубины, проведён сравнительный анализ качества фильтрации в терминах среднеквадратичной ошибки и метрики Хаусдорфа, а также в точности трёхмерной реконструкции и скорости применения фильтров.

- Исследовано влияние фильтрации данных глубины и облаков точек на точность реконструкции трёхмерных моделей лиц, а также на точность существующих систем распознавания лиц, основанных на глубоких нейронных сетях.

Результаты по части алгоритмов распознавания на основе глубоких нейронных сетей:

- Исследовано влияние прунинга и квантизации глубоких свёрточных сетей на точность и скорость работы систем распознавания лиц, в том числе при использовании на мобильных устройствах.

- Разработан и реализован алгоритм гибридного подхода с использованием глубоких свёрточных сетей, в том числе с множественными входами и смешанными данными.

Апробация результатов.

Все положения, выносимые на защиту, а также дополнительные результаты исследований опубликованы в соответствующих тематических журналах, включённых в список Web of Science и SCOPUS. Список публикаций:

- Accuracy analysis of 3D object shape recovery using depth filtering algorithms // Proceedings of the SPIE. – 2018. – Vol. 10752, id. 1075221. - 10 pp.

- A switching morphological algorithm for depth map recovery // In: et al. Analysis of Images, Social Networks and Texts. AIST. Springer. Lecture Notes in Computer Science. - 2019. - vol. 11832.

- 3D face recognition using depth filtering and deep convolutional neural network // Proceedings of the SPIE. Applications of Digital Image Processing XLII. - 2019. - vol. 11137.

- Accuracy analysis of 3D object reconstruction using point cloud filtering algorithms // Information Technology and Nanotechnology. - 2019.

- Design of autonomous mobile systems for face recognition based on a DCNN with compression and pruning // Proceedings of the SPIE. Applications of Digital Image Processing XLIII. - 2020. - vol. 11510

- Сравнительный анализ уязвимостей биометрических систем распознавания лиц // Вестник УрФО. Безопасность в информационной сфере. - 2022. - № 3 (статья на этапе публикации).

- Гибридный подход к реализации надёжных биометрических систем распознавания лиц (статья на этапе рецензирования).

Содержание диссертации.

Во введении обосновывается актуальность выбранной темы диссертационного исследования, приводится степень её разработанности, результаты предыдущих исследований, определяются цели и задач работы, выбирается предмет и объект исследования. Формулируются положения, выносимые на защиту.

Рассматриваются нюансы трёхмерной реконструкции объектов и сцен (Рис. 1-2).

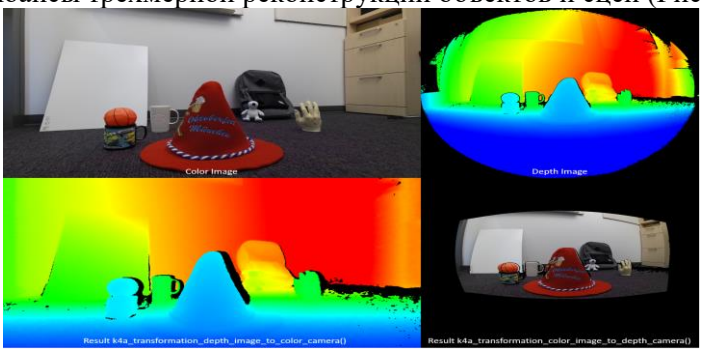


Рис. 1. Пример изображения с RGB-D датчика.

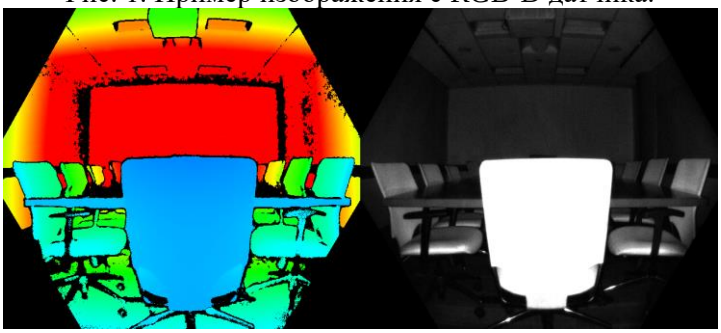


Рис. 2. Пример изображения с проблемными областями в карте глубины.

Приводятся основные технологии получения данных глубины, перечисляются плюсы и минусы каждой из технологий, производится сравнение современных датчиков. Рассматриваются проблемы и актуальные задачи информационной безопасности, приводится сравнительный анализ современных подходов к построению биометрических систем, способы защиты от предъявления поддельных лиц, распечатанных фотографий, масок, сгенерированных данных и прочее (Рис. 3-5).

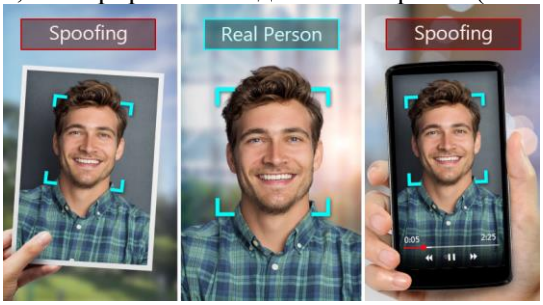


Рис. 3. Примеры атак с использованием распечатанной фотографии и с помощью визуализации изображения.

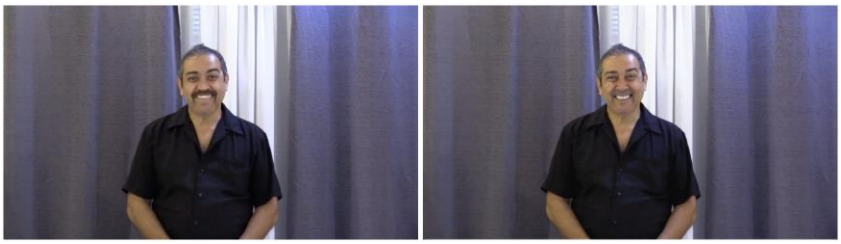


Рис. 4. Пример применения deepfake технологии (настоящее и сгенерированное изображения).

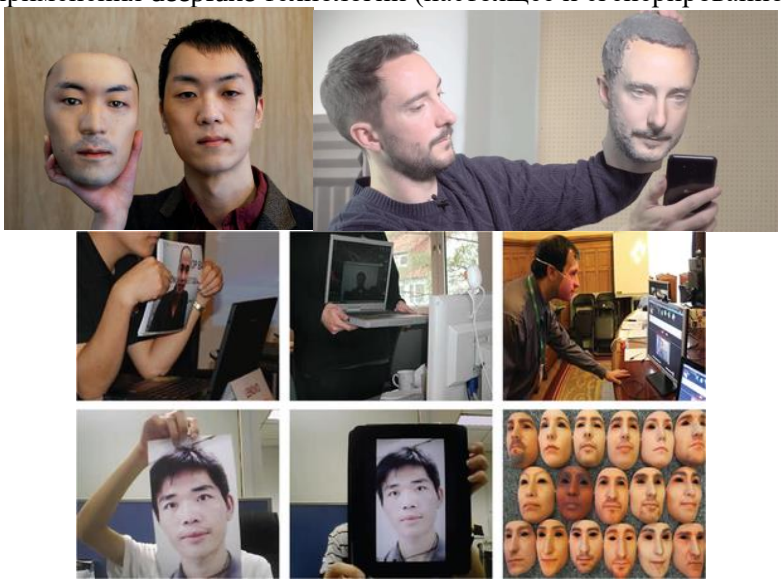


Рис. 5. Примеры напечатанных на трёхмерном принтере масок и примеры атак.

В первой главе приводятся полученные результаты по части предобработки данных (как двумерных, так и трёхмерных). Описывается разработанный и реализованный переключающийся морфологический алгоритм фильтрации данных глубины. Также приводятся результаты исследования влияния фильтрации трёхмерных облаков точек на точность реконструкции трёхмерных объектов и сцен.

Во второй главе описываются результаты исследования влияния прунинга и квантизации глубоких свёрточных сетей на точность и скорость работы систем распознавания лиц. Также приводятся результаты разработки гибридного подхода к реализации биометрических систем распознавания лиц с использованием глубоких свёрточных сетей, в том числе с множественными входами и смешанными данными.

В заключении резюмируются полученные результаты, описываются рекомендации и перспективы исследования.

Рекомендации и перспективы дальнейшей разработки темы.

В компьютерном зрении и конкретно в распознавании лиц до сих пор существует много проблем и задач, которые ещё предстоит решить. Использование как двумерных, так и трёхмерных систем распознавания лиц сопряжено с известными проблемами и ошибками. Часть исследователей сосредоточила силы на применении многокомпонентных, гибридных, мультимодальных системах [38-40]. Среди основных направлений, трендов и задач для будущих исследований в отрасли можно указать следующее:

- Исследование актуальных и поиск новых архитектур глубоких нейронных сетей.
- Повышение точности распознавания в сложных условиях.
- Построение надёжных алгоритмов и систем обнаружения распечатанных, поддельных и сгенерированных изображений и видео.
- Упрощение интерфейсной части подобного рода систем распознавания, повышение простоты развёртывания, использования и обслуживания таких систем.
- Решение проблемы предвзятости и повышение релевантности систем, расширение обучающих баз в контексте использования изображений людей из различных рас и национальностей, разного цвета кожи и других особенностей.
- Повышение точности распознавания лиц в маске, сильно перекрытых лиц.
- Решение и обсуждение этических проблем биометрии, влияние систем распознавания на личную жизнь.

- Внедрение систем распознавания в повседневную жизнь, в узкие отрасли: в ритейл системы, в системы оплаты, использование распознавания при мониторинге водителя, управляющего транспортным средством и прочее.

СПИСОК ЛИТЕРАТУРЫ

1. Goodfellow, I. Deep learning / I. Goodfellow, Y. Bengio, A. Courville // Cambridge, MA: MIT Press. - 2016.
2. Guo, Y. Deep learning for visual understanding / Y. Gio, Y. Liu, A. Oerlemans, S. Lao, S. Wu, M.S. Lew // A review, Neurocomputing. - 2016. - 187. - 27–48.
3. He, R. Delving deep into rectifiers: Surpassing human-level performance on imagenet classification / R. He, X. Zhang, S. Ren, J. Sun // Proc. IEEE International Conference on Computer Vision. - 2015. - 1026–1034.
4. Taigman, Y. Deepface: Closing the gap to human-level performance in face verification / Y. Taigman, M. Yang, M. Ranzato, L. Wolf // Proc. IEEE Conference on Computer Vision and Pattern Recognition. - 2014. - 1701–1708.
5. Sun, Y. Deeply learned face representations are sparse, selective, and robust / Y. Sun, X. Wang, X. Tang, X. // Proc. IEEE Conference on Computer Vision and Pattern Recognition. - 2015. - 2892–2900.
6. Sun, Y. Deepid3: Face recognition with very deep neural networks / Y. Sun, D. Liang, X. Wang, X. Tang // arXiv 1502.00873.
7. Zhou, E. Naive-deep face recognition: Touching the limit of LFW benchmark or not? / E. Zhou, Z. Cao, Q. Yin // arXiv 1501.04690.
8. Schroff, F. Facenet: A unified embedding for face recognition and clustering / F. Schroff, D. Kalenichenko, J. Philbin // Proc. IEEE Conference on Computer Vision and Pattern Recognition. - 2015. - 815–823.
9. Rawat, W. Deep convolutional neural networks for image classification: A comprehensive review / W. Rawat, Z. Wang // Neural Computation. - 2017.
10. Huang, G.B. Labeled faces in the wild: A database for studying face recognition in unconstrained environments / G.B. Huang, M. Ramesh, T. Berg, E. Learned-Miller // Technical Report 07-49. Amherst: University of Massachusetts.
11. Sochenkova, A. Convolutional neural networks and face recognition task / A. Sochenkova, I. Sochenkov, A. Makovetskii, A. Vokhmintsev, A. Melnikov // Proc. SPIE 62 Annual Meeting: Applications of Digital Image Processing XL. - 2017. - 0277-786X.
12. Rajamanoharan, G. Static and dynamic 3D facial expression recognition: A comprehensive survey / G. Rajamanoharan, S. Zafeiriou, M. Pantic, L. Yin // Image Vis. Comput. - 2012. - Vol. 30 (10). - 683–697.
13. Pan, G. Establishing point correspondence of 3D faces via sparse facial deformable model / G. Pan, X. Zhang, Y. Wang, Z. Hu, X. Zheng, Z. Wu // IEEE Trans. Image Process. - 2013. - Vol. 22 (11). - 4170–4181.
14. Cao, C. Displaced dynamic expression regression for real-time facial tracking and animation / C. Cao, Q. Hou, K. Zhou // ACM Trans. Graph. - 2014. - Vol. 33 (4). - 43:1–43:10.
15. Zhang, X. BP4D Spontaneous: a high-resolution spontaneous 3D dynamic facial expression database / X. Zhang, L. Yin, J.F. Cohn, S. Canavan, M. Reale, A. Horowitz, P. Liu, J.M. Girard // Image Vis. Comput. - 2014. - Vol. 32 (10). - 692–706.
16. Li, X. Fully automatic 3D facial expression recognition using polytypic multi-block local binary patterns / X. Li, Q. Ruan, Y. Jin, G. An, R. Zhao // Signal Processing. - 2015. - Vol. 108. - 297-308.
17. Tam, G. Registration of 3D point clouds and meshes: A survey from rigid to nonrigid / G. Tam, Z.-Q. Cheng, Y.-K. Lai, F. Langbein, Y. Liu, D. Marshall, R. Martin, X.-F. Sun, P. Rosin // IEEE Trans. Vis. Comput. Graph. - 2013. - Vol. 19 (7). - 1199–1217.
18. Cheng, S. Statistical non-rigid ICP algorithm and its application to 3D face alignment / S. Cheng, I. Marras, S. Zafeiriou, M. Pantic // Image Vis. Comput. - 2017. - Vol. 58. - 3–12.
19. Besl, P. A method for registration of 3-D shapes / P. Besl, N. McKay // IEEE Transactions of Pattern Analysis and Machine Intelligence. - 1992. - Vol. 14 (2). - 239–256.
20. Horn, B. Closed-Form Solution of Absolute Orientation Using Unit Quaternions / B. Horn // Journal of the Optical Society of America A. - 1987. - Vol. 4(4). - 629–642.
21. Horn, B. Closed-form Solution of Absolute Orientation Using Orthonormal Matrices / B. Horn, H. Hilden, S. Negahdaripour // Journal of the Optical Society of America A. - 1988. - Vol. 5 (7). - 1127-1135.
22. Du, S. Affine iterative closest point algorithm for point set registration / S. Du, N. Zheng, S. Ying, J. Liu // Pattern Recognition Letters. - 2010. - Vol. 31. - 791–799.
23. Low, K.L. Linear least-squares optimization for point-to-plane ICP surface registration / K.L. Low // Technical Report TR04-004, Department of Computer Science, University of North Carolina at Chapel Hill. - 2004.

24. Makovetskii, A. An efficient point-to-plane registration algorithm for affine transformations / A. Makovetskii, S. Voronin, V. Kober, D. Tihonkih // Proc. SPIE 10396, Applications of Digital Image Processing XL. - 2017. -103962J.
25. Khoshelham, K. Closed-form solutions for estimating a rigid motion from plane correspondences extracted from point clouds / K. Khoshelham // ISPRS Journal of Photogrammetry and Remote Sensing. - 2016. - Vol. 114. - pp. 78–91.
26. Cheng, S. Active nonrigid ICP algorithm / S. Cheng, I. Marras, S. Zafeiriou // Proc. 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition. - 2015. - 1-8.
27. Gonzalez-Fraga, J.A. An efficient algorithm for matching of SLAM video sequences / J.A. Gonzales-Fraga, V.H. Diaz-Ramirez, V. Kober, J.J. Tapia-Higuera, O. Alvarez-Xochihua // Proc. SPIE's 61 Annual Meeting: Applications of Digital Image Processing XXXIX. - 2016. - Vol. 9971. - 99712Z-10.
28. Gonzalez-Fraga, J.A. Accurate generation of the 3d map of environment with a rgb-d camera / J.A. Gonzalez-Fraga, V. Kober, V.H. Diaz-Ramirez // Proc.SPIE. - 2017. - Vol. 10396. - 10396–7.
29. Khoshelham, K. Accuracy and resolution of kinect depth data for indoor mapping applications / K. Khoshelham, S.O. Elberink // Sensors. - 2012. - Vol. 12(2). - 1437–1454.
30. Wen, Y. A discriminative feature learning approach for deep face recognition / Y. Wen, K. Zhang, Z. Li, Y. Qiao // Springer. In European Conference on Computer Vision. - 2016. - 499–515.
31. Schroff, F. FaceNet: A unified embedding for face recognition and clustering / F. Scgroff, D. Kalenichenko, J. Philbin // In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). - 2015. - 815–823.
32. Deng, J. ArcFace: Additive angular margin loss for deep face recognition / J. Deng, J. Guo, N. Xue, S. Zafeiriou // arXiv preprint. - 2018. - arXiv:1801.07698.
33. Cao, Q. VGGFace2: A dataset for recognising faces across pose and age / Q. Cao, L. Shen, W. Xie, O. Parkhi, A. Zisserman // In Proceedings of the International Conference on Automatic Face & Gesture Recognition. - 2018. - 67–74.
34. Ruchay, A.N. Accurate reconstruction of the 3D indoor environment map with a RGB-D camera based on multiple ICP / A.N. Ruchay, K.A. Dorofeev, A.V. Kober // CEUR Workshop Proceedings, 2210. - 2018. - 300-308.
35. Ruchay, A.N. Accuracy analysis of 3D object reconstruction using RGB-D sensor / A.N. Ruchay, K.A. Dorofeev, A.V. Kober // CEUR Workshop Proceedings 2210. - 2018. - 82-88.
36. Ruchay, A.N. Fusion of information from multiple kinect sensors for 3D object reconstruction/ A.N. Ruchay, K.A. Dorofeev, V.I. Kolpakov // Computer Optics, 42 (5). - 2018. - 898-903.
37. Ruchay, A. Accuracy analysis of 3D object shape recovery using depth filtering algorithms / A. Ruchay, K. Dorofeev, A. Kober, V. Kolpakov, V. Kalschikov // Proceedings of SPIE - The International Society for Optical Engineering, 10752. - 2018. - № 1075221.
38. Elaggoune, Hybrid descriptor and optimized CNN with transfer learning for face recognition / Elaggoune, Hocine & Belahcene, Mebarka & Bourennane, Salah // Multimedia Tools and Applications. - 2022. - 81.
39. Tharewal, S. Score-Level Fusion of 3D Face and 3D Ear for Multimodal Biometric Human Recognition / S. Tharewal, Timothy Malche, Pradeep Kumar Tiwari, Mohamed Yaseen Jabarulla, Abeer Ali Alnuaim, Almetwally M. Mostafa, Mohammad Aman Ullah // Computational Intelligence and Neuroscience. - 2022. - 9 pp.
40. Szczuko, P. Evaluation of Decision Fusion Methods for Multimodal Biometrics in the Banking Application / P. Szczuko, A. Harasimiuk, A. Czyżewski // Sensors. - 2022. - 22, 2356.

Евсюков М.В.
ФГБОУ ВО КубГТУ, аспирант,
michael.evsyukov@gmail.com

РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И КОНТРОЛЯ ПРИ ВЗАИМОДЕЙСТВИИ С ГОЛОСОВЫМИ АССИСТЕНТАМИ НА ОСНОВЕ ИДЕНТИФИКАЦИИ РЕЧИ ПОЛЬЗОВАТЕЛЯ

Аннотация: Многие современные информационные системы предоставляют пользователям возможность голосового взаимодействия. В связи с этим, актуальной задачей становится обеспечение безопасной голосовой аутентификации. Алгоритмы распознавания личности по голосу имеют долгую историю исследования и практического применения, однако их основным недостатком является уязвимость к спуфингу, т.е. к злоумышленным действиям, направленным на аутентификацию под видом пользователя системы. Цель данного исследования – повышение надёжности систем голосовой аутентификации путём разработки нового алгоритма противодействия спуфингу. В данной статье выполнен краткий обзор современных методов спуфинга и приведены ссылки на актуальные исследования в области голосовой аутентификации. В ходе разработки алгоритма противодействия спуфингу мы придерживаемся подхода, основанного на классификации с одним классом и обнаружении аномалий. Его основное преимущество заключается в высокой приспособленности к защите от ранее неизвестных атак, использующих алгоритмы синтеза или преобразования речи. Основным нововведением данного исследования является идея реализации противодействия спуфингу не на уровне всей системы, а на уровне каждого пользователя. Данный подход ранее был описан применительно к антиспуфингу при распознавании личности по геометрии лица, и продемонстрировал высокую эффективность. Однако на данный момент, не существует исследований, реализовавших данную технологию применительно к голосовому антиспуфингу. В дальнейшем планируется провести серию экспериментов, направленных на оценку конкурентоспособности предложенного подхода и выбор оптимальных алгоритмов антиспуфинга. Результаты экспериментов и полученные выводы будут представлены в последующих статьях.

Ключевые слова: Нейронный сети, аутентификация, голос, идентификация личности, искусственный интеллект, машинное обучение, биометрия, информационная безопасность, спуфинг, обработка сигналов.

Введение

Важным направлением современной информационной безопасности является биометрическая аутентификация. Аутентификация (подтверждение) личности – процесс подтверждения подлинности субъекта при взаимодействии с информационной системой путём предъявления фактора аутентификации. В случае биометрической аутентификации, в качестве фактора аутентификации выступают уникальные биологические или поведенческие особенности человека. Предъявляя эти особенности информационной системе, пользователь подтверждает, что является именно тем субъектом, за которого он себя выдаёт [1].

Существует множество биометрических характеристик, которые пригодны для использования в качестве фактора аутентификации: отпечатки пальцев, контур ладони, геометрия лица, узоры радужной оболочки и сетчатки, а также походка, однако, объектом исследования данной работы является голосовая аутентификация.

Важность голосовой аутентификации обусловлена широкой распространённостью голосовых интерфейсов, которая продолжает увеличиваться. Голосовое взаимодействие применяется для управления смартфонами, устройствами интернета вещей, автомобилями и т.д [2,3]. Для человека устная речь является наиболее удобным и естественным видом общения, а для людей, имеющих серьёзные проблемы со зрением, это, зачастую, основной способ взаимодействия с высокотехнологичными устройствами.

Многие современные банковские приложения позволяют совершать покупки и платежи при помощи голосовых команд. Кроме того, голосовая аутентификация применяется для увеличения безопасности телефонных систем, например, в колл-центрах банков и многих других организаций [4].

Несмотря на это, голосовая аутентификация обладает недостатками, главным из которых является уязвимость к спуфингу. Спуфингом называются злоумышленные действия, направленные на аутентификацию в системе в качестве другого пользователя [5].

В научной литературе, посвящённой голосовой аутентификации принята следующая классификация видов спуфинга [5]:

1. Выдача себя за другое лицо

Данный вид спуфинга подразумевает подражание одним человеком голосовым характеристикам другого человека. Выдача себя за другое лицо отличается от других видов спуфинга тем, что для его реализации злоумышленник не использует вспомогательных технических средств и методов. В связи с этим, противодействие этому виду спуфинга не требует дополнительных контрмер и реализуется за счёт качественной реализации алгоритма распознавания личности по голосу.

2. Повторное воспроизведение речи

Повторное воспроизведение речи – эффективный и самый простой в реализации вид спуфинга, который, по мнению многих исследователей, представляет наиболее серьёзную угрозу системам голосовой аутентификации [5]. Его реализация заключается в записи фрагмента речи человека с целью его последующего предъявления системе аутентификации. Исследование методов противодействия данному виду спуфинга являлось целью конференций ASVspoof 2017 [6] и ASVspoof 2019 [7].

3. Преобразование речи

Преобразование речи подразумевает использование специализированных программных средств, изменяющих речь человека таким образом, чтобы она стала похожей на речь другого человека. Исследование методов противодействия данному виду спуфинга являлось целью конференций ASVspoof 2015 [8] и ASVspoof 2019 [7].

4. Генерация речи

Данный метод подразумевает генерацию искусственного голоса, на основе произвольного текста, обладающего характеристиками голоса определённого человека. Исследование методов противодействия данному виду спуфинга являлось целью конференций ASVspoof 2015 [8] и ASVspoof 2019 [7].

Ввиду развития методов искусственного интеллекта сравнительно недавно появилась технология дипфейк, использующая генеративно-состязательные нейронные сети. Данная технология нашла своё применение во многих задачах искусственного интеллекта, в т.ч. в алгоритмах преобразования и генерации речи. Исследование методов противодействия спуфингу систем голосовой аутентификации, использующих технологию дипфейк, является одной из главных целей конференции ASVspoof 2021 [9].

Кроме того, существует широкое разнообразие атак, основной целью которых являются системы распознавания речи, но которые также применимы к системам распознавания личности по голосу. В зависимости от механизма реализации, среди таких атак выделяются атаки, эксплуатирующие алгоритмы цифровой обработки голосового сигнала, а также общие атаки на алгоритмы машинного обучения, известные как оптимизационные атаки [10].

Противодействие описанным выше видам спуфинга является основным направлением исследований, посвящённых совершенствованию систем голосовой аутентификации. Главным событием в области противодействия голосовому спуфингу является конференция ASVspoof, которая проводится каждые два года [6,7,8,9].

В связи уязвимостью алгоритмов распознавания личности по голосу к спуфингу, каждая система голосовой аутентификации должна включать в себя дополнительный механизм противодействия спуфингу, который называется контрмерой (Рис. 1). Задача контрмеры – зафиксировать факт того, что система подвергается спуфинг-атаке [11].

Рис. 1. Общая схема системы голосовой аутентификации

Цель данного исследования – повышение надёжности систем голосовой аутентификации за счёт разработки нового алгоритма противодействия спуфингу.

Методы распознавания личности по голосу

Для распознавания личности по голосу необходимо извлечь из аудиозаписи голоса значимые голосовые характеристики, позволяющие наиболее эффективно идентифицировать пользователя, и применить к ним алгоритм распознавания личности по голосу [11].

Существует большое количество алгоритмов извлечения голосовых характеристик. Применительно к задаче распознавания личности по голосу, наибольшее распространение получили кратковременные спектральные характеристики, основанные на преобразовании Фурье или схожих математических механизмах [11].

Среди контрмер против спуфинга, поданных на конференции ASVspoof, можно выделить две разновидности голосовых характеристик [6,5,11]:

— характеристики, созданные человеком: MFCC, LFCC, CQCC амплитудная спектрограмма сигнала, и т. д. Данные характеристики извлекаются из звукового сигнала при помощи некоторого детерменированного алгоритма;

— характеристики, использующие технологии машинного обучения, например, нейросетевые характеристики или i-векторы, основанные на модели гауссовой смеси [11].

После извлечения характеристик, необходимо применить к ним метод распознавания личности по голосу. Обычно в качестве такого метода используется некоторый алгоритм машинного обучения, который аппроксимирует распределение характеристик пользователя в общем пространстве характеристик (например, модель гауссовой смеси) или строит границу между распределениями характеристик различных пользователей в пространстве характеристик (например, нейронные сети или машины опорных векторов) [6].

В рамках нашего исследования, в качестве отличительных характеристик голоса применяется амплитудная спектрограмма с нормализованными полосами частот. В качестве механизма распознавания личности по голосу мы используем свёрточную нейронную сеть ResNet-34. Данная нейронная сеть хорошо зарекомендовала себя применительно к задаче распознавания образов и позднее нашла применение к задаче распознавания личности по голосу [12].

На текущий момент существуют более свежие научные работы, предлагающие более продвинутые архитектуры нейронных сетей для распознавания личности по голосу, например, Thin ResNet и архитектуры, полученные при помощи технологии автоматического интеллектуального поиска архитектур [13]. Тем не менее, перечисленные архитектуры сложнее в реализации, чем оригинальная ResNet, и не несут существенного, для задачи нашего исследования, прироста точности.

Для улучшения качества системы распознавания личности по голосу мы используем технологию трансфера обучения [14]. А именно, мы используем обученную ранее сеть ResNet для распознавания большого количества пользователей, убираем последний слой сети и используем результаты работы предпоследнего слоя сети в качестве отличительных голосовых характеристик. Далее, при обучении, мы рассчитываем среднее значение данных характеристик для каждого пользователя. На этапе распознавания пользователя, из представленной записи речи извлекаются характеристики при помощи нейронной сети. Далее полагается, что запись относится к тому пользователю у которого оказывается наименьшее косинусное расстояние между извлечёнными из записи характеристиками и рассчитанном на этапе обучения средним значением его характеристик. Данный подход позволяет переиспользовать ранее обученную сеть для нашей задачи и обеспечивает простоту добавления новых пользователей.

Также в процессе нашего исследования была реализована классификация личности с использованием модели гауссовой смеси [15], однако свёрточная нейронная сеть продемонстрировала значительно большие точность и устойчивость к изменениям условий записи.

Методы противодействия спуфингу

Существует большое количество методов противодействия спуфингу. Некоторые из них нацелены на эффективное противодействие конкретным видам спуфинга, другие – на универсальную защиту от всех видов спуфинга. В ходе конференции ASVspoof 2015 большинство заявок использовали простой классификатор, такой как модель гауссовой смеси или машина опорных векторов, и делали акцент на тщательном подборе акустических характеристик, позволяющих отличить синтезированный или преобразованный голос от подлинно человеческого [8].

Среди перспективных направлений исследований в сфере противодействия спуфингу, мы посчитали наиболее эффективным подход, основанный на классификации с одним классом и обнаружении аномалий. Основное преимущество данного подхода заключается в том, что он лучше всего приспособлен к защите от ранее неизвестных атак, использующих синтез или преобразование речи.

Например, в результате исследования [16] была разработана система, использующая LFCC в качестве характеристик и нейронную сеть ResNet-18 в качестве классификатора. Кроме того, в данном исследовании была предложена функция потерь, которая в большей степени приспособлена для решения задачи классификации с одним классом, по сравнению со стандартными функциями. В ходе

конференции ASVspoof 2019 данная система показала EER = 2.19%, заняла третье место по эффективности среди всех систем и первое место среди систем без слияния.

Научная новизна

Новым предложением нашего исследования, по сравнению с работой [16] является идея реализации противодействия спуфингу не на уровне всей системы, а на уровне каждого идентифицируемого пользователя. Данный подход ранее уже был описан применительно к антиспуфингу при распознавании личности по геометрии лица [17], и продемонстрировал высокую эффективность, однако, на данный момент, не существует других исследований, реализовавших данную технологию применительно к антиспуфингу при распознавании личности по голосу.

В ходе данного исследования планируется провести ряд экспериментов, направленных на оценку общей эффективности системы, использующей данный подход, и выбор оптимальных голосовых характеристик, а также метода распознавания личности по голосу. В качестве набора данных планируется использовать датасет ASVspoof 2019.

Предполагается протестировать набор отличительных голосовых характеристик (MFCC, LFCC, CQCC, мел-спектрограмма), а также классификаторов (свёрточные нейронные сети, модель гауссовой смеси, машина опорных векторов) из которых будет выбрана наилучшая конфигурация.

Выводы

В данной статье выполнен краткий обзор современных методов спуфинга и приведены ссылки на актуальные исследования в области голосовой аутентификации.

В ходе разработки алгоритма противодействия спуфингу мы придерживаемся подхода, основанного на классификации с одним классом и обнаружении аномалий. Основное преимущество данного подхода заключается в том, что он лучше всего приспособлен к защите от ранее неизвестных атак, использующих алгоритмы синтеза или преобразования речи.

Основным нововведением исследования является идея реализации противодействия спуфингу не на уровне всей системы, а на уровне каждого пользователя.

В дальнейшем планируется провести серию экспериментов, направленных на оценку конкурентоспособности предложенного подхода и выбор оптимальных алгоритмов антиспуфинга. Результаты и выводы экспериментов будут представлены в последующих статьях.

Предложенный метод противодействия спуфингу является центральной частью диссертационного исследования, выполняемого в рамках гранта. Эффективность данного метода планируется оценить путём в результате разработки и экспериментального исследования прототипа системы голосовой аутентификации со встроенным модулем антиспуфинга.

СПИСОК ЛИТЕРАТУРЫ

1. Ravika, N. An Overview of Automatic Speaker Verification System / N. Ravika // Intelligent Computing and Information and Communication — 2018 — С. 603-610.
2. Vlasenko, A.V. Possibilities of Improving the Cyber Security of Mobile Devices Based on the Integration of Dynamic Biometric Methods / A.V. Vlasenko, M.M. Putyato, A.S. Makaryan // Selected Papers of the V International Scientific and Practical Conference "Distance Learning Technologies" (DLT 2020) — 2020 — С. 518-526.
3. Путято, М.М. Исследование возможности совершенствования кибербезопасности инфраструктуры интернета вещей на основе интеграции биометрических методов аутентификации / М.М. Путято, А.С. Макарян // Информационные системы и технологии в моделировании и управлении. Сборник трудов V Международной научно-практической конференции — 2020 — С. 267-270.
4. El-Abed, M. Evaluation of Biometric Systems / M. El-Abed, C. Charrier // New Trends and Developments in Biometrics — 2012 — С. 149-169.
5. Hao, B. Voice Liveness Detection for Medical Devices / B. Hao, X. Hei // Design and Implementation of Healthcare Biometric Systems — 2019 — С. 109-136.
6. Kinnunen, T. The ASVspoof 2017 Challenge: Assessing the Limits of Replay Spoofing Attack Detection / T. Kinnunen, M. Sahidullah, H. Delgado, M. Todisco, N. Evans, J. Yamagishi, K.A. Lee // Proceedings of 18th Annual Conference of the International Speech Communication Association (Interspeech 2017) — 2017 — С. 6-11.
7. Kinnunen, T. ASVspoof 2019: Future Horizons in Spoofed and Fake Audio Detection / T. Kinnunen, M. Sahidullah, H. Delgado // Proceedings of 20th Annual Conference of the International Speech Communication Association (Interspeech 2019) — 2019 — 35 с.

8. Wu, Z. ASVspoof: the Automatic Speaker Verification Spoofing and Countermeasures Challenge / Z. Wu, J. Yamagishi, T. Kinnunen, C. Hanilc, M. Sahidullah, A. Sizov, N. Evans, M. Todisco // IEEE Journal of Selected Topics in Signal Processing — 2017 — Т. 11. № 4 — С. 588-604.
9. Delgado, H. ASVspoof 2021: Automatic Speaker Verification Spoofing and Countermeasures Challenge Evaluation Plan / H. Delgado, N. Evans, T. Kinnunen и др. [Электронный ресурс]. — Режим доступа: https://www.asvspoof.org/asvspoof2021/asvspoof2021_evaluation_plan.pdf
10. Abdullah, H. The Faults in our ASRs: An Overview of Attacks against Automatic Speech Recognition and Speaker Identification Systems / H. Abdullah, K. Warren, V. Bindschaedler, N. Papernot, P. Traynor — 2020 — 18 с. [Электронный ресурс]. — Режим доступа: https://www.researchgate.net/publication/342944303_The_Faults_in_our_ASRs_An_Overview_of_Attacks_against_Automatic_Speech_Recognition_and_Speaker_Identification_Systems
11. Kinnunen, T. An Overview of Text-Independent Speaker Recognition: from Features to Supervectors / T. Kinnunen., H. Li // Speech Communication — 2010 — № 52 — С. 12-40.
12. Chung, J. S. VoxCeleb2: Deep Speaker Recognition / J. S. Chung, A. Nagrani, A. Zisserman // Proceedings of 19th Annual Conference of the International Speech Communication Association (Interspeech 2018) — 2018 — С. 1086-1090.
13. Ding, S. AutoSpeech: Neural Architecture Search for Speaker Recognition / S. Ding, T. Chen, X. Gong, W. Zha, Z. Wang — 2020 — [Электронный ресурс]. Режим доступа: https://www.researchgate.net/publication/341232380_AutoSpeech_Neural_Architecture_Search_for_Speaker_Recognition
14. Rahul, P. Audio Spoofing Verification using Deep Convolutional Neural Networks by Transfer Learning / P. Rahul, P. Aravind, C. Ranjith, U. Nechiyil, N. Paramparambath — 2020 — [Электронный ресурс]. Режим доступа: https://www.researchgate.net/publication/343568673_Audio_Spoofing_Verification_using_Deep_Convolutional_Neural_Networks_by_Transfer_Learning
15. Reynolds, D. Speaker Verification Using Adapted Gaussian Mixture Models / D. Reynolds, T. Quatieri, R. Dunn // Digital Signal Processing — 2000 — Т. 10 — С. 19-41.
16. Zhang, Y. One-Class Learning Towards Synthetic Voice Spoofing Detection / Y. Zhang, F. Jiang, Z. Duan // IEEE Signal Processing Letters — 2021 — [Электронный ресурс]. Режим доступа: https://www.researchgate.net/publication/351174426_One-Class_Learning_Towards_Synthetic_Voice_Spoofing_Detection
17. Fatemifar, S. Client-Specific Anomaly Detection for Face Presentation Attack Detection. Pattern Recognition / S. Fatemifar, S. Arashloo, M. Awais, J. Kittler — [Электронный ресурс]. Режим доступа: https://www.researchgate.net/publication/344899642_Client-Specific_Anomaly_Detection_for_Face_Presentation_Attack_Detection

Егорова А. О.
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)», аспирант,
aoegorova@internet.ru

ПОСТРОЕНИЕ МОДЕЛИ АДАПТИВНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Аннотация: В данной статье представлен анализ существующих моделей защиты информации с адаптивным управлением Рассмотрены структурные компоненты разрабатываемой модели и оптимальные методы их построения. В работе приведена разработанная модель адаптивной системы защиты информации от утечки по техническим каналам и алгоритм реализации данной модели в виде аппаратно-программного комплекса.

Ключевые слова: информационная безопасность, адаптивная защита информации, технические каналы утечки информации.

В соответствии с тенденциями развития современного общества, возникает необходимость в расширении распространения цифровизации на новые виды деятельности. Так, на данный момент федеральный проект «Информационная безопасность» является одной из ключевых составляющих национальной программы «Цифровая экономика Российской Федерации», что подчеркивает актуальность развития данного направления. Такое развитие подразумевает, в том числе, совершенствование методов и средств защиты конфиденциальной информации. Например, применение интеллектуальных систем различной степени сложности организации и представления стало нормальным в процессе обеспечения компьютерной безопасности. Использование механизмов адаптации в условиях осуществления деятельности по технической защиты информации на данный момент не имеет такого широкого применения, как в других сферах информационной безопасности. В связи с этим возникает необходимость в разработке моделей систем защиты информации, реализующих алгоритмы адаптивного управления в отношении блокирования технических каналов утечки информации. Первым этапом является постановка цели научной работы.

Целью данной научной работы является разработка и реализация модели адаптивной системы защиты информации от утечки по техническим каналам.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Рассмотреть существующие исследования и актуальные разработки в области построения адаптивных систем защиты информации [1, 2].
2. Произвести разработку и построение модели функционирования адаптивной системы защиты информации [2, 3, 4].
3. Реализовать разработанную модель в виде аппаратно-программного комплекса адаптивной защиты информации.
4. Произвести испытания и сбор данных о функционировании разработанного средства.

Объектом исследования являются системы защиты информации от утечки по техническим каналам.

Предмет исследования — методы и средства построения систем защиты информации от утечки по техническим каналам с адаптивным управлением.

Научная новизна работы заключается в следующем:

1. Впервые принципы адаптивного управления были применены в защите информации от утечки по техническим каналам.
2. Разработанная модель адаптивной системы защиты информации отличается от существующих более высокой степенью универсальности по отношению к разнообразию информационных систем.
3. Разработанный программно-аппаратный комплекс позволяет обеспечивать высокий уровень защиты от утечки по техническим каналам утечки информации.

Теоретическая значимость представленной работы состоит в развитии методов построения средств и систем защиты информации от утечки по техническим каналам с применением алгоритмов адаптивного управления.

Практическая значимость полученных в работе результатов заключается в том, что разработанная модель и её программно-аппаратная реализация могут быть использованы для

автоматизации процессов защиты информации в физических полях разной природы в информационных системах [5].

Первоначально для разрабатываемой модели следует определить задачи, которые она должна решать, поскольку данный этап определяет направления разработки и основные требования к системе:

– обеспечение защиты информации в режиме реального времени;

– обеспечение необходимого уровня шумового сигнала, маскирующего информативный сигнал;

– генерирование маскирующего шумового (шумоподобного) сигнала.

Таким образом, разрабатываемая модель должна удовлетворять критериям быстрого реагирования (изменения параметров системы), достаточного уровня маскирующего излучения и достаточной степени энтропии для маскирующего сигнала.

Процесс разработки адаптивной системы, независимо от назначения, включает в себя следующие этапы:

1. Изучение принципов и механизмов адаптации с целью поиска удовлетворяющих требования разрабатываемой системы. На данном этапе следует провести анализ публикаций авторов, проводивших исследования в области изучения и построения адаптивных систем, а также выделить актуальные на данный момент механизмы адаптации.

2. Исследование моделей адаптивных систем, в том числе, систем защиты информации. Данный этап включает в себя изучение и систематизацию существующих разработок моделей систем с адаптивным управлением из различных областей, анализ структур моделей и применяемых принципов адаптации.

3. Построение модели адаптивной системы защиты информации на основании модифицированных выбранных методов и моделей в соответствии с требованиями текущей области применения. На этом этапе проводится разработка не только модели системы, но и моделей подсистем, функционирование которых позволяет выполнять задачи разрабатываемой системы. Также определяется механизм взаимодействия подсистем на уровне модели.

4. Апробация внедрения адаптированных принципов по отношению к разрабатываемой системе, и проверка на соответствие итогов планируемым результатам. Данный этап представляет собой проведение испытаний и оценку эффективности системы, а также формирование заключения об адекватности модели и работоспособности системы.

Проведя анализ существующих моделей систем защиты информации с адаптивным управлением, можно выделить модель типовой адаптивной системы защиты информации (Рис. 1) [1, 6].

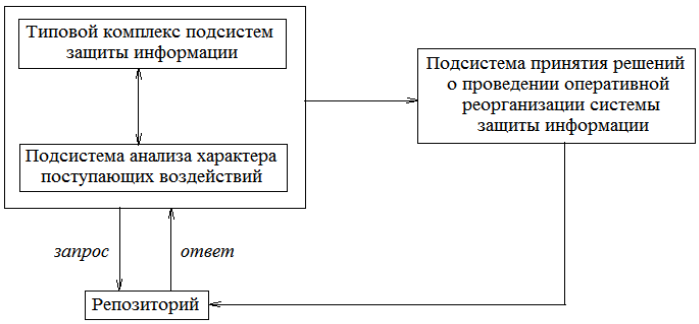


Рис. 1. Типовая адаптивная система защиты информации

Приведенная типовая систем актуальна для моделей со структурной адаптацией, поскольку подразумевает реорганизацию системы в ответ на дестабилизирующие воздействия. На основе применения структурной адаптации преимущественно разрабатываются самообучающиеся модели. Тем не менее, принцип самообучения используется также в системах с параметрической адаптацией. В области информационной безопасности наиболее часто разрабатываются системы с использованием структурной адаптации.

Обобщенная архитектура адаптивного самообучающегося средства защиты информации приведена на Рис. 2 [1, 7].

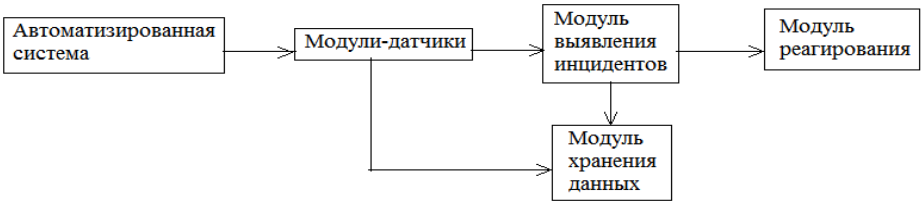


Рис. 2. Архитектура адаптивного самообучающегося средства ЗИ

В обобщенном виде приведенный механизм обучения адаптивной системы защиты информации имеет широкое применение.

Большая часть существующих адаптивных систем защиты информации направлены на обеспечение компьютерной безопасности и основываются на принципе обнаружения аномалий. Приведенный на рис. 3 алгоритм позволяет производить анализ состояния системы в сравнении с контрольными параметрами нормального состояния [2, 8].

Рис. 3. Алгоритм обнаружения аномалий

Таким образом, проведенный анализ позволяет сделать вывод о том, что рассмотренные модели требуют структурного и содержательного преобразования с целью возможного использования для технической защиты информации. Это связано с тем, что для данной области неприменима структурная адаптация, но общие принципы могут быть заимствованы.

На первом этапе разработки модели адаптивной системы защиты информации от утечки по техническим каналам следует определить структуру разрабатываемой системы. Это позволит произвести корректный выбор методов и средств реализации разрабатываемой системы, а также обеспечить её корректное функционирование за счёт правильно подобранных способов взаимодействия элементов системы. Планируемым подсистемам соответствуют следующие модели:

1. Модель генератора случайных чисел.

На основе линейного конгруэнтного метода генерации псевдослучайной последовательности определяется выделенная контрольная частота (диапазон частот зависит от канала утечки информации) [4, 9, 10].

2. Модель блокирования канала утечки информации.

Определяет порядок осуществления защиты инфекции с использованием активных средств. В данной модели под блокированием каналов утечки информации по техническим каналам подразумевается применение устройств пространственного и линейного зашумления. Зашумление производится с помощью шумового сигнала, генерируемого вычислительным устройством [4, 11, 12].

3. Модель машинного обучения.

Задаёт алгоритм и параметры обучения. На данном этапе выбрана модель обучения адаптивной системы на основе базовой модели машинного обучения. В качестве алгоритма обучения выбран метод восстановления регрессии — метод наименьших квадратов [4, 13].

4. Модель системы оценки эффективности защиты информации.

Проводит анализ функционирования системы защиты информации на соответствие критериям защищенности. Базовым методом оценки эффективности защиты информации от утечки по техническим каналам является определение уровня сигнал/шум для рассматриваемого объекта информатизации [4, 12].

Подробное описание математической модели системы приведено в другой работе автора [4].

Следующим этапом является реализация разработанной модели. Для начала следует определить набор и структуру данных в системе (рис. 4).

Рис. 4. Структура данных системы

Прежде чем перейти к разработке, следует описать планируемый принцип действия аппаратно-программного комплекса. Полезный сигнал поступает на фиксирующее устройство (устройство ввода), затем, проходя аналогово-цифровой преобразователь, видоизменяется в удобный для дальнейшей обработки вид. При помощи цифрового фильтра происходит выделение сигнала контрольной частоты f_i (частота генерируется вычислительным устройством) и определяется мощность полезного сигнала P_i. Следующим шагом выполняется вычисление мощности шумового сигнала P_j и новой контрольной частоты f_j. После чело на устройство вывода направляется шумовой сигнал заданной мощности, но с исключением из спектра выделенной частоты при помощи цифрового фильтра на пути к цифроаналоговому преобразователю. Таким образом, рабочими данными для системы

Алгоритм работы программы в виде блок-схемы представлен на рис. 5. В представленной блок схеме есть подпрограммы, выполняющие вынесенные за пределы основного алгоритма функции для улучшения работы.

В общем представлении программа представляет собой цикл. Первым шагом программа производит генерацию псевдослучайной последовательности (Подпрограмма_1) на основании приведенной выше модели генератора случайных чисел и возвращает в основную структуру значения f_i и f_j, затем на основе модели блокирования канала утечки информации выполняет прием данных с устройств ввода, обработку и фильтрацию (Подпрограмма_2); возвращается значение P_i. Следующим этапом на основании значений f_i и P_i производится обучение и дальнейшее прогнозирование (Подпрограмма_3); возвращается значение P – прогнозируемая мощность, реализуя модель машинного обучения. После сравнения значения P_i (из элемента Подпрограмма_2) и P (из элемента Подпрограмма_3), большему из значений приравнивается P_j. Дальше на основе модели блокирования канала утечки информации выполняется генерация шума P_j и передача его на устройства вывода (Подпрограмма_4). Заключительным шагом итерации программа производит оценку эффективности на основании значений f_j, P_j и P_{i+1} на основании критериев, заданных моделью системы оценки эффективности защиты информации (Подпрограмма_5).

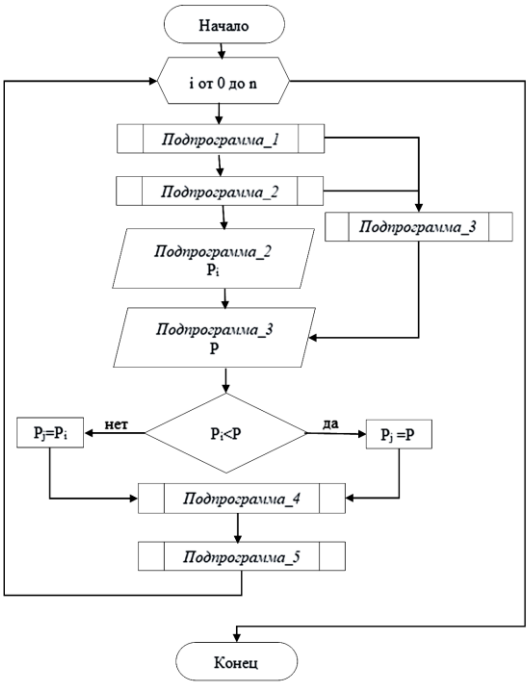


Рис. 5. Блок-схема программной реализации модели

Аппаратная часть проектируемого программно-аппаратного комплекса включает в себя: вычислительные устройства, преобразователи и устройства ввода и вывода (Рис. 6).

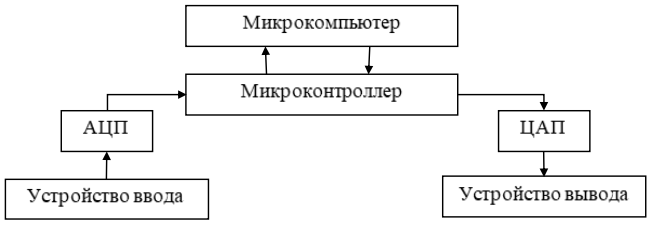


Рис. 6 Схема построения аппаратно-программного комплекса

В качестве устройств ввода могут быть различные датчики: микрофоны, индикаторы поля, анализаторы спектра и т.д. Устройства вывода – излучатели поля различной природы (акустические, электромагнитные, вибрационные и т.д.).

Вычислительные устройства совместно выполняют алгоритм, представленный на рис. 4, распределяя подпрограммы между собой: микроконтроллер выполняет основное тело программы и подпрограммы взаимодействия с устройствами ввода/вывода и первичной обработкой сигналов; микрокомпьютер генерирует псевдослучайные числа и выполняет модуль машинного обучения и прогнозирования. Такая комбинация вычислительных устройств позволяет оптимизировать работу системы, распределяя нагрузку и давая возможность выполнять процессы параллельно без потери скорости, а значит и эффективности системы. Возможным недостатком данного выбора может стать замедление быстродействия системы за счет потерь во времени на этапах передачи данных от одного вычислительного устройства к другому. Однако, данный нюанс может быть компенсирован преимуществами скорости обработки сигнала. Более точную оценку можно будет произвести только непосредственно по результатам экспериментальной проверки работы системы.

Дальнейшее развитие данного научного проекта подразумевает проведение испытаний работоспособности системы и оценку её эффективности. Данный этап позволяет не только произвести оценку качества работы системы, но и внести изменения и доработки в структуру и принцип действия системы с целью улучшения и оптимизации.

Таким образом, в ходе выполнения данной работы был представлен анализ существующих моделей систем защиты информации с адаптивным управлением, приведено описание модели адаптивной системы защиты информации от утечки по техническим каналам, а также алгоритм реализации данной модели. Сделан вывод о дальнейшей перспективе планируемой реализации проекта. При условии проведения успешных испытаний работоспособности системы, данная модель и её реализация могут занять своё место среди способов и средств защиты информации от утечки по техническим каналам.

СПИСОК ЛИТЕРАТУРЫ

1. Калита, А. О. Основы организации адаптивных систем защиты информации / А. О. Калита, М. И. Ожиганова, Е. Н. Тищенко // НБИ технологии. — 2019. — Т. 13. — № 1. — С. 11-15.
2. Ожиганова, М. И. Построение адаптивных систем защиты информации / М. И. Ожиганова, А. О. Калита, Е. Н. Тищенко // НБИ технологии. — 2019. — Т. 13. — № 4. — С. 12-21.
3. Реализация ESG-принципов в стратегии устойчивого развития экономики России / Н. Г. Вовченко, Н. Г. Кузнецов, Е. Н. Макаренко [и др.]. . — Ростов-на-Дону : Ростовский государственный экономический университет "РИНХ", 2022. . — С. 166-175.
4. Егорова, А. О. Математическая модель адаптивной системы защиты информации от утечки по техническим каналам / А. О. Егорова, Е. Н. Тищенко // Вестник УрФО. Безопасность в информационной сфере. — 2022. — № 2 (44). — С. 37-42.
5. Егорова, А. О. Разработка модели адаптивной системы защиты информации от утечки по техническим каналам / А. О. Егорова // Сборник научных трудов по материалам Всероссийской научной школы-семинара «Современные тенденции развития методов и технологии защиты информации». — 2021. — С. 25-27.
6. Левкин, И. М. Типовая структура и состав адаптивной системы защиты информации большой информационной систем / И. М. Левкин, А. А. Володина. — Электрон. текстовые дан. — Режим доступа: http://ubs.mtas.ru/bitrix/components/bitrix/forum.interface/show_file.php?fid=16693.

7. Жуков, В. Г. Применение нечетких искусственных иммунных систем в задаче построения адаптивных самообучающихся средств защиты информации / В. Г. Жуков, М. Н. Жукова, Н. А. Коромыслов // Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. — 2012. — № 1(41). — С. 18-23.
8. Абрамов, Е. С. Построение адаптивной системы информационной безопасности / Е. С. Абрамов // Известия ЮФУ. Технические науки. — 2009. — № 11(100). — С. 99-109.
9. Генераторы случайных чисел [Электронный ресурс]. — Режим досту-па: https://intellect.icu/generatory-sluchajnykh-chisel-5256.
10. Генераторы случайных чисел [Электронный ресурс]. — Режим досту-па: http://stratum.ac.ru/education/textbooks/modelir/lection22.html.
11. Хорев, А. А. Технические каналы утечки акустической (речевой) информации // Специальная техника. — 1998. — № 1. — С. 50.
12. Хорев, А. А. Способы и средства зашиты информации. — 2000. — 316 с.
13. Миронов, А.М. Машинное обучение, часть 1. — 2018. — 90 с.

Изергин Д.А.
РТУ МИРЭА, ст. преподаватель
izergind@mirea.ru

МЕТОД ОБНАРУЖЕНИЯ КАНАЛОВ КОМПРОМЕТАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛИЗИРОВАННЫХ ТЕХНОЛОГИЙ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ УСТРОЙСТВ

Аннотация:
Возможности обработки персональных и банковских данных на мобильных устройствах обуславливают полномасштабное профилирование пользователей различными сервисами. Таким образом, цифровой портрет пользователя является наиболее востребованным товаров для злоумышленников с целью проведения шантажа и социальной инженерии, а также легитимных сервисов для технического и психологического воздействия. Качественное формирование профиля пользователя обеспечивается высокой производительностью современных вычислительных систем в совокупности с методами интеллектуального анализа и наличием больших наборов данных. Однако требования к механизмам обеспечения сохранности данных на мобильных устройствах, заключаются в обеспечении работоспособного состояния системы и направлены на нейтрализацию возможного вредоносного воздействия, не учитывая возможности компрометации пользователя различными легитимными сервисами.

Анализ проблемной области показал, что для качественного решения задачи обнаружения каналов компрометации персональных данных требуется учитывать не только функциональные возможности исполняемых файлов, а также связь между владельцами сервисов для исключения фактов агрегации данных сообществами разработчиков. Учет фактов связности разработчиков мобильных приложений позволяет формировать совокупную оценку полноты обнаружения каналов утечек пользовательских данных, т.к. производится анализ привилегий доступа к ресурсам устройства несколькими приложениями. В представленной работы решена задача повышения полноты обнаружения каналов компрометации персональных данных.

Ключевые слова: информационная безопасность, персональные данные, мобильные операционные системы, Android, нейронные сети, глубокое обучение.

Актуальность исследования. Развитие информационных систем подразумевает увеличение качества сбора и обработки информации благодаря использованию современных технологий передачи данных и систем аналитики. Основополагающей технологией в данной концепции является мобильное устройство. Созданные условия позволяют формировать цифровой портрет владельца устройства, что существенно расширяет границы как технического, так и психологического воздействия. Выполнение качественного профилирования достигается благодаря современным возможностям вычислительных систем в совокупности с методами интеллектуального анализа и наличием больших наборов данных.

Большой объём данных и растущее количества цифровых сервисов делают вопрос сохранности пользовательской информации наиболее важным. Существующие требования к механизмам обеспечения сохранности персональных данных, заключаются в обеспечении работоспособного состояния системы и направлены на нейтрализацию возможного вредоносного воздействия, не учитывая возможности компрометации личности различными приложениями, либо набором сервисов. Таким образом, на основе проведённого анализа возможно выделить следующие ***противоречия***:

1. *В практике* между потребностью в механизмах обнаружения каналов сбора персональных данных различными сервисами на мобильных устройствах и требованиями пользователей к обеспечению защиты конфиденциальных данных.
2. *В науке* между потребностью в обеспечения заданной достоверности обнаружения каналов сбора персональных данных и несовершенством методов и алгоритмов их детектирования.

В качестве путей решения противоречий в диссертационных исследованиях *решалась научная задача* разработки метода обнаружения каналов компрометации персональных данных на мобильных операционных системах на основе интеллектуализированных средств принятия решений, позволяющего повысить уровень защищённости пользовательских данных. Полученные результаты могут быть использованы при создании систем защиты мобильных операционных систем от вредоносного программного обеспечения и возможных утечек персональных данных

Степень разработанности темы исследования. Проблему обнаружения каналов компрометации персональных данных рассматривали такие российские учёные, как: Гамаюнов Д.Ю.,

Гвоздика Я.М., Еремеев М.А., Зегжда П.Д., Зегжда Д.П., Корниенко А.А., Котенко И.В., Красов А.В., Молдовян Н.А., Молдовян А.А., Саенко И.Б., Петренко С.А., Ломако А.Г., Овчаров В.А., а также зарубежных учёные: Evita Bakopoulou, Milad Asgari Mehrabadi, Nattanon Wongwiwatchai, Phannawhat Pongkham, Kunwadee Sripanidkulchai, Jinhong Yang, Md Mehedi Hassan Onik, Nam Yong Lee и др.).

Анализ существующих научных подходов и практических решений данной тематики в работах [1-7] позволил выявить, что требуется решение ряда научно-технических задач, в частности:

– создание модели представления приложения;

– выявление подозрительных приложений на основе сравнения с аналогичными приложениями из представленной категории;

– автоматизированное выявление связи между владельцами приложений на основе данных из открытых источников и исполняемых файлов;

– определение полноты формируемого цифрового портрета пользователя на стороне владельцев приложений.

Для решения перечисленных задач необходимо осуществить поиск новых научно-технических решений, позволяющих обеспечивать высокий уровень безопасности пользовательских данных. Таким образом, данное исследование является востребованным и актуальным.

Целью диссертационной работы является *повышение полноты обнаружения каналов компрометации персональных данных при использовании мобильных устройств*.

Задачи исследования:

1. Оценка уровня информационной безопасности мобильных операционных систем. Исследование существующих механизмов защиты персональных данных, угроз и уязвимостей.
2. Разработка модели оценки рисков компрометации персональных данных приложением.
3. Разработка способа определения сообществ разработчиков мобильных приложений.
4. Разработка модели оценки рисков компрометации персональных данных на мобильном устройстве.
5. Разработка метода обнаружения каналов компрометации персональных данных на мобильных устройствах с применением интеллектуализированных средств принятия решений.
6. Построение архитектуры интеллектуализированной системы детектирования утечек персональных данных, проведение вычислительных экспериментов с целью оценки результатов предложенного метода.
7. Разработка программной реализации интеллектуализированной системы детектирования утечек персональных данных на мобильных устройствах.

Объектом исследования являются процесс обнаружения каналов компрометации персональных данных на мобильных операционных системах.

Предметом исследования являются методы, модели, способы и алгоритмы обнаружения каналов компрометации персональных данных на мобильных операционных системах.

Методология и методы исследования. В качестве методическойи теоретической основы в данном диссертационном исследовании использовались методы: теории вероятностей и математической статистики, к-средних, опорных векторов, наивного Байеса, выявления аномалий, иерархической кластеризации, глубокого обучения, нейросетевого подхода.

Для создания программной реализации разработанного метода использовались языки программирования Python, NodeJS и Kotlin.

Научная задача диссертационного исследования заключается в разработке метода, модели и алгоритма обнаружения каналов компрометации персональных данных при использовании мобильных устройств и обеспечении требуемого уровня их защиты.

Научная новизна работы состоит в следующем:

1. Построена математическая модель оценки рисков компрометации персональных данных приложением, отличающаяся от существующих использованием дополнительных наборов выделенных признаков. В модели учитывается не только запрашиваемые разрешения на доступ к пользовательским данным, но и производится анализ программной реализации методов доступа к данным, что значительно повышает адекватность модели для решения задачи поиска каналов утечек данных.
2. Разработана новая модель оценки рисков компрометации персональных данных на мобильном устройстве, отличающаяся от существующих учётом вероятностных показателей агрегирования информации из различных приложений. С помощью моделирования, возможно оценить сформированные портреты пользователя на стороне владельцев сервисов учитывая совокупность установленных приложений на мобильном устройстве.

3. Разработан новый метод определения связности разработчиков приложений на основе признаков о владельцах сервисов, полученных из открытых источников, а также учёте информации в исполняемых файлах. Данный способ позволяет обнаружить факты агрегации данных из различных источников.

4. Впервые разработан метод обнаружения каналов компрометации персональных данных на мобильных устройствах с применением интеллектуализированных средств принятия решений, позволяющий детектировать аномальные приложения заданных категорий и производить оценку рисковых показателей устройства.

5. Разработана архитектура программного комплекса детектирования каналов утечек персональных данных с применением интеллектуализированных средств принятия решения, позволяющая определять рисковые показатели использования мобильного устройства.

Теоретическая значимость работы состоит в развитии научного аппарата обнаружения наличия каналов компрометации персональных данных и обоснования мероприятий по определению качества формируемого цифрового портрета пользователя.

Практическая значимость работы заключается в применении метода обнаружения каналов компрометации персональных данных в мобильных приложениях с применением интеллектуальных средств принятия решения для формирования гипотетического цифрового портрета пользователя на стороне владельцев сервисов, агрегирующих информацию с целью изучения степени критичности использования данного сервиса.

Положения, выносимые на защиту:

1. Разработан новый способ определения сообществ разработчиков приложений на основе признаков владельцах сервисов из открытых источников и исполняемых файлах, позволивший выявить из 44 210 владельцев сервисов 1 588 сообществ для платформ Google Play и App Store соответственно.

2. Предложен новый многомодельный подход к оцениванию рисков компрометации персональных данных на мобильных устройствах, позволяющий улучшить показатель полноты обнаружения каналов компрометации в среднем на 35%.

3. Предложены научно-обоснованные рекомендации по архитектуре программного комплекса обнаружения каналов утечек персональных данных с применением интеллектуализированных технологий.

4. Разработано математическое и программное обеспечение решения задачи детектирования каналов утечек персональных данных с применением интеллектуальных средств принятия решений.

Реализация результатов работы диссертационных исследований реализованы в учебном процессе Института кибербезопасности и цифровых технологий Российского технологического университета – МИРЭА при организации учебных дисциплин «Технологии разработки мобильных приложений» и «Интеллектуальные мобильные приложения» в виде методических рекомендаций по проведению лекционных, практических и лабораторных занятий (приложение В). Разработанные в диссертационном исследовании модели, метод и методика использованы при выполнении работ по гранту ИБ при финансовой поддержке Минобрнауки России в рамках научного проекта № 40469-18/2021-К.

Обоснованность и достоверность полученных результатов исследования подтверждается всесторонним анализом предшествующих научных работ в данной области, полученными экспериментальными данными, апробацией результатов в научных публикациях и докладах на конференциях, их внутренней непротиворечивостью и адекватностью физическим представлениям об исследуемом процессе.

Апробация результатов работы. Основные положения, представленные в диссертационной работе, докладывались и обсуждались на следующих конференциях:

- Международный научный форум по компьютерным и энергетическим наукам (WFCES 2021) / Risk assessment model of compromising personal data on mobile devices (с докладом), 2021 г.
- VIII Международная научно-практическая конференция «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И МАШИНОСТРОЕНИЕ» (ITE2022) / Модель детектирования аномального поведения мобильных приложений (с докладом), 2022 г.
- Международный научный форум по компьютерным и энергетическим наукам (WFCES 2022) / MODEL FOR DETECTING ANOMALOUS BEHAVIOR OF MOBILE APPS (с докладом), 2022 г.
- Международный научный форум по компьютерным и энергетическим наукам (WFCES 2022) / Метод определения связности разработчиков мобильных приложений (с докладом), 2022 г.

Личный вклад. Все выносимые на защиту научные результаты получены автором лично. Автор под руководством научного руководителя принимал личное участие в постановке цели исследования, формулировке основных задач, разработке методики и научно обоснованных решений по повышению вероятности обнаружения каналов компрометации персональных данных на мобильных операционных системах на основе интеллектуальных средств принятия решения, а также подготовке материалов для публикации совместно с соавторами.

Публикации. Основные результаты научно-квалификационной работы отражены в 5 печатных работах, в том числе 3 публикация в рецензируемых журналах из перечня ВАК РФ, 3 публикации в изданиях из перечня Scopus и Web of Science, четыре свидетельства о регистрации про граммы для ЭВМ

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы исследования, поставлена цель и определены основные задачи. Сформулированы основные научные результаты исследований и положения, выносимые на защиту. Раскрыта научная новизна, теоретическая и практическая значимость полученных результатов. Представлены сведения по апробациям и публикациям по теме исследований. Приведена краткая аннотация содержания диссертации по главам. Рассмотрены возможности практического применения предложенных в работе подходов и методов.

В первой главе приведены результаты анализа исследуемой области. Рассмотрены встроенные механизмы обеспечения безопасности персональных данных в мобильных операционных системах и возможности антивирусных программ. Произведен анализ регламентирующих документов в отношении пользовательских данных и существующих научных подходов и практических решений обеспечения конфиденциальности персональных данных, позволяющий выявить, что требуется решение ряда **научно-технических задач** с целью повышения уровня защищённости персональных данных на мобильных устройствах, в частности:

- повышение точности связывания авторов сервисов;
- выявление подозрительных приложений на основе сформированного цифрового портрета;
- создание метода определения связности разработчиков сервисов на основе данных из открытых источников и исполняемых файлов;
- детектирование возможности агрегирования пользовательских данных из различных источников.

Во второй главе представлены основные научные результаты, полученные в исследовательской работе, направленные на разрешение научной задачи исследования. В работе, с целью получения знаний для функционирования разрабатываемого метода выполняется построение модели оценки рисков компрометации персональных данных, требующей наличие репрезентативного набора исходных данных. Образцы исполняемых файлов получены из сервиса Androzoo (Play Market – 107 238 ед., Appchina – 27 086 ед.), сервиса ApkPure – 27 083 ед; ISCX (Canadian Institute for Cybersecurity) – 33 426 ед. и VirusTotal – 34 850 ед.

Результатом этапа формирования признаков является набор множеств признаков, на основе которых формируется портрет приложения:

$$A_{app} = \{M, C, P, F, L, I, R, O\} \quad (1)$$

где M – множество данных о разработчике; F – множество особенности реализации исполняемого файла; P – множество запрашиваемых привилегий; C – множество компонент приложения; L – множество идентификаторов используемых библиотек; I – множество извлеченных строковых ресурсов (ip, платежные реквизиты, почтовые адреса); R – множество программных реализаций к ПД с использованием Android SDK; O – множество программных реализаций наиболее распространённых пакетов и классов, предназначенные для работы с сетью в ОС Android.

Результатом работы этапа «Кодирование» являются входные данные для системы детектирования аномального поведения исполняемых файлов и обнаружения каналов утечки PII и ICP на основе интеллектуальных технологий. Процедура кодирования заключается в приведении восьми групп признаков к виду тензора различного ранга. Тензоры имеют фиксированную длину, ограниченную количеством записей в базе знаний для каждой группы признаков. Таким образом, возможно детерминировать некоторое приложение в виде набора, координатам которого сопоставляется множество характеристик T:

$$T_{app} = \{T_{Marker_{developer}}, T_{Future}, T_{Component}, T_{Perm}, T_{Lib}, T_{Ident}, T_{Realiz}, T_{Opening}\}, \quad (2)$$

При формировании модели системы противодействия построению цифрового портрета пользователя требуется учитывать не только исполняемые файлы, а также связь между владельцами

сервисов для исключения возможности агрегации данных из различных источников. В качестве обеспечения возможности выявления фактов агрегирования информации из различных приложений представлен способ связывания разработчиков приложений на основе корреляции данных, извлечённых из политик безопасности и контактных данных.

Страница разработчика предоставляет информацию только о разработанных сервисах, на основе которых возможно сформировать следующий тензор:

$$D_{org} = \{m_{package\_name_1}, m_{package\_name_2}, \dots, m_{package\_name_n}\}, \quad (3)$$

Проведение автоматизированного связывания разработчиков сервисов производится на основе извлечения признаков из открытых источников. К выделяемым признакам относится:

– *контактная информация о разработчике:*

$$L_{app} = \{L_{email}, L_{address}, L_{website}\}, \quad (4)$$

где L_{email} – набор почтовых адресов; $L_{address}$, – набор юридических адресов организации, либо фактического расположения; $L_{website}$ – набор ссылок на владельца.

– *пользовательское соглашение:*

$$S_{app} = \{S_{key,} S_{link}, L_{app}\}, \quad (5)$$

где S_{key} – набор ключевых слов; S_{link} – набор ссылок на веб-ресурсы; L_{app} – контактная информация о разработчике.

Таким образом, из множеств 3,4 и 5 формируется цифровой портрет на основе информации, полученной из набора исследуемых приложений, связанных с разработчиком.

$$T_{dev} = \{D_{org}, \bigcup_{i \in A} S_i, \bigcup_{i \in A} L_i\}, \quad (6)$$

Обработка множеств $L_{email}, L_{website}, S_{key,} S_{link}$ различных приложений заключается в их пересечении и поиске общих значений.

$$G = \begin{cases} 1, \text{если } T_{dev_1} \bigcap T_{dev_2} \neq \emptyset \\ 0, \text{если } T_{dev_1} \bigcap T_{dev_2} = \emptyset \text{'} \end{cases} \quad (7)$$

Таким образом возможно представить подход связывания разработчиков в следующем виде:

$$P_{org} = \begin{cases} 1, \text{если } T_{dev_1} \bigcap T_{dev_2} \neq \emptyset \\ 0, \text{если } T_{dev_1} \bigcap T_{dev_2} = \emptyset \text{'} \end{cases} \quad (8)$$

Полученный результат позволяет учитывать степень связности владельцев сервисов при расчёте рисков компрометации персональных данных мобильным устройством. В данном исследовании использовались два уровня статистической значимости результатов связывания разработчиков $P = 0$ – отсутствует связность и $P = 1$ – высокий уровень связности. Результат приведённого способа представляет множество фактических владельцев сервисов или дочерних организаций:

$$H_{corp} = \{D_{org_1}, \dots, D_{org_n}\}, \quad (9)$$

где $D_{org_n} = \{I_{app_1}, \dots, I_{app_n}\}$ – заявленный владелец сервиса.

После проведения процедуры связывания владельцев сервисов требуется оценить возможное качество цифрового портрета пользователя, на основе переданных данных из различных приложений. При формировании U_{org} возможно наличие одинаковых типов данных в множествах U_{PII_i} и U_{ICP_i}, что является избыточным при оценке полноты цифрового портрета. Цифровой портрет пользователя возможно представить в виде:

$$U_{org} = \left\{ \sum_{i=1}^{n} \left| U_{PII_i} \right| - \sum_{i<j}^{n} \left| U_{PII_i} \cap U_{PII_j} \right|, \sum_{i=1}^{n} U_{ICP_i} - \sum_{i<j}^{n} \left| U_{ICP_i} \cap U_{ICP_j} \right| \right\}, \quad (10)$$

где U_{PII_i} – множество обрабатываемых персональных данных приложением; U_{ICP_i} – множество обрабатываемых данных, соотносимых с конкретной личностью.

Функция, выполняющая оценку рисков компрометации персональных данных на мобильном устройстве, обозначена символом δ и рассмотрена в третьей главе. Таким образом, математическую модель оценки рисков компрометации персональных данных на мобильном устройстве возможно представить в следующем виде:

$$S_{dev} = \delta \left(\sum_{i=1}^{n} \{ \boldsymbol{T_{app_i}} : T_{app_i} \in \bar{\omega}_j \}, \sum_{i=1}^{n} U_{\boldsymbol{org_i}}, \sum_{i=1}^{n} P_{\boldsymbol{org_i}} \right), \quad (11)$$

где T_{app_i} – модель представления приложения (формула 2); δ – решающая функция.

В третьей главе приведена сравнительная характеристика выявления возможных каналов утечек персональных данных на основе методов машинного обучения для выявления наиболее

оптимального алгоритма определения рисковых показателей и результаты применения метода определения связности разработчиков мобильных приложений.

Описанные во второй главе компоненты исполняемого файла формируют обучающий набор данных для интеллектуальной системы. Данный набор представлен на содержит 67 360 строк и 2 931 признак. Данные обрабатываются с помощью метода стратификации, т.е. выполняется равномерное распределение количества классов в наборах данных. На данном этапе производится деление на обучающую и тестовую выборку, а также генерируется случайное вхождение классов в данные выборки. Число классификаторов соответствует идентификаторам категорий в Play Market, объединённые в девять групп. Результатом работы классификатора является вероятностный показатель соответствия цифрового портрета приложения определённой группе.

В таблице 1 представлены результаты функционирования обученных моделей нейросетевых классификаторов на тестовых данных.

Табл. 1. Результаты обучения нейросетевых классификаторов

№	Тип метода	Параметры	Описание	Точность
1.	Случайный лес	n_estimators: 600	число деревьев в лесу	0,64
		max_features: sqrt	кол-во функций	
		max_depth: 15,	глубина дерева	
		min_samples_leaf: 18,	число обр. в листах	
		min_samples_split: 23	число обр. для сплита	
2.	K-ближних соседей	n_neighbors: 9	количество соседей	0.42
		weights: distance	метод расчета веса	
3.	Наивный байесовский классификатор	-	-	0,21
4.	Регрессор градиентного бустинга	learning_rate: 0.75	скорость обучения	0.43
		subsample: 0.9	доля выборки обуч.	
		n_estimators: 1000	кол-во этапов повыш.	
		max_depth: 8	max глубина оценок регрессии	
5.	Градиентный бустинг деревьев решений	learning_rate: 0.75	скорость обучения	0,37
6.	Глубокое обучение	activation:relu	функция активации	0,86
		loss: categorical crossentropy	функция потерь	
		epochs: 60	количество эпох	
		optimizer: rmsprop	оптимизатор	

Для определения уровня связности разработчиков были собраны статистические данные по различным признакам из открытых источников и декомпилированного кода приложений. В докладе, в качестве примера, рассмотрены показатели пересечений доменных имён, IP-адресов, доменов адресов электронных почт и географических адресов. В таблице 2 представлены численные характеристики признаков связывания.

Табл. 2. Численные показатели признака почтовых адресов

Источник	Электронные почтовые адреса			Доменные имена		
	Всего	Уникальные	Процент	Всего	Уникальные	Процент
Play Market	48 388	30 323	62	17 925	10 329	58
App Store	5 987	4 059	68	789 396	458 193	58
Исполняемые файлы	51 380	21 531	42	466 5274	748839	16

Полученные цифровые портреты разработчиков на основе формулы 6 позволяют сформировать графы связности по различным показателям (пример на рисунке 1).

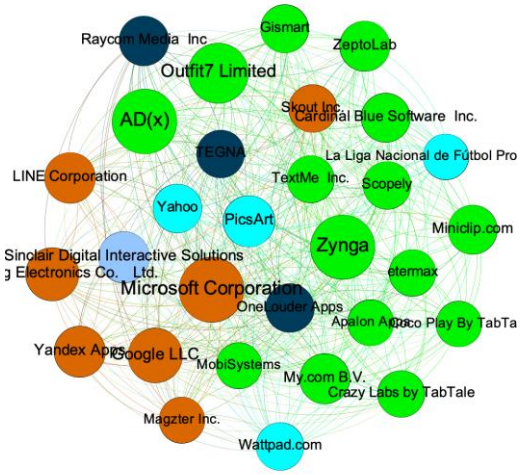


Рис. 1. Граф связности разработчиков по доменным адресам в исполняемых файлах ОС Android

На приведенном примере графа отражены узлы с наибольшим количество связей. Для алгоритмического поиска кластеров и сообществ используется метод из работы «Fast unfolding of communities in large networks» [6]. По имеющемуся набору данных из 44 210 разработчиков было обнаружено 1 588 различных сообществ.

Полученные знания из метода выявления аномальной структуры приложения и выявления сообществ разработчиков позволяют представить состояние мобильного устройства графически. В таблице 3 представлен пример соответствия типа данных значениям количественного показателя.

Табл. 3. Шкала значений персональных данных

№	Тип данных	Значение	№	Тип данных	Значение
1.	IP - адрес	0.001	9.	Геолокационные данные	0.256
2.	Учетные записи в приложениях	0.002	10.	Медиаданные	0.512
3.	Образование, работа	0.004	11.	Отпечаток пальца	1.024
4.	Показатели здоровья	0.008	12.	Сведения о радужной оболочке глаза	2.048
5.	Номер телефона	0.016	13.	Фамилия Имя Отчество	4.096
6.	Различные сообщения	0.032	14.	Домашний или рабочий адрес	8.192
7.	Список вызовов	0.064	15.	Паспортные данные	16.384
8.	Список контактов	0.128	16.	Сведения о банковских картах	32.768

В качестве примера выбраны пять случайных исполняемых файла из набора данных. В таблице 4 представлены основные характеристики приложений, учитывающиеся при принятии решения о состоянии безопасности персональных данных. Источниками данных для таблицы 4 являются механизм разрешений ОС Android вместе с облачным антивирусом Google Play Protected и разработанный *метод*.

Табл. 4. Характеристика приложений встроенным механизмом разрешений с облачным антивирусом Google Play Protected / разработанным методом

№	Тип обрабатываемых данных	Значение, метод/Google	
App1	Вероятность соответствия категории	0.87/0	
	IP - адрес	0.001/0	0.069/0.064
	Образование, работа	0.004/0	
	Список вызовов	0.064	
	Количество разработчиков в связанных сообществах	1/0	
App2	Вероятность соответствия категории	0.88/0	
	IP - адрес	0.001/0	17.091/0.706
	Учетные записи в приложениях	0.002	

	Список вызовов	0.064	
	Список контактов	0.128	
	Медиаданные	0.512	
	Паспортные данные	16.384/0	
	Количество разработчиков в связанных сообществах	3/0	
App3	Вероятность соответствия категории	0.89/0	
	IP - адрес	0.001/0	0.785/0.784
	Номер телефона	0.016	
	Геолокационные данные	0.256	
	Медиаданные	0.512	
	Количество разработчиков в связанных сообществах	2/0	
App4	Вероятность соответствия категории	0.65/0	
	Показатели здоровья	0.008/0	8.458/0.256
	Геолокационные данные	0.256	
	Домашний или рабочий адрес	8.192/0	
	Количество разработчиков в связанных сообществах	5/0	
App5	Вероятность соответствия категории	0.78/0	
	Номер телефона	0.016/0	3.120/1.056
	Различные сообщения	0.032	
	Отпечаток пальца	1.024	
	Сведения о радужной оболочке глаза	2.048/0	
	Количество разработчиков в связанных сообществах	4/0	

Анализ таблицы 4 показал, что современные методы и средства защиты значительно уступают разработанному методу в *полноте обнаружения каналов компрометации персональных данных легитимными сервисами*. Рассмотренные системы защиты не формируют информацию о возможных случаях агрегации или передачи данных между владельцами сервисов, а также отсутствует оценочный показатель соответствия типу категории. Механизм разрешений частично предоставляет пользователю информацию о возможной обработке PII приложением, однако некоторые типы данных также не регулируются. На рисунке 2 представлена лепестковая диаграмма, содержащая количественный показатель персональных данных от механизма разрешений и разработанного метода из таблицы 4.

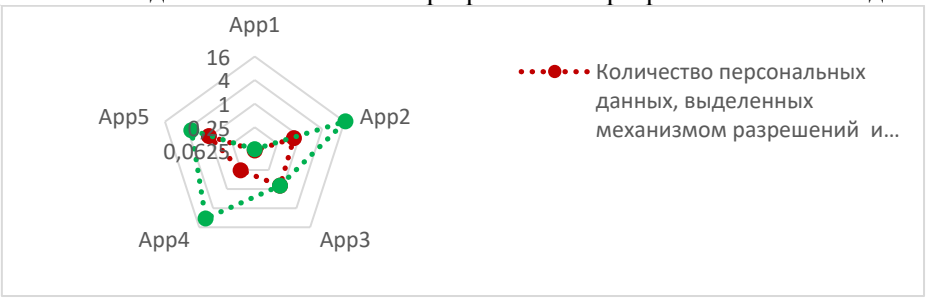


Рис. 2. Лепестковая диаграмма количества персональных данных

Анализ диаграммы показал, что сформированная площадь разработанным *методом* значительно превышает площадь, выделенная механизмом разрешений, что говорит о более высокой степени полноты определения количества ПД. Таким образом, анализ результатов разработанного метода и механизма разрешений, показал, что показатель полноты обнаружения каналов компрометации ПД был улучшен в среднем на ***35%***.

Рисунок 3 содержит показатели разработанного метода из таблицы 4, позволяющих визуально оценить уровень угрозы со стороны приложений. Стоит отметить, что на лепестковой диаграмме возможно производить наглядную установку пороговых значений, при которых достигается эффективность разработанной *системы противодействия утечек персональных данных*

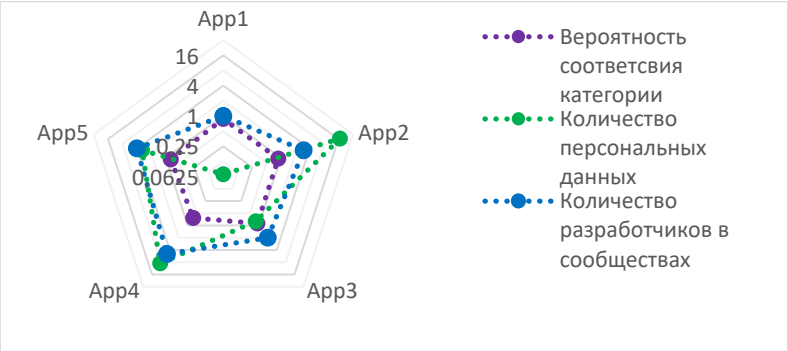


Рис. 3. Лепестковая диаграмма характеристик мобильных приложений, полученных на основе метода обнаружения каналов утечек персональных данных на мобильных операционных системах

Как правило, определение степени конфиденциальности и класса защиты информации является зоной ответственности собственника мобильного устройства или организации, а разработанный метод детектирования каналов утечек персональных данных должен обеспечить выполнение комплекса организационно-технических и технических мер защиты, соответствующих выбранному уровню защиты данных.

В заключении приведены основные результаты и выводы по разработанному методу обнаружения каналов компрометации персональных данных на мобильных операционных системах на основе интеллектуальных средств принятия решения. С целью проверки точности идентификации каналов утечек персональных данных при помощи разработанного метода была проведена серия экспериментов. Проведён сравнительный анализ полученных результатов с существующими исследованиями. В результате был сделан обоснованный вывод, заключающийся в том, что в условиях проведения статического анализа кода и оперативности принятия решения, разработанный метод обеспечивает более высокий уровень защиты конфиденциальных данных.

СПИСОК ЛИТЕРАТУРЫ

1. Linghui Luo; Eric Bodden; Johannes Spath. A Qualitative Analysis of Android Taint-Analysis Results // 34th IEEE/ACM International Conference on Automated Software Engineering (ASE). 2019. С. 102-114.
2. Nattanon Wongwiwatchai, Phannawhat Pongkham, Kunwadee Sripanidkulchai. Detecting personally identifiable information transmission in android applications using light-weight static analysis // Computers & Security 2020. vol.99
3. Jinhong YANG, Chul-Soo KIM, Md Mehedi Hassan ONIK. Aggregated Risk Modelling of Personal Data Privacy in Internet of Things // 21st International Conference on Advanced Communication Technology (ICACT). 2019. С. 425-430.
4. Ajay Kumar Jha, Woo Jin Lee. An empirical study of collaborative model and its security risk in Android // Journal of Systems and Software. 2018. том 137. С. 550-562.
5. Allix K., Bissyand, T.F., Klein J., Le Traon Y. AndroZoo: Collecting Millions of Android Apps for the Research Community // MSR '16: Proceedings of the 13th International Conference on Mining Software RepositoriesMay. 2016. pp. 468-471.
6. Yinglan Feng, Liang Chen, Angyu Zheng, Cuiyun Gao, Zibin Zheng. Assessing the Consistency of Description and Permission in Android Apps. IEEE Access. Computer Science. 2019
7. Chenglin Li, Keith Mills, Di Niu, Rui Zhu, Hongwen Zhang, Husam Kinawi. Android Malware Detection Based on Factorization Machine // IEEE Access. 2019. vol. 7.
8. Салахутдинова К.И.: Методика идентификации исполняемых файлов на основе статического анализа характеристик дизассемблированного кода программ // Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук. 2019
9. Рачковский Д.А. Бинарные векторы для быстрой оценки расстояний и сходств // Кибернетика и системный анализ. 2017. Т. 53. №1. С. 160-183.

Кушко Е.А.
СибГУ им. М.Ф. Решетнева, НУЛ ИИТК, м.н.с,
evgeny.kushko@gmail.com

О СПОСОБЕ ЗАЩИТЫ ОТ ИССЛЕДОВАНИЯ МЕТОДОМ ДИНАМИЧЕСКОЙ РЕКОНФИГУРАЦИИ ТОПОЛОГИИ ВЗАИМОДЕЙСТВИЯ УЗЛОВ

Аннотация: В работе автором предложен новый метод реализации защищенного обмена данными на основе динамической топологии сети, который направлен на повышение уровня защищенности информационных систем, для которых невозможно или недостаточно применить традиционные подходы к защите. Предложенный метод отличается от существующих подходом к маршрутизации и применен в качестве меры защиты для сенсорных сетей. Данный метод позволяет защитить от компрометации не только передаваемые данные, но также и стороны сетевого взаимодействия. Динамическая реконфигурация логической топологии сети не позволяет злоумышленнику обладать долгосрочной информацией об внутрисетевом обмене данными.

Ключевые слова: защищенный обмен данными, защита от исследования, технология защиты движущейся цели, сенсорные сети, динамические сети, маршрутизация.

Актуальность темы исследования. С каждым годом все большее развитие получают информационные системы, которые все глубже проникают во все сферы деятельности, и применяются в том числе и в критических сферах, например, в здравоохранении, энергетике, оборонной промышленности, финансовом секторе и других сферах. Поэтому данные системы представляют все больший интерес для злоумышленников. С каждым годом растет число удаленных сетевых атак на информационные системы и этот факт отмечают аналитики ведущих организаций в сфере информационной безопасности [1].

Несмотря на то, что средства защиты информации совершенствуются, выявляют и блокируют атаки злоумышленников с высокой долей эффективности, статистика инцидентов информационной безопасности показывает высокий процент успешных атак [2]. Это говорит о том, что информационные системы, несмотря на использование средств защиты, имеют уязвимости, которые злоумышленники эксплуатируют.

Этому есть несколько причин. Во-первых, средства защиты информации, например, межсетевые экраны, средства обнаружения и предотвращения вторжений, работают на периметре безопасности. В случае, если злоумышленник проник за этот периметр, то обнаружить его достаточно сложно и, очень часто, он неограничен в своих действиях. Во-вторых, в основе работы средств защиты информации лежит сигнатурный подход, это означает, что если средство защиты не содержит правило, по которому однозначно можно идентифицировать некоторые событие как некую аномалию, то средство защиты информации на это событие не реагирует. Может пройти значительное время пока администраторы безопасности или производители средств защиты информации зафиксируют факт атаки, определят уязвимость и примут соответствующие меры, которые в будущем будут препятствовать злоумышленникам.

В результате для того, чтобы построить эффективную систему защиты информации, необходимо иметь квалифицированный персонал, который будет собирать информацию из различных источников информационной системы: сетевой трафик, файлы журналов, логи и так далее. После чего, эти данные необходимо проанализировать на предмет аномалий, и далее – определить, какие события являются инцидентами информационной безопасности, провести расследование и принять соответствующие меры. Для эффективной защиты, данные действия должны выполняться непрерывно. В результате, защищающиеся вынуждены тратить значительные ресурсы, как финансовые, так и временные.

Для решения этой проблемы исследовательские группы разрабатывают системы автоматизации сбора данных, мониторинга и анализа событий информационной безопасности, но существует также и другой подход, появившийся относительно недавно, а именно защита от исследования.

Перед реализацией самой атаки злоумышленник осуществляет разведку [3]. Защита от исследования предполагает, что без успешно собранных данных об информационной системе, злоумышленник не может осуществить атаку, и препятствует этому, не ограничивая в действиях злоумышленника. В результате, защищающимся не требуется постоянно быть готовым к потенциальным атакам. На текущий момент, системы защиты от исследования находятся на раннем

этапе своего развития: есть некоторые прототипы и теоретические концепты, но конечных решений нет. Кроме того, они имеют некоторые существенные проблемы, которые, как правило, касаются применимости, развертывания и масштабируемости.

Очевидно, что для построения эффективной защиты, необходимо использовать комплексный подход: выстраивать эшелонированную защиту, систему мониторинга, анализа событий и реагирования на инциденты, а также защиту от исследования.

Кроме того, в некоторых информационных системах из-за требований, налагаемых на них, невозможно применить традиционные подходы к защите [4]. Примером такой системы может являться сенсорная сеть. Задачи, решаемые информационными системами такого рода, требуют от сенсорной сети соответствия следующим характеристикам: автономность, надежность, отказоустойчивость и масштабируемость. Сенсорная сеть, как правило, функционирует на устройствах низкой производительности и в условиях низкой пропускной способности. Также в некоторых случаях стоит задача сбора и анализа данных в режиме реального времени, что дополнительно накладывает требования к задержкам при передаче данных. Поэтому и меры защиты, применяемые для сенсорных сетей, направлены прежде всего на обеспечение высокой доступности.

В результате, производители систем, построенных на базе сенсорных сетей, вынуждены разрабатывать собственные протоколы и технологии передачи данных, где-то жертвуя производительностью для повышения уровня защищенности, а в некоторых случаях – наоборот.

Учитывая вышеизложенные факты, автором предложено новое решение – метод реализации защищенного обмена данными на основе динамической топологии сети, который может быть применен для повышения уровня защищенности сторон внутрисетевого обмена в различных информационных системах.

Таким образом, разработка и исследование метода реализации защищенного обмена данными на основе динамической топологии сети является актуальной научно-технической задачей.

Проблемой защиты от сетей исследования, разработками решений для реализации сокрытия конфигурации и архитектуры информационных систем, а также разработками решений для защиты сенсорных сетей занимаются в следующих зарубежных университетах: Университет штата Канзас (Скотт Делоач, Руй Чжуан, Синьмин Оу), Университет штата Северная Каролина (Гарри Перрос), Неаполитанский университет имени Федерико II (Валентина Казола, Алессандра Де Бенедиктис), Технологический институт Флориды (Марко Карвальо, Ричард Форд), а также в научно-исследовательских лабораториях крупных IT-компаний: Cisco Systems (Панос Кампанакис, Цегереда Бейене), Symantec Corpotation (Су Чжан), Athens Information Technology (Танассис Гианнетсос, Тассос Димитриоу).

В Российской Федерации данную проблему изучают в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича (Красов А.В., Петрив Р.Б., Сахаров Д.В., Сторожук Н.Л., Ушаков И.А.), в Краснодарском высшем военном училище (Ворончихин И.С., Иванов И.И., Максимов Р.В., Соколовский С.П.), в АО «Научно-исследовательский институт «Рубин» (Буренин А.Н.), в Военно-космической академии А.Ф. Можайского (Легков К.Е., Терещенко Г.В.), в Московском государственном техническом университете им. Н.Э. Баумана (Бельфер Р.А., Огурцов И.С.).

Цель и задачи исследования. Целью диссертационного исследования является повышение уровня защищенности сторон внутрисетевого обмена методом сокрытия факта взаимодействия узлов.

Для достижения поставленной цели необходимо решить комплекс задач.

1. Проанализировать существующие методы и подходы к защите сети от исследования, способы и решения по сокрытию архитектуры и конфигурации информационной системы, а также классические меры и средства по обеспечению информационных систем различного рода.

2. Разработать алгоритмы, лежащие в основе метода реализации защищенного обмена данными на основе динамической топологии сети.

3. Реализовать и проанализировать эффективность метода реализации защищенного обмена данными на основе динамической топологии сети, а также проанализировать защищенность сенсорной сети, в которой применен метод в качестве меры защиты.

Методология и методы исследования. Объектом исследования является передача данных внутри сети. Предметом исследования является защищенный обмен данными в сети.

Использовались имитационный, лабораторный и реальный типы экспериментов для всестороннего изучения разрабатываемого метода. На первом этапе разрабатывается модель, далее – прототип, и финальная стадия – разработка конечного решения. Каждый этап предполагает анализ эффективности разрабатываемого решения и оценку защищенности сенсорной сети, в которой в

качестве меры защиты применен метод реализации защищенного обмена данными на основе динамической топологии сети.

Научная новизна работы. В результате выполнения исследования:

1. Разработан новый метод, который отличается от существующих подходом к коммутации, позволяющий скрыть стороны внутрисетевого обмена, что значительно затрудняет осуществление анализа перехваченных данных.

2. Разработанный метод применен в качестве меры для прикладной задачи информационной безопасности по обеспечению сокрытия архитектуры и конфигурации информационной системы сенсорной сети, для решения которой ранее не существовало аналогичных технических средств.

3. Разработана методология оценки эффективности применения метода реализации защищенного обмена данными на основе динамической топологии сети и методология оценки защищенности сенсорной сети, в которой метод применен в качестве меры защиты.

Значение для теории состоит в развитии методов обеспечения защиты информационных систем от исследования.

Практическая ценность работы заключается в расширении технических средств по повышению уровня защищенности сторон внутрисетевого обмена информационных систем, построенных на базе различных технологий.

Положения, выносимые на защиту. Основные защищаемые положения:

1. Предложенный метод реализации защищенного обмена данными на основе динамической топологии сети позволяет защитить передаваемые внутри сети данные от анализа.

2. Предложенный метод позволяет скрыть стороны взаимодействия внутри сети.

3. Предложенный метод может быть использован в качестве меры по обеспечению сокрытия архитектуры и конфигурации сенсорной сети.

Все положения соответствуют пункту 8 паспорта специальности 05.13.19 – Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем.

Достоверность и апробация результатов. Достоверность работы подтверждается результатами, полученными с использованием предлагаемого в работе решения, и их сопоставлением с имеющимися современными теоретическими и экспериментальными данными, полученными другими авторами в этой области.

Основные положения и результаты работы были апробированы на конференциях:

1. Международная научно-практическая конференция «Актуальные проблемы авиации и космонавтики», г. Красноярск (2016, 2018, 2019, 2020, 2021, 2022 годы);

2. Международная научно-практическая конференция «Решетневские чтения», г. Красноярск (2018, 2020 годы);

3. Всероссийский конкурс-конференция студентов и аспирантов по информационной безопасности «Сибинфо», г. Томск (2017 год);

4. Международная научно-техническая конференция «Автоматизация», г. Сочи (2019 год);

5. Международная конференция «Apitech: Прикладная физика, информационные технологии и инжиниринг», г. Красноярск (2019 год);

6. Международная конференция «MIP Engineering: Модернизация, инновации, прогресс: передовые технологии в материаловедении, машиностроении и автоматизации», г. Красноярск (2020, 2021 годы);

7. Межвузовская научно-теоретическая конференция в рамках Сибирского форума «Информационная безопасность», г. Новосибирск (2021 год).

Проблема защиты от перехвата и анализа данных. Первая глава диссертационного исследования посвящена проблеме защиты от перехвата и анализа данных, передаваемых внутри сети. В главе приведена и рассмотрена статистика и аналитика инцидентов информационной безопасности ведущих компаний в сфере информационной безопасности, таких как Positive Technologies, Infowatch, Ростелеком Solar, Перспективный мониторинг и других.

Согласно статистике, сети предприятий уязвимы, и в большинстве случаев злоумышленник может преодолеть их внешний сетевой периметр. Отдельно отмечен тот факт, что после проникновения внутрь сети злоумышленник становится трудно детектируем. Как правило, после проникновения за периметр безопасности, злоумышленник осуществляет сетевую разведку. Он практически неограничен во времени и поэтому имеет возможность тщательно спланировать свою атаку.

В главе также рассмотрены требования и меры по обеспечению безопасности внутри сети в случае, когда злоумышленник преодолел внешний сетевой периметр. В главе рассмотрены приказы ФСТЭК №17, №21, №31, №239, методический документ ФСТЭК по мерам защиты информации в ГИС, специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), стандарт ИСО/МЭК 27002, стандарт ИСО/МЭК 27033, стандарт Банка России СТО БР ИББС-1.0, а также международный опыт, изложенный в международном стандарте безопасности данных индустрии платежных карт PCI DSS и руководство по безопасности Национального института стандартов и технологий США (NIST) SP 800-47 для соединения информационных технологических систем.

Рассмотренные меры по обеспечению безопасности передачи данных внутри сети информационной системы имеют широкое распространение, так как являются обязательными для большинства категорий информационных систем. Эти меры имеют апробированные способы и средства их обхода [5, 6].

В главе также рассмотрены новые и пока еще малоиспользуемые технологии для защиты передачи данных внутри сети. В частности, были рассмотрены решения по защите от исследования, а также решения, направленные на сокрытие факта передачи: технология защиты движущейся цели, сетевая стеганография и децентрализованные анонимные сети.

Каждая из технологий имеет свои преимущества, недостатки, уязвимости, а также различные цели и модель угроз. Решения технологии движущейся цели находятся на раннем этапе своего развития и имеет ряд проблем, связанных с внедрением и применимостью [7]. Сетевая стеганография имеет ограничения по задержкам и пропускной способности, и прежде всего направлена на организацию скрытых каналов связи [8]. Анонимные сети направлены на обмен данными через глобальную сеть и неприменимы в случае защиты локальной сети от исследования [9].

Метод реализации защищенного обмена данными на основе динамической топологии сети. Во второй главе рассматривается метод реализации защищенного обмена данными на основе динамической топологии сети, в частности, его алгоритмическое обеспечение.

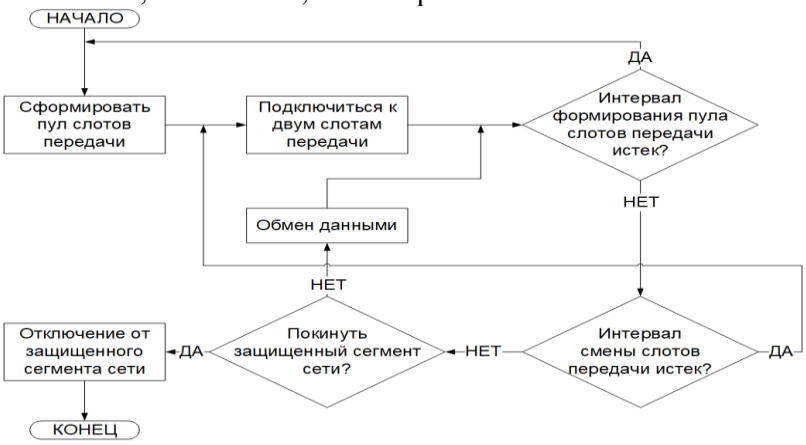


Рис. 1. Алгоритм инициализации защищенного обмена данными

В основе разрабатываемого метода реализации защищенного обмена данными на основе динамической топологии сети лежат принципы технологии движущейся цели. Узлы, участвующие в защищенном обмене данными, перемещаются по слотам передачи и посылают данные, используя групповое вещание. Каждый узел, состоит одновременно в нескольких слотах передачи и перенаправляет полученные данные во все слоты, к которым он подключен в данный момент, т.е. используется лавинная маршрутизация.

На этапе инициализации защищенного обмена, каждый узел участник формирует пул номеров слотов передачи, через которые осуществляется обмен данными, по алгоритму, зависящему от текущей даты, времени и количества участников обмена. Этот пул слотов переформируется через определенные интервалы времени. После формирования пула узел выбирает два слота передачи и подключается к ним. По истечению другого временного интервала, который меньше, чем интервал переформирования пула слотов передачи, узел заново выбирает случайным образом слоты передачи из текущего пула. Общий алгоритм инициализации защищенного обмена данными представлен на рисунке 1.

Рис. 2. Структура пакета данных

Для того, чтобы передать данные, каждый узел-участник защищенного обмена данными формирует пакет данных и отправляет его во все слоты передачи, к которым он в данный момент подключен. Все пакеты данных имеют одинаковый размер, и в случае, если размер передаваемых данных превышает размер пакета, данные дробятся на несколько пакетов, в противном случае – пакет заполняется случайными данными до нужного размера. Пакет, содержит идентификаторы получателя и отправителя, шифруется открытым ключом получателя по алгоритму RSA с длиной ключа 1024 бит. Формат пакета приведен на рисунке 2. Узлы, подключенные к слотам передачи, в которые был отправлен пакет данных, ретранслируют этот пакет во все остальные слоты, пока пакет не окажется в каждом слоте передачи.

Каждый узел-участник выбирает слоты передачи таким образом, чтобы иметь хотя бы одну общий слот передачи с любым другим узлом, который является участником защищенного обмена. Предусмотрена передача данных методом квитирования – данные гарантировано будут переданы от отправителя к получателю.

После ретрансляции каждый узел предпринимает попытку расшифровать пакет и извлечь из его заголовка свой идентификатор. В случае успешной дешифровки пакета данных узел обрабатывает его, в противном – отбрасывает. Алгоритм обработки входящих пакетов данных представлен на рисунке 4. Для того, чтобы ретрансляция не была бесконечной, каждый пакет данных имеет время жизни. После каждой ретрансляции узел, ретранслирующий пакет, увеличивает счетчик пакета, и после достижения предельной величины счетчика, данный пакет далее не ретранслируется. Пакет также отбрасывается в случае, если он превысил максимальный размер или был уже ранее обработан узлом, вне зависимости от того, предназначен он узлу или нет.

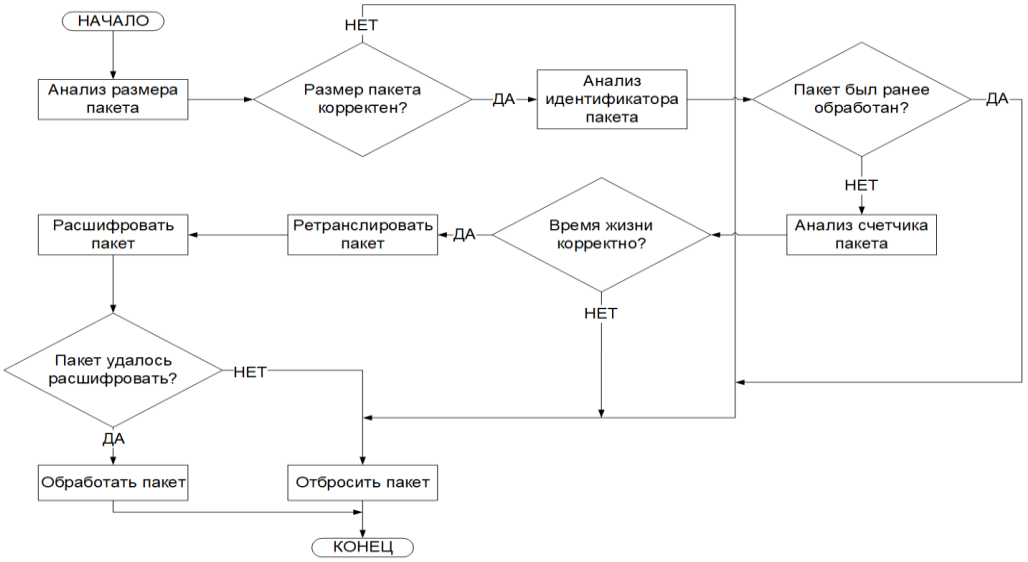


Рис. 4. Алгоритм обработки входящих пакетов данных

При передаче данных таким образом, злоумышленник, осуществляющий перехват и анализ передаваемых данных по сети, не может идентифицировать получателей и отправителей, так как пакеты данных не содержат в явном виде их адреса. Любой пакет данных имеет строго фиксированный размер и зашифрован. Участники защищенного обмена данными переключаются между слотами

передачи, в результате чего логическая структура системы имеет динамическую топологию. Ретрансляция в совокупности с фиксированным размером пакета не позволит установить, какой пакет является запросом или ответом, а какой узел является источником или получателем. В результате злоумышленник не может установить потоки данных и взаимосвязи между узлами, а также не может обладать долгосрочной информацией о логической структуре системы.

Также в главе разработана аналитическая модель такой сети. Аналитическая модель необходима для получения статистики сетевого взаимодействия. При моделировании необходимо учитывать процессы, происходящие как на отдельных узлах, так и в сети в целом.

Практическая реализация разработанного метода. В третьей главе описано практическое решение разработанного метода реализации защищенного обмена данными на основе динамической топологии сети. Данный метод применен в качестве решения прикладной задачи повышения уровня защищенности сенсорной сети.

Практическое решение разработано как сенсорная сеть на базе Wi-Fi. В качестве протокола прикладного уровня выбран MQTT-SN v1.2, так как он предназначен для функционирования в беспроводной сенсорной сети в условиях низкой пропускной способности и низкой производительности конечных устройств, в отличие от обычного протокола MQTT [10]. Кроме того, он поддерживает протокол UDP, который необходим для организации группового вещания на основе сети TCP/IP.

Сенсорная сеть MQTT-SN не поддерживает защищенные соединения: данные передаются незашифрованными UDP дейтаграммами, отсутствуют какие-либо механизмы аутентификации сторон взаимодействия и контроля целостности данных.

MQTT-SN сеть состоит из клиентов, трансляторов и шлюзов, которые в свою очередь соединяются с брокером MQTT, который располагается вне сенсорной сети, средствами стабильного и опционально защищенного TCP-соединения по протоколу обычного MQTT.

Следует отметить тот факт, что клиенту MQTT-SN (сенсору), необходимо знать только открытые ключи транслятора или шлюза, которые направят данные до брокера MQTT. Соответственно, администратор прописывает в устройство открытый и закрытый ключ, а также необходимые конкретному устройству открытые ключи для приема и передачи данных от конкретных узлов, необходимых для решения прикладной задачи.

Программное решение метода реализации защищенного обмена данными на основе динамической топологии сети представляет собой демон, который принимает UDP дейтаграммы от клиента MQTT-SN, инкапсулирует их в пакет данных, структура которого приведена во второй главе, и передает их далее по сети. На рисунке 5 приведена схема такой сенсорной сети. NSPProxy – это программная реализация метода.

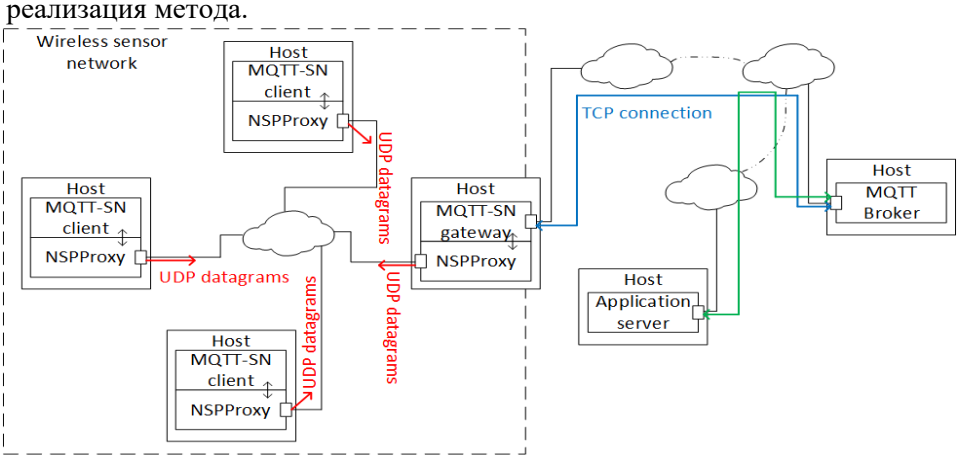


Рис. 5. Схема сенсорной сети

Передача данных таким способом позволяет скрыть роль каждого узла в разработанной системе, так как весь объем трафика, передаваемый между узлами, распределен между всеми участниками системы, а пакеты данных имеют одинаковый размер, при этом логическая структура системы постоянно изменяется через временные интервалы.

Связи между конкретными узлами скрыты среди абсолютно идентичных потоков данных, а сами данные защищены шифрованием. Отправители и получатели данных скрыты из-за отсутствия явной адресации пакетов.

Алгоритм выбора новых слотов передачи выглядит следующим образом. В момент времени, когда минуты системного времени кратны 10, вычисляется два параметра – смещение и шаг. На основе этих двух параметров алгоритм выбора слотов передачи формирует пул адресов мультикаст-групп.

Смещение вычисляется как сумма значения текущего дня и значение умножения значения текущего часа и значения текущего месяца (формула 2.1).

$$offset = hour * month + day, \quad (2.1)$$

где *offset* – значение смещения, *hour* – значение текущего часа, *month* – значение текущего месяца и *day* – значение текущего дня.

Шаг вычисляется по формуле 2.2.

$$step = \frac{minute}{10} + 1, \quad (2.2)$$

где *step* – множитель и *minute* – значение текущих минут.

Диапазон выбора формируется следующим образом. Первый и второй октет адреса мультикаст-группы статичны и равны 239 и 41 соответственно. Третий октет и четвертый октет вычисляются по формулам 2.3 и 2.4 соответственно.

$$net^3 = \frac{(offset+step*i)}{255}, \quad (2.3)$$

где net^3 – значение третьего октета мультикаст-группы, *offset* – значение смещение, *step* – значение шага, а *i* принимает значения от 1 до размера диапазона выбора.

$$net^4 = (offset + step * i) \,\%\, 255, \quad (2.4)$$

где net^4 – значение третьего октета мультикаст-группы, *offset* – значение смещение, *step* – значение шага, а *i* принимает значения от 1 до размера диапазона выбора.

Для того, чтобы между всеми участниками был как минимум один путь доставки, число адресов в пуле не должно превышать количество участников обмена более чем на 1. Данный алгоритм это гарантирует.

Также в третьей главе проанализирована эффективность разработанного решения и защищенность сенсорной сети.

Для проведения анализа и тестирования подготовлен тестовый стенд из восьми машин на базе беспроводного маршрутизатора Mikrotik RB941-2nD-TC на частоте 2.4 ГГц. Максимальная ширина канала составила 300 Мбит/с, которая была поделена между участниками обмена данными.

Практический анализ эффективности разработанного решения и защищенности сенсорной сети строится на основе двух практических экспериментов:

1. эксперимент на определение характера распределения пакетов внутри системы;
2. эксперимент на определение характеристик производительности передачи данных.

Результаты и описание экспериментов приведены в статье [11]. Равномерное распределение всего трафика указывает на то, что связь между двумя узлами скрыта среди множества идентичных потоков данных. Характеристики производительности передачи данных в разработанной системе: средняя пропускная способность – 320 кбит/с, а задержка – 28 мс.

Основным недостатком текущей реализации является использование Wi-Fi в качестве основы сенсорной сети. Wi-Fi имеет централизованную структуру, а соответственно – единую точку отказа. Типичная архитектура сети Wi-Fi – это звезда или дерево. Данный факт в совокупности с относительно невысокой дальностью действия сети ограничивает монтаж конечных устройств сенсорной сети.

Механизм добавления новых узлов в сети Wi-Fi также создает сложности в масштабировании сенсорной сети. Wi-Fi – это высокоскоростной стандарт связи, но за высокой пропускной способностью следует и повышенное энергопотребление. Скорости, поддерживаемые стандартом Wi-Fi, избыточны для сенсорной сети, гораздо важнее низкое энергопотребление. Несмотря на широкую распространённость данного беспроводного стандарта существуют еще более доступные по цене решения, которые лишены указанных недостатков.

Однако, эти недостатки не относятся к самому разрабатываемому методу реализации защищенного обмена данными на основе динамической топологии сети.

В ходе экспериментов установлено, что на показатели производительности передачи данных влияет количество информационных потоков, проходящих через конкретный узел-ретранслятор. Текущая реализация механизма формирования сети не гарантирует количество проходящих информационных потоков через узел-ретранслятор, поэтому необходимо оценить потери производительности в зависимости от количества информационных потоков.

Для этого разработана имитационная модель в среде GPSS, блок-схема процесса моделирования которой представлена на рисунке 6. В таблице 1 представлены результаты эксперимента.

С увеличением количества информационных потоков, проходящих через узел-ретранслятор, возрастают и временные характеристики всех параметров. Так как метод предполагает лавинную маршрутизацию, то все узлы сети обрабатывают одинаковое количество информационных потоков. Чем больше узлов-ретрансляторов располагается между узлом-отправителем и узлом-получателем, тем сильнее падает пропускная способность и растут задержки.

Рис. 6. Блок-схема процесса моделирования, однопоточный ретранслятор

В случае применения данного метода в качестве меры повышения уровня защищенности сенсорной сети, характеристики производительности допустимы, так как такие сети генерируют относительно небольшой объем сетевого трафика. Однако для систем чувствительных к задержкам, такое решение может быть неприменимо.

Табл. 1. Результаты моделирования, однопоточный ретранслятор

Показатель\Кол-во информ. потоков	1	2	10	100	1000
Коэффициент использования	0,39	0,71	0,99	0,99	1
Среднее время обработки (мс)	5,04	5,16	5,04	5,02	4,99
Среднее время в очереди запроса (мс)	21,60	24,79	8,59	1000,94	9981,04
Среднее время в очереди ответа (мс)	4,52	8,01	2,19	739,37	7473,35
Средняя длина очереди запросов	0,83	1,71	0,68	99,7	999,7
Средняя длина очереди ответов	0,17	0,55	0,11	73,64	748,53

Дальнейшее исследование необходимо направить на снижение влияния узлов-ретрансляторов между узлом-отправителем и узлом-получателем данных на характеристики производительности, в условиях функционирования данного метода на устройствах низкой производительности.

Основные результаты и выводы. Существующие меры по обеспечению безопасности локальной вычислительной сети информационной системы заключаются в построении эшелонированной защиты всей сети и её сегментов. Однако, по статистике инцидентов, злоумышленники успешно преодолевают эти периметры безопасности. После проникновения

злоумышленник неограничен во времени и, очень часто, в действиях для развития и планирования атаки, так как его достаточно сложно обнаружить.

Существующие стандартные меры по сокрытию архитектуры и конфигурации информационной системы, противодействию анализу и перехвату сетевого трафика, по защите от исследования, заключаются в противодействии несанкционированного доступа к сети и в контроле санкционированного доступа с использованием традиционных технических средств защиты информации.

Перспективные новые технологии для защиты сети от исследования имеют существенные недостатки, например, наличие центрального узла, высокая сложность внедрения и развертывания, низкое качество связи, нарушение прочих требований безопасности, влияние на легитимные службы и сервисы, и другие.

Разработанный метод реализации защищенного обмена данными на основе динамической топологии сети не содержит центральные узлы, построен на базе стандартных технологий, которые поддерживаются большинством проводных и беспроводных сетевых устройств. Данный метод не влияет на другие сервисы, службы и другие требования безопасности. Разработанный метод позволяет защитить от компрометации передаваемые данные и стороны сетевого взаимодействия, а также позволяет защитить всю сенсорную сеть от исследования.

В текущей реализации узлы-ретрансляторы значительно влияют на общую производительность системы, поэтому дальнейшее исследование необходимо направить на снижение этого влияния, например, путем использования более производительных узлов для осуществления маршрутизации.

Таким образом, в исследовании был разработан метод реализации защищенного обмена данными на основе динамической топологии сети. Цель исследования была достигнута, а задачи – выполнены.

СПИСОК ЛИТЕРАТУРЫ

1. Positive Research 2021 [Электронный ресурс]. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2021-rus.pdf (дата обращения: 31.07.2022);
2. Positive Research 2020 [Электронный ресурс]. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2020-rus.pdf (дата обращения: 31.07.2022);
3. Котенко И.В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак / И.В. Котенко, М.В. Степашкин // Труды Института системного анализа Российской академии наук. – 2007. – Т. 31. – С. 126;
4. Русанов П.И. Особенности работы беспроводных сенсорных сетей / П.И. Русанов, А.Г. Юрочкин // Вестник Воронежского института высоких технологий. – 2019. – № 4 (31). – С. 79–81;
5. Germann, B. OFFWall: A Static OpenFlow-Based Firewall Bypass / B. Germann, M. Schmidt, A. Stockmayer, M. Menth // DFN-Forum Kommunikations technologien. Günzburg, Germany, 27–28 June 2018. – P. 43–55;
6. Rosenberg I. Bypassing system calls-based intrusion detection systems / I. Rosenberg, E. Gudes // Concurrency and Computation: Practice and Experience. – 2017. – № 29;
7. Zhuang R. Towards a theory of moving target defense / R. Zhuang, S.A. DeLoach, X. Ou // Proceedings of the First ACM Workshop on Moving Target Defense. Scottsdale, Arizona, USA, 3 November, 2014. – P. 31–40;
8. Пескова О. Ю. Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет / О.Ю. Пескова, Г.Ю. Халабурда // Материалы Всероссийской объединенной конференции «Интернет и современное общество». Санкт- Петербург, 10–12 октября, 2012. – С. 348–354
9. Negi N. Comparison of anonymous communication networks – Tor, I2P, Freenet // International Research Journal of Engineering and Technology. – 2017. – Т. 4. – № 7;
10. Stanford-Clark A. Mqtt for sensor networks (mqtt-sn) protocol specification / A. Stanford-Clark, H.L. Truong // International business machines (IBM) Corporation version. – 2013. – V. 1. – №. 2. – P. 1–28;
11. Кушко Е.А. Метод реализации защищенного обмена данными на основе динамической топологии сети // Вестник СибГУТИ. – 2020. – № 4. – С. 39-52.

Лимов М.Д.
Самарский университет, кафедра безопасности информационных систем, аспирант
maiklim@mail.ru

СПОСОБ РЕГИСТРАЦИИ ВИБРОАКУСТИЧЕСКИХ СИГНАЛОВ НА ОСНОВЕ МЕТОДА КОГЕРЕНТНОЙ ОПТИКИ – СПЕКЛ-ИНТЕРФЕРОМЕТРИЯ НА ОДИНОЧНОМ СПЕКЛЕ

Аннотация: В статье представлены результаты теоретических и экспериментальных исследований, связанные с использованием метода когерентной оптики на основе спекл-интерферометрии на одиночном спекле. Представлена оптическая схема спекл-интерферометра на одиночном спекле для регистрации виброакустических сигналов. Данная оптическая схема позволяет одновременно наблюдать исследуемый объект и регистрировать его виброакустическое поведение. Разработана математическая модель для анализа выходного сигнала с точечного фотодетектора спекл-интерферометра. На основе математической модели проведен теоретический анализ поведения выходного сигнала в зависимости от амплитуды виброакустического сигнала. Показано, что выходной сигнал с точечного фотодетектора спекл-интерферометра зависит как от расположения точечного фотодетектора относительно одиночного спекла, так и от амплитуды виброакустического сигнала. Показано, что выходной сигнал с точечного фотодетектора полностью соответствует виброакустическому сигналу, если его амплитуда меньше или равна λ/8, а точечный фотодетектор располагается на спекл-картине точно посередине между максимальным и минимальным значением интенсивностей спекл-картины.

Ключевые слова: бесконтактные методы измерения, виброакустический сигнал, спекл-структура, интерферометрия, спекл-интерферометрия, обработка сигнала.

ВВЕДЕНИЕ

Одним из самых опасных каналов утечки информации является виброакустический. Воздействие акустических волн на поверхность твердого тела приводит к возникновению в нем вибрационных колебаний в результате виброакустического преобразования. Эти колебания, распространяющиеся в твердой среде, могут быть зарегистрированы специальными техническими средствами, а речевая информация, содержащаяся в виброакустическом поле, при определенных условиях может быть восстановлена [1,2].

Виброакустический канал также позволяет исключить непосредственный контакт с источником акустического сигнала. Для этого могут использоваться различные средства регистрации сигнала: как контактные, так и бесконтактные. Направленные средства регистрации сигнала воспринимают распространяющуюся в среде акустическую волну без прямого контакта с объектом. Узкая диаграмма направленности позволяет регистрировать акустический сигнал на больших расстояниях, за счет узкой направленности фиксируются только та часть акустических волн, которая необходима, исключая побочные звуковые волны. Различают три вида направленных средств регистрации речевого сигнала: параболические, с плоской фазированной решеткой и синфазные трубчатые. Все три вида основаны на различных свойствах акустического сигнала, как волны, и позволяют регистрировать речевой сигнал на сравнительно больших расстояниях [1, 3]. Однако, они имеют ряд недостатков:

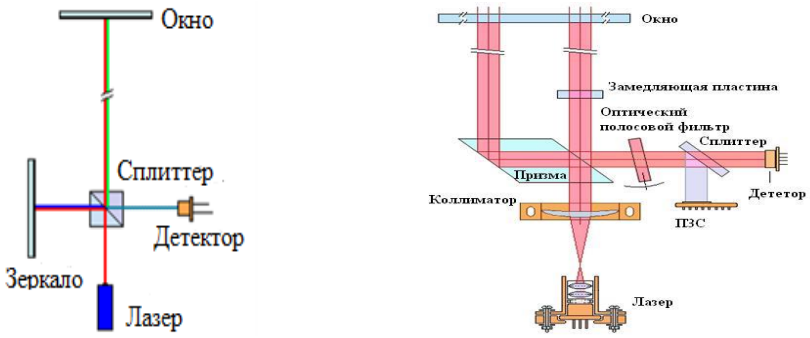
– помимо информационного сигнала такие средства регистрируют различные паразитные шумы, которые могут ослабить сигнал;

– низкая чувствительность регистрации виброакустических сигналов..

Наиболее практичными являются устройства, которые регистрируют виброакустический сигнал и передают информацию не по воздуху, а с использованием других полей. В последнее время уделяют особое внимание оптическим методам, которые передают информацию по оптическому каналу.

Оптические средства регистрации виброакустического сигнала основаны на модуляции излучения вибрирующим объектом, который совершает механические колебания под действием акустической волны. Первоначально использовался свет от ламп накаливания, который при помощи набора линз узким пучком фокусировался на вибрирующий объект. Для этого метода требовались мощные источники излучения и применение хорошей фокусирующей оптики для создания направленного излучения. С открытием лазеров эти проблемы были устранены, т. к. лазерное излучение монохроматично, когерентно, имеет малый угол расходимости и большую мощность.

Регистрация виброакустического сигнала оптическими методами происходит на основе обработки зеркально отраженного от вибрирующего объекта промодулированного оптического излучения. Для повышения чувствительности были предложены интерферометрические методы (Рис.1), которые позволяли повысить чувствительность регистрации вибросмещений сравнимую с длиной волны [4].



а б

Рис.1. Схема лазерных интерферометрических микрофонов:
а – без выравнивания оптических путей; б – с выравниванием оптических путей

Основным недостатком оптических методов регистрации виброакустического сигнала является то, что необходимо иметь зеркально отражающую вибрирующую поверхность. Исходя из этого, отражающая вибрирующая поверхность должна быть оптически гладкой, что практически невозможно в не лабораторных условиях. Кроме того, регистрация зеркально отраженного излучения накладывает жесткие условия к юстировке всей оптической системы. Как правило, отражающие поверхности являются шероховатыми. Наличие неровностей или шероховатостей размером сравнимым с длиной волны, приводит к рассеянию падающего излучения, и, следовательно, затрудняют регистрацию виброакустического сигнала указанными оптическими методами.

При отражении когерентного лазерного излучения от шероховатой поверхности образуется в пространстве над поверхностью сложная интерференционная картина, называемая спекл-структурой [5, 6]. Динамическое изменение поверхности, под воздействием акустического сигнала, приводит к изменению пространственной структуре спекл-картины, и, следовательно, регистрация изменения структуры спекл-картины позволяет восстановить исходный акустический сигнал.

Теоретические и экспериментальные исследования в работах [7-15] показали, что применение спекл-структур является перспективным направлением, для применения в различных областях науки и техники.

ОСНОВЫ СПЕКЛ-ИНТЕРФЕРОМЕТРИИ

Интерферометрические методы, такие как спекл-интерферометрия, являются уникальными бесконтактными измерительными технологиями, позволяющими одновременно контролировать перемещение точек по всей наблюдаемой поверхности объекта. Кроме того, спекл-интерферометрия не предъявляет жестких требований к качеству исследуемой поверхности, в отличие от классической интерферометрии.

Как сказано выше, отраженное рассеянное когерентное лазерное излучение от объекта образует сложную пространственную интерференционную картину – спекл-структурой. Спекл-структуры классифицируются следующим образом: объективные и субъективные спекл-структуры. Объективные спекл-структуры – это интерференционные картины образованные рассеянным когерентным излучением в пространстве над отражающей поверхностью. Субъективные спекл-картины – это интерференционные картины, образующиеся в плоскости сфокусированного изображения исследованного объекта оптической системой. Следовательно, субъективная спекл-картина на сфокусированном изображении, точно соответствует спекл-картине на исследуемом объекте. Смещение объекта приводит к изменению как субъективных, так и объективных спекл-картин. Следовательно, по изменению спекл картины можно решить обратную задачу по определению смещения исследуемого объекта.

Усредненный поперечный размер одиночного спекла h определяются следующим уравнением [5]:

$$h = 1{,}22\,\lambda/\alpha\,, \qquad (1)$$

где λ – длина волны лазера; α – отношение диаметра входной апертуры D к расстоянию l до сфокусированного изображения на фотоматериале, для субъективных спекл-картин и отношение диаметра освещенной части исследуемой поверхности D к расстоянию l до плоскости наблюдения объективных спекл-структур.

Так как, субъективная спекл-картина на сфокусированном изображении, точно соответствует спекл-картине на исследуемом объекте то, сфокусируемся на исследовании их поведения в зависимости от динамики исследуемой поверхности. Динамические перемещения поверхности приводит к изменению интенсивности и пространственных размеров спекл-картины, следовательно, измерение изменения этой спекл-картины позволяет решить обратную задачу – определить динамическое поведение исследуемой поверхности. Оценим изменения размеров спекл-структур в зависимости от смещения поверхности. Смещение поверхности исследуемого объекта на некоторую величину $\pm\Delta r$ приводит к смещению сопряжённой точки в плоскости изображения на величину $\pm\Delta l$. В этом случае поперечный размер спекла измениться, согласно уравнению (1), на величину:

$$\Delta h = 1{,}22\lambda(\pm\Delta l)/D. \qquad (2)$$

При регистрации оптической системой удаленных объектов смещение Δr приводит к смещению в плоскости изображения на величину $\Delta l = m\Delta r$, где m – увеличение оптической системы. Как правило, m много меньше 1. Следовательно, изменение усредненного размера одиночного спекла согласно уравнению (2) стремится к нулю так как $\Delta l/l$, стремиться к нулю. Таким образом, проводить измерение динамических перемещений поверхности по геометрическим размерам спеклов практически не возможно.

Для повышения чувствительности регистрации динамических перемещений поверхности, применяется метод спекл-интерферометрии – использование опорной волны. При наложении опорной волны на субъективную спекл-картину образуется вторичная интерференционная картина, покрывающая субъективную спекл-картину сфокусированного изображения исследуемого объекта (Рис. 2). При этом, смещение поверхности на величину сравнимую с длинной волны, в зависимости от используемой оптической схемы, приводит к изменению интенсивности одиночных спеклов в спекл-картине от минимальной, до максимальной и наоборот. Следовательно, по динамике изменения интенсивности одиночного спекла можно определить амплитуду вибрационных смещений поверхности с точностью меньше чем длина волны, используемого лазерного излучения.

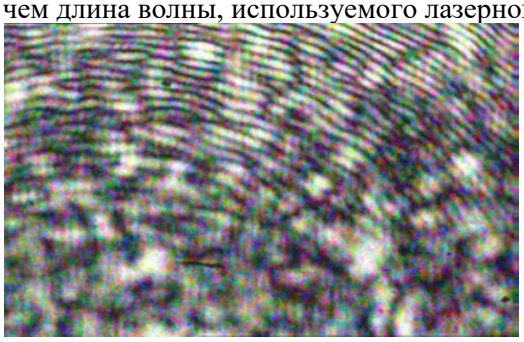


Рис. 2. Фотография исследуемой поверхности, покрытой спекл-структурой и вторичными интерференционными полосами

В работах [13-15] предложен способ исследования виброакустических сигналов на основе спекл-интерферометрии одиночного спекла, образованного за счёт рассеянного лазерного излучения от исследуемой конструкции. Его преимущество перед существующими методами спекл-интерферометрии заключается в высокой интерферометрической чувствительности к измерению смещений, и проводить измерения виброакустических сигналов в реальном времени.

СПОСОБ РЕГИСТРАЦИИ ВИБРАЦИЙ НА ОСНОВЕ СПЕКЛ-ИНТЕРФЕРОМЕТРИИ ОДИНОЧНОГО СПЕКЛА

Рассмотрим оптическую схему спекл интерферометра для регистрации виброакустического сигнала (Рис. 3). Излучение лазера 1, проходя через оптическую систему 2, преобразуется в световую волну для освещения исследуемого объекта и образования опорной волны. С помощью светоделителя 3 излучение лазера 1 расщепляется на два пучка, один из которых (предметный пучок) освещает поверхность исследуемого объекта 5, а другой направляется на опорное зеркало 4 для формирования опорной световой волны (опорный пучок). Отраженное излучение от поверхности объекта 5 и опорного зеркала 4 с помощью светоделителей 3 и 7 и оптической системы 6 формируют одновременно сфокусированное изображение поверхности исследуемого объекта 5 в плоскости ПЗС-матрицы

цифровой видеокамеры 8 и в плоскости быстродействующего точечного фотодетектора 9. С помощью источника акустического (речевого) сигнала 11 возбуждают колебания исследуемой конструкции 5. Информация с ПЗС-матрицы цифровой видеокамеры 8 и с быстродействующего точечного фотодетектора 9 поступает на компьютер 10 для последующей обработки и визуализации.

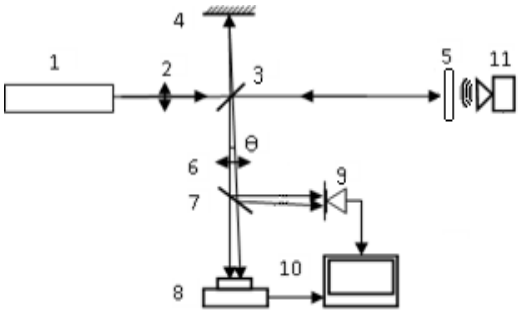


Рис. 3. Оптическая схема спекл интерферометра

Использование опорной волны, как сказано выше, в оптической схеме приводит к тому, что сфокусированное изображение исследуемой поверхности покрыто субъективной спекл-структурой, которая промодулирована вторичными интерференционными полосами (Рис. 2) для последующей обработки и визуализации.

Период d вторичных интерференционных полос определяется хорошо известной формулой [16]:

$$d = \lambda/(2\sin\theta/2) \tag{3}$$

где θ – угол схождения между опорным лазерным излучением и сфокусированным рассеянным лазерным излучением от поверхности конструкции.

В работах авторов [13-15] показано, что при регистрации виброакустического сигнала методом спекл-интерферометрии на одиночном спекле необходимо выполнить следующие условия: максимальный размер H рабочей поверхности быстродействующего точечного фотодетектора 9 должен быть согласован с размером h одиночного спекла субъективной спекл-структуры и периодом d вторичных интерференционных полос, образованных в плоскости фотодетектора. Соотношение между этими величинами должно соответствовать следующему неравенству:

$$d>h>H \tag{4}$$

Данные условия выполняются подбором параметров оптической схемы – значение диафрагмы и фокусного расстояния оптической системы 6, угла схождения θ между опорным и предметным пучками за счет расположения опорного зеркала 4.

Любые изменения вибрирующей поверхности приводят к изменению интенсивности спекл-структуры в плоскости изображений.

Рассмотрим теоретически изменение интенсивности света в плоскости точечного быстродействующего фотодетектора.

Запишем значения вектора напряженности электрического поля на фотодетекторе для каждой волны (предметной и опорной) в следующем виде:

$$\boldsymbol{E}_1=\boldsymbol{E}_0\, e^{i(kx1-\omega t+\varphi)}, \tag{5}$$

$$\boldsymbol{E}_2=\boldsymbol{E}_0\, e^{i(kx2-\omega t+\varphi)}, \tag{6}$$

где $\boldsymbol{E}_0$ – амплитуда напряженности электрического поля электромагнитного поля;

$k=2\pi/\lambda$ – волновое число;

ω – круговая частота лазерного излучения;

φ – начальная фаза;

x_1 – оптический путь опорного пучка – расстояние от делителя до фотоприемника;

x_2 – оптический путь предметного пучка – расстояние от делителя до исследуемого объекта и от объекта до фотоприемника.

В этом случае оптический путь предметного луча x_2, запишется в следующем виде:

$$x_2=r_0+r\pm 2\Delta r, \tag{7}$$

где r_0 – расстояние от делителя до объекта исследования;

r – расстояние от объекта исследования до фотодетектора;

$\pm\Delta r$ – величина смещения исследуемой поверхности.

Так как фотоприемник регистрирует интенсивность, распределение интенсивности в интерференционной картине записывается в следующем виде:

$$I(x,t)=|\boldsymbol{E}_1+\boldsymbol{E}_2|^2\approx 2\boldsymbol{E}^2_0\{1+cos[k(x_1-r_0-r\mp 2\Delta r)]\} \quad (8)$$

Как следует из уравнения (8) интенсивность спекла меняется от минимального до максимального значения (или наоборот) при изменении значения его фазы на $\pm\pi(2n+1)$, (где n=0,1,2...), которая связана с динамикой исследуемой поверхности, то есть с изменением Δr во времени.

Из анализа выражения (8) следует, что изменение интенсивности одиночного спекла в спекл-структуре на входе фотодетектора преобразуется в изменение выходного напряжения фотодетектора, которое записывается следующим образом:

$$u(t)=A+B\,cos[\varphi(0)\mp\varphi(t)]\,, \quad (9)$$

где $u(t)$ – выходное напряжение электрической схемы фотоприемника;

A – выходное напряжение смещения, которое связано со средней интенсивностью спекла;

B – амплитуда полезного выходного напряжения, которое определяется параметрами оптико-электронной схемы;

$\varphi(0)=k(x_1-r_0-r)$ – начальное значение разности фаз между опорным и объектным пучками в плоскости регистрации, оно может меняться, но остается постоянным во время измерений;

$\varphi(t)=\pm 2k\Delta r$ – изменение фазы спекла, связанное с изменением оптического пути при динамических смещениях исследуемой поверхности.

Рассмотрим изменение интенсивности в плоскости быстродействующего точечного фотодетектора для рассматриваемой оптической схемы (Рис. 3)

При колебаниях исследуемой поверхности происходящих по гармоническому закону $\varphi(t)$ запишется в следующем виде:

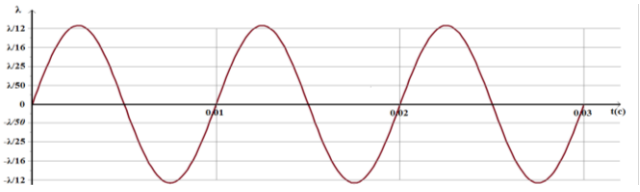
$$\varphi(t)=\pm 2kasin(\omega t) \quad (10)$$

где a – амплитуда колебаний исследуемой поверхности;

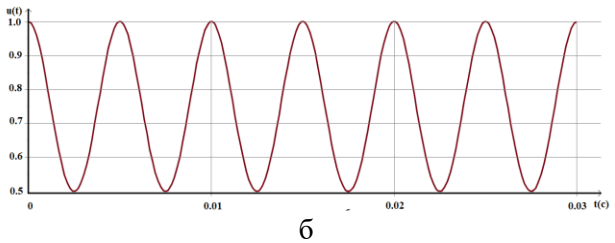
ω – частота колебаний исследуемой поверхности.

Анализ уравнения (9) показывает, что форма выходного сигнала с фотодетектора зависит как от амплитуды колебания a исследуемой поверхности, так и от расположения фотодетектора в начальный момент времени исследований, то есть от значения начальной разности фаз $\varphi(0)$.

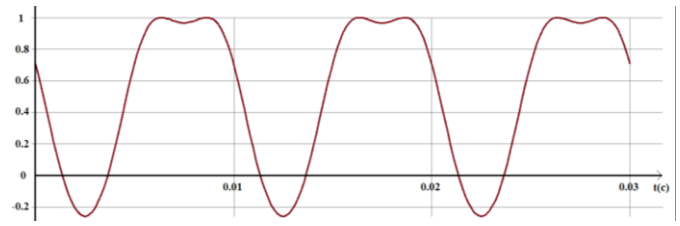
На Рис. 4 и 5 представлены графики теоретических расчетов зависимости выходного сигнала с фотодетектора от колебаний поверхности с амплитудой $\lambda/12 < a < \lambda/8$ (Рис. 4а) и с амплитудой $a = \lambda$ (Рис. 5а) согласно выражению (9). Расчёты выполнены для начальных значений разности фаз: $\varphi(0) = 0$ (Рис. 4б и Рис. 5б); $\varphi(0) = \pm\pi/4$ (Рис. 4в и Рис. 5в); $\varphi(0) = \pm\pi/2$ (Рис. 4г и Рис. 5г). Величины выходного сигнала и амплитуды колебаний исследуемой точки поверхности представлены в относительных единицах.



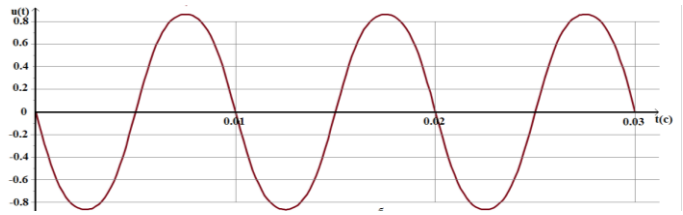
а



б

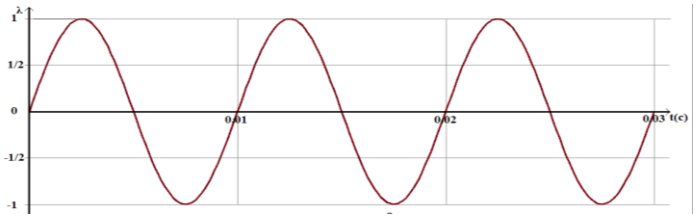


в

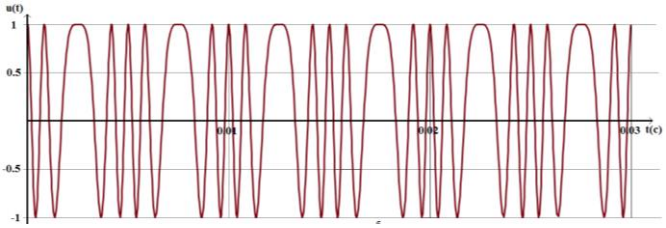


г

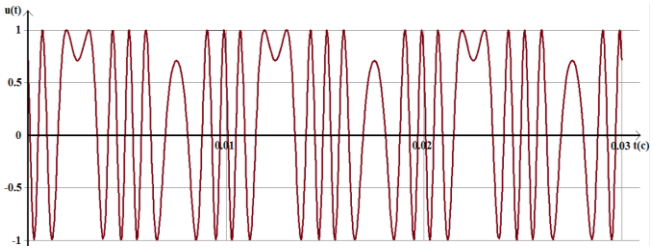
Рис. 4. Поведение выходного сигнала с фотодетектора при колебаниях поверхности с амплитудой меньше λ/8



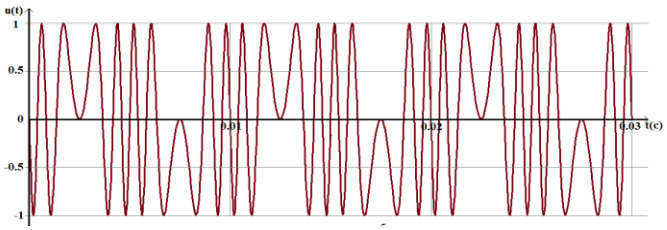
а



б



в



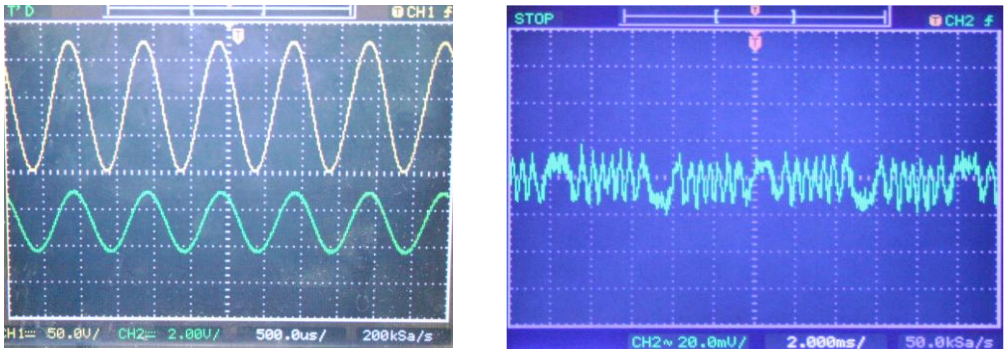
г

Рис. 5. Поведение выходного сигнала с фотодетектора при колебаниях поверхности с амплитудой больше λ/8

Как следует из анализа уравнения (9) и представленных графиков, при колебаниях исследуемой точки поверхности с амплитудой меньше или равной λ/8 выходной сигнал с фотодетектора пропорционален этим колебаниям. При расположении фотодетектора в начальный момент времени в области спекл-картины с максимальной или минимальной интенсивностью ($\varphi(0) = 0$; $\varphi(0) = \pi$) амплитуда выходного сигнала с фотодетектора пропорциональна амплитуде соответствующих колебаний исследуемой поверхности, однако, частота выходного сигнала с фотодетектора увеличивается в два раза по сравнению с частотой колебаний исследуемой поверхности. Так же, при этих условиях из анализа уравнения (9) следует, что чувствительность по амплитуде спекл-интерферометра уменьшается. При расположении фотодетектора в начальный момент времени в области спекл-картины с интенсивностью равной среднему значению между максимальной и минимальной интенсивностями спекл-картины, амплитуда выходного сигнала с фотодетектора пропорциональна амплитуде соответствующих колебаний исследуемой поверхности, а частота колебаний выходного сигнала с фотодетектора равна частоте колебаний исследуемой поверхности (Рис. 4г). В этом случае, чувствительность по амплитуде спекл-интерферометра максимальна. При расположении фотодетектора в начальный момент времени в области спекл-картины с интенсивностью не равной максимальной или минимальной, а также среднему значению между максимальной и минимальной интенсивностями, выходной сигнал с фотодетектора искажается и не соответствует форме колебаний исследуемой поверхности (Рис. 4в). На рисунке 6а представлена фотография осциллограммы выходного сигнала с фотодетектора для колебаний исследуемой поверхности с амплитудой λ/12 и частотой 10^3 Гц. На осциллограмме верхний сигнал соответствует колебаниям исследуемой поверхности, а нижний сигнал описывает поведение выходного сигнала фотодетектора.

При амплитудах колебаний исследуемой поверхности больше λ/8 (Рис. 5а) образуются осциллирующие пакеты. При расположении фотодетектора в начальный момент времени в области спекл-картины с начальным значением разности фаз $\varphi(0) = 0$ или $\varphi(0) = \pi$, период следования пакетов в два раза меньше периода колебаний исследуемой поверхности. В остальных случаях период следования пакетов соответствует периоду колебаний исследуемой поверхности. Однако, независимо от расположения точечного фотодетектора, следование пакетов соответствует спаду и подъёму колебательного процесса, то есть полной амплитуде. Следовательно, количество осцилляций внутри пакета определяет величину полной амплитуды колебаний. На рисунке 6 представлена экспериментальная осциллограмма выходного напряжения с быстродействующего точечного фотодетектора при амплитудах колебаний исследуемой поверхности больше λ/8. На рисунке 6б представлена фотография осциллограммы выходного сигнала с фотодетектора для колебаний исследуемой поверхности с амплитудой 15λ/4 и частотой 10^2 Гц.

Как видно, экспериментальные и теоретические результаты исследований полностью совпадают (Рис.4-6).



а б

Рис. 6. Осциллограмма выходного сигнала с фотодетектора: а – амплитуда колебаний исследуемой поверхности меньше λ/8; б – амплитуда колебаний исследуемой поверхности больше λ/8

Таким образом, при измерении виброакустического сигнала с амплитудой колебаний меньше λ/8 необходимо учитывать расположение точечного фотодетектора, и располагать его таким образом, чтобы начальное значение разности фаз равнялось $\varphi(0) = \pm\pi/2$, т. е. расположение фотодетектора в начальный момент времени должно быть в области спекл-картины с интенсивностью равной среднему значению между максимальной и минимальной интенсивностями спекл-картины. В этом случае, восстановленный виброакустический сигнал будет соответствовать полностью исходному

виброакустическому сигналу и кроме того необходимо отметить высокую чувствительность по амплитуде колебаний исследуемой поверхности.

При измерении амплитуд колебаний больше λ/8 нет необходимости учитывать расположение точечного фотодетектора, так как количество осцилляций в любом осциллирующем пакете соответствует полной амплитуде, но не соответствует по виду амплитуде и частоте колебаний исследуемой поверхности. Следовательно, в этом случае необходимо применять дополнительные меры для точного восстановления виброакустического сигнала. Одной из мер, для успешного детектирования виброакустического сигнала с амплитудами больше λ/8 необходимо выбирать на вибрирующей поверхности точки, где амплитуда будет меньше λ/8. Данное требование, практически, всегда выполнимо, так как все вибрирующие поверхности имеют жестко закреплённые границы.

ЗАКЛЮЧЕНИЕ

В результате проведённых исследований разработана математическая модель поведения выходного сигнала с точечного быстродействующего фотодетектора спекл-интерферометра. На основе математической модели проведён теоретический анализ поведения выходного сигнала с точечного быстродействующего фотодетектора в зависимости от частоты и амплитуды вибрирующей диффузно отражающей поверхности. Показано, что выходной сигнал с точечного фотодетектора спекл-интерферометра зависит как от расположения точечного фотодетектора относительно одиночного спекла, так и от амплитуды виброакустического сигнала. При амплитуде меньше или равной λ/8 происходит точное восстановление виброакустического сигнала, если быстродействующий точечный фотодетектор располагается на спекл-картине точно посередине между максимальным и минимальным значением интенсивностей спекл-картины. При амплитуде большей λ/8 выходной сигнал с фотодетектора превращается в осциллирующие пакеты и для успешного детектирования сигнала необходимо дополнительные аппаратные и/или программные методы обработки сигнала, что требует дополнительных как теоретических, так и экспериментальных исследований.

Таким образом, теоретические и экспериментальные исследования показали, что предложенный метод когерентной оптики на основе спекл-интерферометрии на одиночном спекле позволяет детектировать виброакустический сигнал с вибрирующей диффузно отражающей поверхности.

СПИСОК ЛИТЕРАТУРЫ

1. Зайцев А.П. Технические средства и методы защиты информации / Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков; под ред. А.П. Зайцева и А.А. Шелупанова. // М.: Горячая линия–Телеком. – 2012. – 442 с.
2. Каторин Ю.Ф. Защита информации техническими средствами: Учебное пособие / Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, – 2012. – 416 с
3. Сапожков, М.А. Электроакустика: учебное пособие для вузов / М.А. Сапожков. // М.: Связь. – 1978. – 271 с.
4. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. / А.А. Хорев // В 3 т. Том 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», – 2008. – 436 с.
5. Франсон, М. Оптика спеклов / М. Франсон. – М.: Мир. — 1980. . —172 с.
6. Джоунс Р. Голографическая и спекл-интерферометрия / Р. Джоунс, К. Уайкс – М: Мир, 1986. – 327 с.
7. Mohan N.K. Recent developments in digital speckle pattern interferometry / N.K. Mohan, P. Rastogi // J. Optics and Lasers in Engineering – Vol. 40. – 2003. – pp. 439-445.
8. Zalevsky Z., Simultaneous remote extraction of multiple speech sources and heart beats from secondary speckles pattern / Y. Beiderman , I. Margalit , S. Gingold , M. Teicher , V. Mico, J. Garcia // Optics express. — 2009 — Vol. 17. – pp. 21566-21580.
9. O'Donnell L. Optimising backscatter from multiple beam interference / M. J. Padgett, S. D. Johnson // Optics express. — 2021 — Vol. 29. – pp. 8770-8776.
10. Sirkis T. Monitoring blood vital bio signs using secondary speckle patterns. / Y. Beiderman, S. Agdarov, Y. Beiderman, Z. Zalevsky // Optics express. – 2016 – Vol. 24. – pp. 27899-27909.
11. Nan Wu. Real-time audio detection and regeneration of moving sound source based on optical flow algorithm of laser speckle images / S. Haruyama // Optics express. – 2020 – Vol. 28. – pp. 4475-4488.

12. Duadi D., Non-contact optical sensing of vocal fold vibrations by secondary speckle patterns / N. Ozana, N. Shabairou, M. Wolf, Z.V. Zalevsky, A. Primov-Fever // Optics express. – 2020. – Vol. 28. – pp 20040-20050.
13. Осипов М.Н.. Развитие цифровой спекл-интерферометрии для исследования динамических процессов в реальном времени / М.Н. Осипов, В.А. Хохлов, А.Н. Чекменев // Вестник Самарского гос. ун-та. Естественнонаучная серия, Механика. – 2013. – С. 109-118.
14. Шарафутдинов Н.А. Оценка помехозащищенности спекл-интерферометрии на основе анализа изменения интенсивности одиночного спекла / Н.А. Шарафутдинов, М.Н. Осипов, Ю.Д. Щеглов, Н.С. Знаменьщикова, М.Д. Лимов // Динамика и виброакустика машин (ДВМ): Материалы третьей международной научно-технической конференции. Самара: Издательство Самарского университета. – 2016. – С. 180-182.
15. Osipov M. Determination of frequency characteristics of mechanical constructions in real time by speckle interferometry / N. Sharafutdinov, Y. Sheglov, I. Falileev, and M. Fedina // Procedia Engineering. – 2015 – Vol. 106. – pp. 224-230.
16. Борн М. Основы Оптики / М. Борн, Э. Вольф – М.: Наука. – 1973. – 719 с.

Магомедова Д.И.
МТУСИ, руководитель НОЦ ИБ Лаборатории Касперского
d.i.magomedova@mtuci.ru

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕТОДОВ И АЛГОРИТМОВ МАРКИРОВКИ НЕПОДВИЖНЫХ ИЗОБРАЖЕНИЙ И АУДИО СИГНАЛОВ С ИСПОЛЬЗОВАНИЕМ ФРАКТАЛЬНЫХ ПРОЦЕССОВ ДЛЯ ЗАЩИТЫ АВТОРСКИХ ПРАВ

Аннотация: Рассмотрены алгоритмы встраивания ЦВЗ в аудио и изображения с использованием фрактальных процессов для защиты авторских прав. Разработан алгоритм встраивания ПСП в аудио путем замены коэффициентов дискретного вейвлет-преобразования (ДВП), где каждому значению ПСП ставится в соответствие последовательность фрактального шума (ФГШ). Для встраивания ЦВЗ в изображения разработано три алгоритма с использованием двухкомпонентных контейнеров в виде сгенерированных алгебраических фракталов и фрактального гауссовского шума. Проведено исследование параметров разработанных алгоритмов для получения высокого качества встраивания и извлечения. Показано, что разработанные алгоритмы обладают повышенной эффективностью с точки зрения статистического анализа и позволяют достичь заданной достоверности извлечения при воздействии широкого ряда атак.

Ключевые слова: стеганография, защита авторских прав, цифровые водяные знаки, фрактальные процессы, дискретное вейвлет преобразование, алгебраические фракталы, фрактальный гауссовский шум.

Актуальность работы.

Повсеместное распространение мультимедийного контента делает чужую интеллектуальную собственность легкой добычей для злоумышленников. Защита авторских прав на аудио и изображения представляет собой актуальную задачу. Одной из научных областей, направленных на решение подобных задач, является стеганография [1].

Методы стеганографии позволяют встроить невидимые водяные знаки путем манипуляции характеристиками цифрового файла (текста, аудио, изображений, видео и т.д.) незаметно для органов чувств человека. Такой подход позволяет обозначить авторство без внесения заметных артефактов в цифровой объект.

Ежегодно разрабатывается большое количество новых методов встраивания ЦВЗ в медиа файлы. Несмотря на это, существует ряд нераскрытых вопросов. Процесс разработки методов стеганографии заметно отстает от развития форматов хранения и передачи мультимедийных данных. Это привело к возникновению проблемы устойчивости известных стеганографических методов [2] к разнообразным атакам, направленным на удаление встроенной метки или возникающих случайно в канале передачи данных.

Обозначенная проблема может быть решена путем использования фрактальных процессов, устойчивых к широкому спектру атак и преобразований. Однако известные методы стеганографии с использованием фрактальных процессов могут быть применены только для передачи секретных данных, поскольку не позволяют выбирать контейнер [3-9].

С учетом приведенных обстоятельств, можно сделать вывод о том, что разработка алгоритмов встраивания ЦВЗ с использованием фрактальных процессов для защиты авторских прав является актуальной задачей.

Степень разработанности темы.

Работы по созданию систем цифровых водяных знаков ведутся отечественными и зарубежными учеными, начиная с конца 1990-ых годов. Основоположниками в данной области науки можно назвать таких ученых, как M. Barni, D. Benham, I. Cox, J. Fridrich, N. Komatsu и др.

Теоретическую базу в области стеганографии и теории фракталов составили работы отечественных и зарубежных ученых Грибунин В. Г., Коржик В. И., Конахович Г. Ф., Оков И. Н., Пузыренко А. Ю., Рябко Б. Я., Туринцев И. В., Фионов А. Н., Шелухин О.И., Chaudhuri B. B., Clarke K. C., Falconer K., Gangepain J., Georgsson F., Jansson S., Mandelbrot B., Padhy L. N., Pentland A. P., Roques-Carmes G., Sarkar N., Voss R. F. и др.

Цели и задачи исследования.

Целью работы является повышение достоверности извлечения ЦВЗ при воздействии различных атак.

Для достижения цели в настоящей работе поставлены и решены следующие задачи:

1. Анализ существующих методов встраивания цифровых водяных знаков в изображения и аудио файлы.
2. Разработка алгоритмов встраивания ЦВЗ в аудио сигналы и изображения с использованием фрактальных процессов, которые обеспечивают большую достоверность извлечения ЦВЗ при воздействии атак по сравнению с известными алгоритмами.
3. Анализ влияния параметров разработанных алгоритмов на достоверность извлечения ЦВЗ. Определение значений параметров алгоритмов, позволяющих достичь достоверности извлечения в пределах заданного порога.
4. Анализ устойчивости разработанных алгоритмов к атакам.

Научная новизна работы состоит в следующем.

1. Разработан новый алгоритм встраивания водяного знака в аудио сигналы путем замены коэффициентов дискретного вейвлет преобразования с использованием фрактального гауссовского шума.
2. Разработан новый алгоритм встраивания ЦВЗ в изображения с использованием алгебраических фракталов для генерации двухкомпонентного контейнера.
3. Разработан новый алгоритм встраивания ЦВЗ в изображения путем замены коэффициентов ДВП с использованием двухкомпонентного контейнера.
4. Разработан новый алгоритм встраивания ЦВЗ в изображения путем замены коэффициентов ДВП с использованием фрактального гауссовского шума.

Теоретическая значимость работы заключается в разработке алгоритмов встраивания ЦВЗ с использованием фрактальной геометрии для изображений и аудио, которые могут использоваться в целях защиты авторских прав.

Практическая значимость работы состоит в следующем:

1. Предложен новый алгоритм встраивания в аудио сигналы с использованием ФГШ, увеличивающий устойчивость к воздействию гауссовского шума.
2. Предложен новый алгоритм встраивания с использованием двухкомпонентного контейнера, обеспечивающий устойчивость метода НЗБ к визуальной атаке.
3. Предложен новый алгоритм встраивания ЦВЗ с использованием двухкомпонентного контейнера и дискретного вейвлет преобразования, повышающий эффективность встраивания с точки зрения статистического анализа и обеспечивающий достоверное извлечение при воздействии атак.
4. Предложен новый алгоритм встраивания ПСП в изображения с использованием фрактального гауссовского шума и дискретного вейвлет преобразования, обеспечивающий повышенную достоверность извлечения при воздействии атак по сравнению с известными методами.

Положения, выносимые на защиту:

1. Алгоритм встраивания ПСП в аудио сигналы с использованием ФГШ (Аа), который позволяет получить достоверность извлечения ЦВЗ >95% при воздействии гауссовского шума при SNR≥35.
2. Алгоритм встраивания ЦВЗ с использованием двухкомпонентного контейнера и дискретного вейвлет преобразования (А2) позволяющий получить выигрыш до одного порядка при вычислении расстояния Бхаттачарьи и примерно в 2 раза при вычислении дивергенции Кульбака-Лейбнера по сравнению с эталоннным алгоритмом (Э2), при этом пропускная способность разработанного алгоритма на 2 порядка выше, чем у эталона.
3. Алгоритм встраивания ПСП на основе фрактального гауссовского шума и дискретного вейвлет преобразования (А3) позволяющий получить статистические показатели того же порядка, что и у эталонного алгоритма (Э2) при повышении пропускной способности на 3 порядка, а также получить вероятность ошибки извлечения при воздействии широкого ряда атак $<10^{-5}$, что на 3 порядка ниже, чем у эталона (Э2), при воздействии усредняющего фильтра и на 1 порядок выше при воздействии сжатия JPEG..

Степень достоверности и апробация результатов.

Достоверность результатов диссертационной работы подтверждается результатами имитационного моделирования и их совпадением с результатами экспериментальных данных. Полученные результаты опубликованы и обсуждались со специалистами на научных конференциях.

Основные результаты работы обсуждались и получили одобрение на 10 научных конференциях:

1. Международный форум информатизации (МФИ-2017), Москва, 2017;
2. XII международная отраслевая научно-техническая конференция "Технологии информационного общества", Москва, 14-15 марта 2018 г.;

3. Международная научно-техническая конференция «Телекоммуникационные и вычислительные системы – 2018», Москва, 2018;
4. Международная научно-техническая конференция «Фундаментальные проблемы радиоэлектронного приборостроения «INTERMATIC-2018», Москва, 19 – 23 ноября 2018;
5. Девятая всероссийская научно-техническая конференция Безопасные информационные технологии, 4 – 5 декабря 2018;
6. 24-ая международная конференция Ассоциации открытых инноваций FRUCT, Москва, 8-12 апреля 2018;
7. Международная научно-техническая конференция «Телекоммуникационные и вычислительные системы – 2019», Москва, 2019;
8. Международная конференция «Системы синхронизации, формирования и обработки сигналов в инфокоммуникациях» СИНХРОИНФО 2020, Калининград, 01-03 июля 2020;
9. Международная конференция “2021 Системы генерации и обработки сигналов в области бортовых коммуникаций”, Москва, 16-18 марта 2021;
10. Международная конференция «Системы синхронизации, формирования и обработки сигналов в инфокоммуникациях» СИНХРОИНФО 2021, Калининград, 30 июня-02 июля 2021.

Постановка задачи.

Проведенный анализ существующих алгоритмов встраивания показывает, что выявление слабых мест известных алгоритмов, связанных с разрушением ЦВЗ под воздействием атак, требует разработки методов встраивания ЦВЗ с использованием фрактальных процессов, обеспечивающих заданную достоверность извлечения.

Алгоритм встраивания ПСП в аудио сигналы с использованием фрактального гауссовского шума (Аа).

В предложенном автором алгоритме (Аа) [10] встраивание производится путем замены коэффициентов дискретного вейвлет преобразования (ДВП) последовательностями фрактального гауссовского шума.

В качестве водяного знака используется ключевая последовательность в виде двоичной псевдослучайной последовательности $ПСП(p) \in \{0,1\},\ p = \overline{1,P}$, однозначно определяющая пользователя.

Каждому биту ПСП в соответствие ставится непрерывнозначная последовательность $\{X_{ФГШ}(t_l);\ l = \overline{1,L}\} = \{X_{ФГШ,l};\ l = \overline{1,L}\}$, где $L = N / P$ в виде фрактального гауссовского шума (ФГШ) с заданной фрактальной размерностью, характеризуемой показателем Херста H [10]. Сформированные фрактальные последовательности используются при маркировании аудиосигнала.

Алгоритм встраивания *p*-го бита ПСП в аудио сигнал описывается соотношением :

$$y_p^*(t) = f\{S_{a,n}, \alpha, ПСП(p), X_{ФГШ,l}\}, \quad (1)$$

где α – масштабирующий коэффициент.

Для встраивания ПСП будем использовать декомпозицию аудио сигнала в виде дискретного вейвлет разложения. Встраивание производится путем замены детализирующих коэффициентов вейвлет разложения на сформированный ФГШ.

Для встраивания «0» используется ФГШ с фрактальной размерностью, характеризуемой показателем Херста H_0, а для встраивания «1» - ФГШ с показателем Херста H_1. Длина фрактальной последовательности *L* определяется длиной сегмента аудио сигнала и уровнем вейвлет разложения, в коэффициенты которого встраивается ПСП.

На заключительном этапе встраивания происходит вейвлет реконструкция аудиосигнала с измененными коэффициентами детализации.

Для извлечения встроенной метки принятый аудио сигнал делится на сегменты. К каждому сегменту применяется процедура разложения на вейвлет коэффициенты. Выделяется та часть детализирующих коэффициентов первого уровня и производится оценка индекса Херста H, по которой пороговое устройство фиксирует «0» или «1» в рассматриваемом сегменте аудио.

Извлечение элемента ПСП осуществляется с использованием найденной оценки в соответствии с формулой

$$ПСП(p)^* = \begin{cases} 1 & при\ H_i \geq H_{пор} \\ 0 & при\ H_i < H_{пор} \end{cases}. \quad (2)$$

Если найденная оценка показателя Херста в анализируемом сегменте ПСП выше заданного порога $H_{пор}$, то принимается решение о встраивании «1», в противном случае – «0».

Для определения оптимальных параметров стеганографической системы, позволяющей достичь баланса между качеством встраивания и извлечения, были произведены эксперименты с использованием набора аудио сигналов двух типов – речь и музыка - с различной частотой дискретизации (8000 Гц, 22050 Гц, 44100 Гц).

Достоверность извлечения определялась, как процент извлеченных ПСП, взаимный коэффициент корреляции которых с опорной ПСП, был выше порогового значения 0.95.

Было учстановлено что для достижения заданной достоверности извлечения, необходимо использовать коэффициенты вейвлет разложения 1-5 уровня для аудио типа речь и 1-3 уровня для аудио типа музыка. Значение масштабирующего коэффициента должно быть $\alpha \leq 10^{-2}$ для сохранения качества аудио сигнала. Для аудио типа речь значение масштабирующего коэффициента не влияет на достоверность извлечения. Для аудио типа музыка достоверное извлечение достигается в следующих случаях: для вейвлетов Хаара при $\alpha \geq 10^{-6}$, а для вейвлетов Добеши 4, Симлет 4 и Койфлет 4 при $\alpha \geq 10^{-4}$. При выборе порогового значения необходимо учитывать, что достоверность извлечения для всех рассматриваемых случаев была достигнута при $H_{пор} \in [0.25;0.9]$. Длина используемой ФГШ последовательности шума и значение показателя Хёрста не оказывают существенного влияния на качество встраивание и достоверность извлечения.

Устамновлено, что при использовании разработанного алгоритма можно достичь извлечения с заданной достоверностью для аудио типа речь при воздействии гауссовского шума при SNR≥35 при использовании вейвлетов Хаара, Симлет 4 и Койфлет 4 и при SNR≥40 при использовании вейвлетов Добеши 4. Для аудио типа музыка требуемая достоверность извлечения достигается при SNR≥50.

Алгоритм встраивания ЦВЗ с использованием алгебраических фракталов для формирования двухкомпонентного контейнера (A1)

Предлагаемый алгоритм использует алгебраические фракталы для скрытия ЦВЗ перед встраиванием непосредственно в контейнер. Секретная информация вводится в момент создания фрактального изображения с использованием исходных параметров и нелинейной модели [11, 12]. Внедрение секретной информации производится одновременно с генерацией фрактальных изображений, сами секретные данные используются как параметры, необходимые для генерации фрактальных изображений.

Алгоритм встраивания A1 состоит из следующих шагов:

Шаг 1. Перевод двоичной матрицы ЦВЗ $Q(Q_w,Q_h)$ размером Q_w*Q_h в вектор $Q(Q_l)$ размером $Q_l = Q_w*Q_h$;

Шаг 2. Генерация фрактального контейнера $F(F_w, F_h)$ с использованием двоичной последовательности ЦВЗ;

Шаг 3. Встраивание фрактального контейнера $F(F_w, F_h)$ в контейнер $S(S_w,S_h)$ путем замены наименее значащих бит синей компоненты $B(S_w,S_h)$ контейнера битами фрактального контейнера;

Шаг 4. Восстановление стегоконтейнера $S^*(S_w,S_h)$ с использованием измененной синей цветовой компоненты $B^*(S_w,S_h)$.

Использовалось 6 типов фракталов с различным расположением начальной точки относительно множество Мандельброта. Используемые фракталы показаны на рисунке 1, их характеристики представлены в таблице 1.

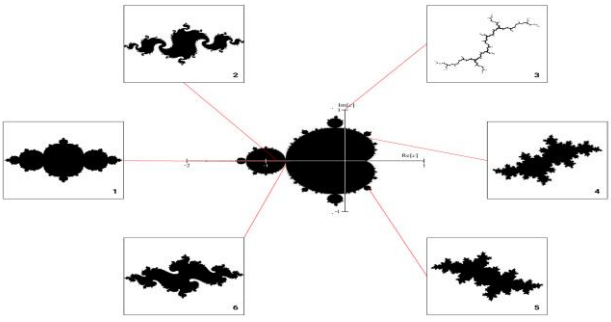


Рис.1. Типы исследуемых фракталов.

Таблица 1. Параметры p и q сгенерированных фракталов

№	Тип фрактала	p	q
1	Множество Жюлиа с одним аттрактором	-0.7	0
2	Множество Жюлиа с аттрактором периода 2	- 0.83	0.16
3	Дендрит	0	1
4	Диск Зигеля	-0.39054	0.58678
5	Множество Жюлиа с аттрактором периода 5 (параболический бассейн)	-0.481762	-0.531657
6	Множество Жюлиа из долины морских коньков	-0.7454	0.113

Установлено, что наибольший объем встраивания можно достичь при использовании множества Жюлиа с одним аттрактором, наименьший – при использовании дендрита. Диск Зигеля, множество Жюлиа с аттрактором периода 5 и множество Жюлиа из долины морских коньков позволяют встроить ЦВЗ имеют приблизительно равную высокую емкость, в то время как множество Жюлиа с аттрактором периода 2 имеет меньшую емкость среди наполненных множеств.

Установлено, что что для сохранения низкого уровня ошибок при любом объеме заполнения фрактального контейнера рекомендуется использовать множество Жюлиа из долины морских коньков. В случае необходимости заполнения большого объема фрактального контейнера (Pr>0.6), рекомендуется использовать множество Жюлиа с одним аттрактором.

Исследование алгоритма показало, что использование двухкомпонентного фрактала делает метод НЗБ устойчивым к визуальной атаке, сохраняя низкую вычислительную сложность и высокую пропускную способность оригинального метода НЗБ. Однако предлагаемый алгоритм позволяет достичь заданной достоверности извлечения только при воздействии гауссовского и импульсного шума.

Алгоритм встраивания ЦВЗ с использованием двухкомпонентного контейнера и дискретного вейвлет преобразования (А2)

Для преодоления недостатков, связанных с устойчивостью алгоритма А1, к некоторым видам атак, был разработан алгоритм, в котором на втором этапе встраивания производится замена коэффициентов дискретного вейвлет-преобразования значениями фрактального контейнера. Алгоритм встраивания и извлечения представлен на рисунке 2.

При анализе параметров алгоритма А2 было показано, что:

- наилучший баланс между качеством контейнера и качеством извлечения достигается при замене диагональных коэффициентов второго уровня разложения;
- параметр alpha должен находиться в пределах [5;20] при использовании вейвлета Хаара и [2.5;20] при использовании вейвлетов Добеши 4, Симлет 4 и Койфлет 4.
- нулевая вероятность ошибки достигается при соотношении порога к alpha Thr/alpha∈[0.4,0.6] для вейвлета Хаара и Thr/alpha∈[0.25,0.8] для Добеши 4, Симлет 4 и Койфлет 4.
- наибольшие искажения при встраивании и при извлечении достигаются при использовании вейвлета Хаара.

Установлдено, что разработанный алгоритм А2 позволяет достичь заданной достоверности при воздействии шума трех типов (гауссовский, импульсный, мультипликативный), усредняющего фильтра с размером маски 3x3 и сжатия JPEG со степенью сжатия $\leq 50\%$.

Недостатком разработанного алгоритма является его низкая пропускная способность.

Алгоритм встраивания ПСП на основе фрактального гауссовского шума и дискретного вейвлет преобразования (А3)

Разработанный алгоритм идентичен алгоритму **Аа** для аудиосигналов .

Использование данного алгоритма помогает преодолеть недостатки, связанные с низкой пропускной способностью алгоритмов А1 и А2, при этом сохранив высокий уровень достоверности извлечения ЦВЗ при воздействии атак.

При анализе параметров алголритма было показано, что:

- наилучший баланс между качеством контейнера и качеством извлечения достигается при замене диагональных коэффициентов второго уровня разложения;
- рекомендуется использовать alpha∈[2.5;12.5];

- значения длины ФГШ, показателя Херста и порога не оказывают значительного влияния на вероятность ошибки извлечения;

- наибольшие ошибки извлечения возникают при использовании вейвлета Койфлет 4, наименьшие – при использовании вейвлета Хаара.

Анализ устойчивости в условиях воздействия атак показал, что алгоритм обеспечивает заданную достоверность извлечения при воздействии шума трех типов, усредняющего фильтра с размером маски 3x3 и сжатия JPEG при степени сжатия ≤ 50%.

Сравнительный анализ разработанных алгоритмов.

Для сравнения эффективности встраивания ЦВЗ разработанными фрактальными методами было произведено вычисление статистических показателей

Помимо трех разработанных алгоритмов: алгоритм встраивания ЦВЗ с использованием алгебраических фракталов для формирования двухкомпонентного контейнера (А1), алгоритм встраивания ЦВЗ с использованием двухкомпонентного контейнера и дискретного вейвлет преобразования (А2) и алгоритм встраивания ПСП на основе фрактального гауссовского шума и дискретного вейвлет преобразования (А3) - производилось сравнение с двумя эталонными методами: методом НЗБ (Э1) и алгоритма Кима [1] (Э2).

В таблице 2 представлены результаты вычисления корреляции, расстояния Бхаттачарьи, дивергенции Кульбака-Лейбнера и пропускной способности.

Таблица 2. Результаты вычисления статистических показателей

	Корреляция	Расстояние Бхаттачарьи	Дивергенция Кульбака-Лейбнера	Пропускная способность, %
А1	0.9987	0.028	300873,8	23,87
А2	0.994	0.008	44,567	1,58
А3	0.994	0.09	673,826	10
Э1	0.999	0.02	573,635	100
Э2	0.994	0.018	71,0744	0,016

Полученные результаты говорят о том, что алгоритм (А1) обладает наибольшей пропускной способностью по сравнению алгоритмами А2 и А3, но уступает им по величине искажений оригинального контейнера . Алгоритм (А2) имеет выигрыш до одного порядка при вычислении расстояния Бхаттачарьи и примерно в 2 раза при вычислении дивергенции Кульбака-Лейбнера по сравнению с алгоритмом Э2, при этом пропускная способность алгоритма на 2 порядка выше, чем у эталона. Алгоритм (А3) позволяет получить статистические показатели того же порядка, что и Э2, при этом его пропускная способность выше на 3 порядка.

Для сравнения достоверности извлечения ЦВЗ в условиях воздействия атак производилось тестирование разработанных алгоритмов с использованием 10000 изображений из двух баз изображений, используемых для оценки стегосистем [13, 14].

В таблице 3 представлены результаты проведенных экспериментов.

Таблица 3. Вероятность ошибки извлечения ЦВЗ при воздействии атак.

Алгоритм	Вейвлет	Фрактал	Вероятность ошибочного извлечения				
			Гауссовский шум v=0.5	Соль и перец v=0.5	Мультипликативный шум v=0.5	Фильтрация h=2	JPEG 30%
Э1			0,025	0,02522	0,558796	0,5655	0,499
А1		1	0, 02472	0,02491	0,386772	0,5650	0,499
А1		3	0,025	0,02508	0,392244	0,5631	0,500
А1		4	0,025	0,02542	0,365936	0,5598	0,501

A1		5	0,024	0,02518	0,426516	0,5625	0,499
A1		6	0,024	0,02499	0,367328	0,5632	0,497
A2	Хаар	1	7,8895e-05	0,00331	0,01988	0,0342	0,006
A2	Хаар	3	0,000105	0,00344	0,02153	0,0301	0,004
A2	Хаар	4	2,6298e-05	0,00389	0,024720	0,0357	0,005
A2	Хаар	5	2,6298e-05	0,00407	0,024930	0,0294	0,005
A2	Хаар	6	7,8895e-05	0,00420	0,023879	0,0309	0,005
A2	Добеши 4	1	$<10^{-5}$	0,01036	0,003681	0,0123	0,114
A2	Добеши 4	3	$<10^{-5}$	0,01070	0,004549	0,0088	0,103
A2	Добеши 4	4	$<10^{-5}$	0,00925	0,007153	0,0114	0,117
A2	Добеши 4	5	$<10^{-5}$	0,01136	0,006916	0,0132	0,104
A2	Добеши 4	6	$<10^{-5}$	0,00796	0,006548	0,0110	0,119
A2	Симлет 4	1	$<10^{-5}$	0,00578	0,003208	0,0112	0,084
A2	Симлет 4	3	$<10^{-5}$	0,00662	0,003839	0,0087	0,087
A2	Симлет 4	4	$<10^{-5}$	0,00581	0,005207	0,0110	0,08
A2	Симлет 4	5	$<10^{-5}$	0,00691	0,005207	0,0111	0,087
A2	Симлет 4	6	$<10^{-5}$	0,00552	0,005443	0,0097	0,081
A2	Койфлет 4	1	$<10^{-5}$	0,00749	0,003024	0,0410	0,019
A2	Койфлет 4	3	$<10^{-5}$	0,00796	0,004996	0,0397	0,021
A2	Койфлет 4	4	2,6298e-05	0,00767	0,005706	0,0418	0,021
A2	Койфлет 4	5	$<10^{-5}$	0,00807	0,004996	0,0449	0,019
A2	Койфлет 4	6	$<10^{-5}$	0,00857	0,005259	0,0421	0,019
A3	Хаар		$<10^{-5}$	$<10^{-5}$	$<10^{-5}$	$<10^{-5}$	0,006
A3	Добеши 4		0,004	0,004	0,004	0,006	0,1
A3	Симлет 4		0,004	0,004	0,004	0,004	0,002
A3	Койфлет 4		0,012	0,012	0,012	0,008	0,049
Э2	Хаар		$<10^{-5}$	0,001	$<10^{-5}$	0,069	0,065
Э2	Добеши 4		0,0006	0,001	0,0009	0,067	0,073

Э2	Симлет 4		0,0054	0,006	0,0054	0,075	0,064
Э2	Койфлет 4		0,0075	0,008	0,0071	0,077	0,069

Из таблицы видно, что наименьшие значения вероятности ошибки имеют место при использовании алгоритма А3 в комбинации с вейвлет разложением Хаара. Полученные значения на 3 порядка ниже, чем у эталона Э2, при воздействии усредняющего фильтра и на 1 порядок выше при воздействии сжатия JPEG..

Выводы.

Использование фрактальных процессов при разработке алгоритмов встраивания ЦВЗ в мультимедийный контент показали высокую эффективность. Разработанные алгоритмы позволяют улучшить качество стегоконтейнера с точки зрения статистического анализа до 10 раз.

Разработанные алгоритмы обеспечивают высокую достоверность извлечения ЦВЗ при воздействии широкого ряда атак.

СПИСОК ЛИТЕРАТУРЫ

1. Шелухин О.И. Стеганография. Алгоритмы и программная реализация / Шелухин О.И., Канаев С.Д. – Горячая линия Телеком – М, 2018 – 592 с.
2. Bender W. Techniques for Data Hiding / Bender W., Gruhl D., Morimoto N., Lu A. // IBM Systems Journal – 1996 - № 35 - pp. 313-336.
3. Ali A.H. High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain / Ali A.H., George L.E., Zaidan A.A., Mokhtar M.R. // Multimed Tools Appl - 77, 2018 – pp. 31487–31516.
4. Sangavi V. An Image Encryption Algorithm Based On Fractal Geometry / Sangavi V., Thangavel P. // Procedia Computer Science, 2019 – pp. 462–469.
5. Zhang H. A Steganography Scheme Based on Fractal Images / Zhang H., Hu J., Wang G. // 2011 Second International Conference on Networking and Distributed Computing, 2011 – pp.28-31
6. Zhang X. A Coverless Image Information Hiding Algorithm Based on Fractal Theory / Zhang X., Peng F., Lin Z. // International Journal of Bifurcation and Chaos, 2020 – pp.1-20
7. Alia M. Improved Steganography Scheme based on Fractal Set / Alia M., Suwais K. // The International Arab Journal of Information Technology, 2020 – pp. 128-136
8. Durafe A. Development and analysis of IWT-SVD and DWT-SVD steganography using fractal cover / Durafe A., Patidar V. // Journal of King Saud University Computer and Information Sciences, 2020 – pp. 1-16
9. Masood F. A Novel Hybrid Secure Image Encryption Based on Julia Set of Fractals and 3D Lorenz Chaotic Map / Masood F., Ahmad J., Shah S.A. , Jamal S.S., Hussain I. // Entropy, 2020 – pp 1-28.
10. Sheluhin O.I. Marking audio signals using fractal gaussian noise / O. I. Sheluhin, D. I. Magomedova, S. Y. Rybakov, A. G. Simonyan // 2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2021 - Conference Proceedings, Svetlogorsk, Kaliningrad Region, 30 июня – 02 2021 года. – Svetlogorsk, Kaliningrad Region, 2021.- pp 1-7
11. Магомедова Д.И., Шелухин О.И. Фрактальные модели и алгоритмы создания защитной маркировки для обеспечения целостности и аутентичности растровых изображений. Системы синхронизации, формирования и обработки сигналов. 2020. Т. 11. № 1. С. 57-67.
12. Шелухин О.И., Магомедова Д.И. Использование алгебраических фракталов в качестве секретных ключей при внедрении водяных знаков в изображения стеганографическими методами Фундаментальные проблемы радиоэлектронного приборостроения. 2018. Т. 18. № 4. С. 1066-1070.
13. Bas P., Filler T. & Pevn´y T. (2011) “Break our steganographic system” the ins and outs of organizing BOSS. LNCS. 6958, 59–70. Available from: doi:10.1007/978-3-642-24178-9_5.
14. PPG-LIRMM-COLOR database. Available at: http://www.lirmm.fr/~chaumont/PPG-LIRMM-COLOR.html

Павлов А.С.
Северо-Кавказский федеральный университет, инженер-лаборант,
losde5530@gmail.com

МЕТОДЫ И АЛГОРИТМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕССА МАСШТАБИРОВАНИЯ ЧИСЛЕННОСТИ АГЕНТОВ В РОЕВЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМАХ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ

Аннотация: Одним из важнейших аспектов развития групповой робототехники, в том числе роевых робототехнических систем (РРТС), является обеспечение корректного взаимодействия между агентами. Перспективность применения РРТС обусловлена такими свойствами, как гибкость, отказоустойчивость и масштабируемость системы. При этом интенсивное развитие и распространение РРТС провоцирует увеличение количества инцидентов информационной безопасности. Существующие механизмы обеспечения информационной безопасности не в полной мере позволяют противодействовать угрозам информационной безопасности при взаимодействии агентов РРТС. Отдельно выделяется такой класс угроз как внедрение «вредоносных» агентов в РРТС, в результате чего нарушитель осуществляет скрытое информационное воздействие на других агентов системы, что, в свою очередь, приводит к снижению эффективности выполнения поставленной задачи агентами РРТС. Реализация данной угрозы не имеет ярко выраженных признаков, что не позволяет использовать стандартные инструменты информационной безопасности для своевременного обнаружения и противодействия им. Таким образом, настоящее исследование направлено на решение задачи повышения уровня информационной безопасности процесса масштабирования численности агентов в РРТС. В отличие от ранее проводимых исследований, в настоящей работе основной акцент сделан на взаимодействии агентов РРТС при масштабировании их численности. В рамках решения поставленной задачи предложена новая научная идея разработки протоколов и методов аутентификации агентов РРТС и обнаружения несанкционированного доступа к управлению отдельными агентами РРТС, а также методов и средств их программной реализации.

Ключевые слова: роевая робототехническая система, масштабирование системы, информационная безопасность, аутентификация и авторизация, машинное обучение, искусственные нейронные сети.

Актуальность темы исследования. Переход к передовым цифровым, интеллектуальным производственным технологиям актуализирует направление развития РРТС, как вида групповой робототехники, которая тесно связана с интенсивным ростом научно-технологического потенциала страны [1]. Использование автономного интеллектуального оборудования и робототехнических комплексов относится к одному из приоритетных направлений развития и использования технологий искусственного интеллекта [2]. Решение вопросов обеспечения требуемой информационной безопасности групповых робототехнических систем также является актуальным направлением рынка Сейфнет Национальной технологической инициативы в части обеспечения информационной безопасности киберфизических и информационных систем [3].

В настоящее время в российских и зарубежных публикациях известны не только академические результаты исследований в области групповой робототехники [4-9], но и примеры реального применения систем подобного типа [10]. Сотрудники компании Ziyan разработали концепцию управления группой из десяти малоразмерных бомбардировщиков на базе беспилотных летательных аппаратов вертолетного типа [11]. Примером гражданского применения групповой робототехники является проект Intel Shooting Star [12], который посвящен созданию световых шоу в развлекательных и рекламных целях за счет использования в ночное время группы из пятиста беспилотных летательных аппаратов. Другим примером успешного гражданского применения групп роботов является индустрия логистики, где многочисленные группы складских роботов выполняют сложные логистические задачи по транспортировке грузов. Яркими примерами таких компаний являются AmazonRobotics [13], Alibaba [14] и др.

Одним из ключевых преимуществ использования РРТС [15] является возможность масштабирования количества агентов при увеличении сложности задания (например, увеличение площади территории, на которой необходимо осуществить мониторинг или разведку для сбора данных) [16]. Дополнительно привлеченные агенты могут быть направлены как из управляющего центра, так и переназначены оператором в ходе выполнения собственного задания с меньшим

приоритетом важности. При этом актуальным вопросом обеспечения информационной безопасности РРТС становится аутентификация и авторизация новых агентов РРТС.

Концептуально групповая робототехника может быть определена как глобальная динамическая сетевая инфраструктура, где агенты интегрируются в информационную сеть с использованием различных интерфейсов [17]. При этом с технической точки зрения могут быть использованы любые технологии взаимодействия агентов, а также способы обработки и передачи данных, исходя из их целевого предназначения. РРТС является частным случаем групповой робототехники, которая имеет следующие особенности:

- идентичное структурно-функциональное устройство агентов, включающее бортовые датчики и сенсоры с ограниченной дальностью действия и низко-производительные вычислительные устройства, независимо от конкретной аппаратной реализации;
- полная децентрализация взаимодействия агентов на основе самоорганизации, из чего следует отсутствие центрального узла (агента-координатора);
- отсутствие полной информации обо всех агентах РРТС ввиду вышеперечисленных ограничений, из чего следует отсутствие идентификаторов у агентов (при этом максимальная численность агентов не лимитирована).

Степень разработанности темы исследования. Исследование и совершенствование методов обеспечения информационной безопасности в групповой робототехнике и РРТС в частности осуществляется в таких отечественных и зарубежных научно-исследовательских и образовательных учреждениях, как Южный федеральный университет, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Казанский федеральный университет, Национальный исследовательский университет ИТМО, Institut de Recherches Interdisciplinaires et de Développements en Intelligence Artificielle (Бельгия), University of London (Великобритания), Delft University of Technology (Нидерланды) и др. Наибольший вклад в исследования по данной тематике внесли ведущие научные коллективы под руководством таких известных ученых, как Каляев И.А., Магид Е.А., Пшихопов В.Х., Кривенко М.П., Зикратов И.А., Коваль Е.Н., Викснин И.И. Басан А.С., Мариненков Е.Д., Dorigo M., Sargeant I., Higgins F., Strobel V., Alonso-Mora J. и др. Известные подходы для обеспечения информационной безопасности в групповой робототехнике и РРТС в частности можно разделить на следующие категории в зависимости от идеи, лежащей в их основе:

– методы доверия и репутации [18];
– технологии анализа поведения и анализа трафика [19];
– специализированные протоколы и модели взаимодействия роботов [20].

Задача обеспечения информационной безопасности на основе методов доверия и репутации рассматривается в работе [18]. Суть данного решения состоит в использовании механизма установления доверительных отношений на основе репутации отдельных агентов [21]. Недостатком такого подхода является тот факт, что выход из строя отдельного агента может привести к возникновению сбоев в системах такого рода.

В работе [22] для обеспечения информационной безопасности группы роботов предложен метод на основе анализа поведения отдельных роботов [15]. Суть предложенного метода заключается в непрерывном поиске отклонений в поведении (действиях) роботов от штатного поведения. Данная процедура выполняется в центре управления на основе анализа трафика, получаемого от каждого робота, что обеспечивает точное своевременное выявление вредоносных роботов. Однако в РРТС концептуально отсутствует центральный канал связи, что существенно ограничивает применимость данного метода.

В работе [23] предложен метод на основе модели полицейских участков в группе роботов. Суть метода заключается в декомпозиции рабочей области роботов на несколько подобластей, в каждой из которых назначается робот, обеспечивающий управление информационной безопасностью. Недостатком такого подхода является риск выхода из строя отдельного робота, что накладывает необходимость применения дополнительных средств для мониторинга состояния и работоспособности роботов. С другой стороны, агентами РРТС, как правило, являются роботы, идентичные по структурному и функциональному исполнению, а бортовые датчики, сенсоры, средства связи и вычислительные устройства имеют невысокую производительность. Этот факт затрудняет выполнение ресурсоемких алгоритмов обеспечения информационной безопасности на борту отдельно взятого робота.

Проблема повышения уровня информационной безопасности в процессе функционирования РРТС является весьма острой и до сих пор не нашла своего окончательного решения в большинстве прикладных задач. Очевидно, что решение данной проблемы возможно только на основе комплексного

подхода, который будет использовать все многообразие методов и средств обеспечения информационной безопасности в процессе функционирования РРТС. При этом должны быть учтены как специфика децентрализованного управления агентами РРТС, так и ограниченные возможности (сенсорные и вычислительные) робототехнических устройств, входящих в состав РРТС.

Цели и задачи работы. Объектом исследования является роевая робототехническая система, предметом – методы и алгоритмы обеспечения информационной безопасности процесса масштабирования численности агентов в РРТС.

Цель исследования состоит в повышении эффективности обеспечения информационной безопасности процесса масштабирования численности агентов в РРТС.

Научная задача исследования заключается в разработке методов и алгоритмов для обеспечения информационной безопасности процесса масштабирования численности агентов в РРТС на основе применения методов машинного обучения с учетом специфики децентрализованного управления и особенностей систем данного типа.

Для достижения цели исследования необходимо решить следующие частные научные задачи:

1. Разработать модель угроз безопасности информации при взаимодействии агентов РРТС в процессе масштабирования их численности с учетом специфических особенностей РРТС.
2. Разработать протокол делегированной аутентификации новых агентов при масштабировании численности агентов в РРТС на основе распределенного реестра и методов машинного обучения.
3. Разработать метод делегированной авторизации агентов на основе модели безопасности с нулевым доверием с использованием искусственных нейронных сетей.
4. Разработать интеллектуальную децентрализованную подсистему аутентификации и авторизации агентов при масштабировании численности РРТС.
5. Выполнить экспериментальные исследования и оценить эффективность моделей, методов и решений обеспечения информационной безопасности в РРТС.

Исследование соответствует паспорту научной специальности 05.13.19 (2.3.6) – «Методы и системы защиты информации, информационная безопасность» по 3 пунктам:

– п. 3 «Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.» (научная задача №1 настоящего исследования);

– п. 11 «Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.» (научные задачи №2 и 3 настоящего исследования);

– п. 13 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» (научная задача №4 настоящего исследования).

Научная новизна. Научная новизна исследования заключается в следующем:

1. Разработанные обобщенные модели функционирования РРТС и модели угроз и нарушителя информационной безопасности при взаимодействии агентов РРТС отличаются от существующих моделей учетом специфических особенностей РРТС, таких как децентрализованная система управления и ограничения сенсорных и вычислительных возможностей робототехнических устройств, используемых в составе РРТС (например, малый объем оперативной памяти, низкая тактовая частота процессора, малая емкость аккумуляторной батареи, низкая производительность бортовых датчиков и сенсоров и т.д.), что позволяет повысить вероятность достижения цели агентами РРТС.
2. Разработанный протокол делегированной аутентификации новых агентов при масштабировании численности агентов в РРТС учитывает свойство масштабируемости системы и позволяет избежать «лавинного эффекта» при аутентификации агентов в результате значительного увеличения их численности, что позволяет сократить время, необходимое для выполнения поставленной задачи.

Теоретическая и практическая значимость работы. Теоретическая и практическая значимость работы заключается в том, что разработанные протоколы, методы и алгоритмы учитывают специфические особенности РРТС, что позволит повысить уровень информационной безопасности при функционировании РРТС. Экономическая значимость работы заключается в уменьшении времени, необходимого для выполнения целевой задачи, при наличии нарушителей в РРТС.

Методология и методы исследования. Методологической основой исследования являются методы теории информационной безопасности, теории систем и системного анализа, аналитической геометрии, оптимизации, машинного обучения.

Положения, выносимые на защиту. На защиту выносятся следующие положения:

1. Модель угроз безопасности информации при взаимодействии агентов РРТС в процессе масштабирования их численности с учетом специфических особенностей РРТС.

2. Протокол делегированной аутентификации новых агентов при масштабировании численности агентов в РРТС на основе распределенного реестра и методов машинного обучения.

3. Метод делегированной авторизации агентов на основе модели безопасности с нулевым доверием с использованием искусственных нейронных сетей.

4. Интеллектуальная децентрализованная подсистема аутентификации и авторизации агентов при масштабировании численности РРТС.

Степень достоверности и апробация результатов. Достоверность и обоснованность результатов исследования подтверждается проведенными вычислительными экспериментами, корректным использованием положений теории информационной безопасности и теории системного анализа, а также рецензированием печатных работ. Основные результаты работы докладывались, обсуждались и получили положительную оценку на 9 международных и межрегиональной научно-практических конференциях: VI Всероссийская научная конференция с международным участием «Информационные технологии интеллектуальной поддержки принятия решений» (ITIDS'2018) (г. Уфа, 2018); IV-VIII Всероссийские научно-технические конференции «Студенческая наука для развития информационного общества» (г. Ставрополь, 2017-2019). Положения диссертационного исследования поддержаны конкурсом региональной научно-практической конференции «Инновационные идеи молодежи Ставропольского края – развитию экономики России» (программа УМНИК-2018) по теме: «Разработка реконфигурируемого робототехнического комплекса с адаптивной кинематической структурой на базе малоразмерных сферических роботов для применения в условиях ЧС».

Основные результаты работы отражены в х научных трудах, в том числе: 4 статьях, размещенных в рецензируемых научных журналах, рекомендованных ВАК при Минобрнауки России; 8 статьях в изданиях, входящих в международную базу данных Scopus; 12 свидетельствах о государственной регистрации программ для ЭВМ.

Краткое содержание исследования с упором на результаты, полученные за период реализации научного проекта в рамках гранта. Первая частная научная задача связана с разработкой модели угроз безопасности информации при взаимодействии агентов РРТС в процессе масштабирования их численности с учетом специфических особенностей РРТС. В рамках решения задачи получены следующие результаты [24]:

1. Выполнено обобщение известных результатов в области проектирования и разработки РРТС, на основе полученных результатов формализована обобщенная модель функционирования РРТС. Также в результате анализа приложений РРТС выделен класс пространственно-распределенных задач, характеризующийся рассредоточенностью агентов в пространстве таким образом, что возможности бортовых телекоммуникационных устройств не обеспечивают стабильного информационного обмена между агентами в процессе выполнения задач. Помимо этого, данный класс задач подразумевает возможность повышения сложности их выполнения (например, увеличение рабочей области), что требует привлечения новых агентов для максимизации эффективности выполнения этих задач.

2. Сформированы обобщенные модели угроз и нарушителя информационной безопасности РРТС в процессе масштабирования численности агентов при выполнении пространственно-распределенных задач с учетом особенностей систем этого типа. Полученные результаты носят декларативно-описательный характер, так как построены на основе концептуального описания РРТС как архитектуры робототехнической системы без учета конкретных характеристик устройств, входящих в состав системы. Данные результаты могут быть полезны специалистам в области проектирования и разработки РРТС.

3. Проведен анализ исследований, направленных на обеспечение информационной безопасности в группах робототехнических устройств с точки зрения возможности их применения в РРТС. Указаны исследования, которые в перспективе могут быть использованы для комплексной защиты информации в РРТС.

4. Проведена количественная оценка воздействия внедренных вредоносных агентов на результат функционирования РРТС при реализации атаки. В рамках эксперимента предполагается, что каждый внедренный вредоносный агент в процессе распределения задач выбирает самую удаленную от него задачу, однако, не выполняет ее. В результате этого оставшиеся легитимные агенты после выполнения закрепленных за ними задач должны повторить процедуру распределения задач и выполнить задачи, ранее закрепленные за вредоносными агентами. Моделирование выполнено на

языке программирования Python, результаты выполнения пространственно-распределенных задач агентами РРТС с различным количеством вредоносных агентов представлены в (Табл. 1).

Табл. 1. Показатели качества выполнения задания РРТС

Критерий	**Время выполнения задания, с**			
Количество агентов / вредоносных агентов	10 / 0	10 / 1	10 / 3	10 / 5
Максимальное значение	156,72	191,32	201,12	237,81
Среднее значение	121,23	134,34	146,14	161,95
Минимальное значение	99,73	101,17	102,61	110,07
Количество агентов / вредоносных агентов	50 / 0	50 / 1	50 / 13	50 / 25
Максимальное значение	160,97	182,17	202,81	223,65
Среднее значение	127,12	140,45	153,16	176,15
Минимальное значение	112,62	109,94	107,79	123,79
Количество агентов / вредоносных агентов	100 / 0	100 / 1	100 / 25	100 / 50
Максимальное значение	159,71	187,38	198,38	217,9
Среднее значение	129,08	140,67	164,46	177,32
Минимальное значение	113,43	115,65	118,28	144,57

Согласно полученным результатам (Табл. 2), при наличии 1 вредоносного агента среднее время выполнения задания РРТС увеличивается от 8,23% (129,08 с против 140,67 с). При масштабировании численности агентов РРТС и увеличении количества вредоносных агентов до 25% среднее время выполнения задания увеличивается на 17% (127,12 с против 153,16 с), а при наличии 50% вредоносных агентов – на 25,14% (121,23 с против 161,95 с).

Вторая частная научная задача связана с разработкой протокола делегированной аутентификации новых агентов при масштабировании численности агентов в РРТС на основе распределенного реестра и методов машинного обучения. Известные подходы к аутентификации агентов роевых робототехнических систем не учитывают свойство масштабируемости системы, что вызывает «лавинный эффект» при значительном увеличении численности агентов. Исходя из этого, целью решения второй частной научной задачи является повышение эффективности выполнения таких заданий агентами РРТС, которые требуют увеличения численности агентов, за счет уменьшения времени, необходимого для аутентификации новых агентов. Для достижения поставленной цели разработано расширение протокола для делегированной аутентификации новых агентов при масштабировании численности агентов РРТС на базе схемы идентификации Фейга-Фиата-Шамира с нулевым разглашением знаний. Элементом научной новизны является разработанный набор продукционных правил, представленных в виде дерева решений, позволяющих путем информационного обмена агентов с использованием распределенного реестра выполнить делегированную аутентификацию агентов, которые ранее прошли успешно эту процедуру. К отличительным особенностям представленного решения относятся возможность использования любого базового протокола аутентификации, удовлетворяющего аппаратным ограничениям вычислительной платформы робототехнических устройств, входящих в состав РРТС, а также возможность агентов «переключаться» между наиболее приоритетными задачами и взаимодействовать с другими агентами без повторной аутентификации, находясь в области действия бортовых средств связи по меньшей мере одного соседнего агента. Представленный протокол реализован в виде программного обеспечения на языке программирования Python. Полученные результаты моделирования с использованием разработанного и базового протоколов аутентификации представлены в (Табл. 2).

Табл. 2. Среднее время выполнения задания, с

Количество агентов РРТС / из них нарушителей	**Разработанный протокол**	**Базовый протокол**
10 / 0	42,9	45,13
10 / 1	46,72	48,98
10 / 3	48,35	50,58
10 / 5	51,97	54,2
50 / 0	68,37	95,07
50 / 1	69,45	96,65
50 / 13	74,82	102,25
50 / 25	73,97	96,23
100 / 0	109,77	172,17

100 / 1	110,13	176,87
100 / 25	109,53	172,07
100 / 50	107,43	167,33

Таким образом, согласно (Табл. 2), прирост среднего значения эффективности выполнения задания агентами РРТС при использовании предложенного протокола по сравнению с базовым составил:

- от 4,12% (51,97 с против 54,2 с) до 4,95% (42,9 с против 45,13 с) при РРТС из 10 агентов;
- от 23,14% (73,97 с против 96,23 с) до 28,14% (69,45 с против 96,65 с) при РРТС из 50 агентов;
- от 35,8% (107,43 с против 167,33 с) до 37,73% (110,13 с против 176,87 с) при РРТС, состоящей из 100 агентов.

Рекомендации и перспективы дальнейшей разработки темы. В традиционных иерархических системах управления принято выделять три основных уровня: стратегический, тактический и исполнительный [25]. С точки зрения модульной или компонентной парадигмы синтеза системы управления, предлагаемая интеллектуальная децентрализованную подсистема аутентификации и авторизации агентов при масштабировании численности РРТС (далее ИДП) может условно располагаться на любом (одном или нескольких) из уровней иерархической системы управления в зависимости от решаемой задачи. В этом случае можно говорить о преобразовании иерархической системы управления в гибридную, так как ИДП не влияет напрямую на работу устройств связи или периферийные устройства исполнительного уровня, а также может быть использована на широком классе роботов. Результатом синтеза интеллектуальной системы управления является унификация протоколов и интерфейсов передачи данных между различными уровнями системы. При использовании в качестве агентов РРТС робототехнических устройств с много платформенной конструкцией [26] предложенный подход обеспечит максимальное использование вычислительных ресурсов платформы, в которую интегрирована ИДП. В результате этого освобождаются ресурсы других вычислительных платформ, например, для выполнения задач картографии, распознавания и т.д.

Основная идея настоящего исследования заключается в реализации комплексного решения для обеспечения информационной безопасности в процессе функционирования РРТС. Исходя из этого, направление дальнейших исследований связано с интеграцией ИДП с другими решениями для защиты информации, затрагивающими те аспекты информационной безопасности, которые не рассматриваются в настоящем исследовании. Как отмечалось ранее, полученные результаты могут быть использованы на широком классе роботов, не только в РРТС, что также требует проведения дополнительных исследований и соответствующих модификаций.

1. СПИСОК ЛИТЕРАТУРЫ

2. Указ Президента Российской Федерации от 01.12.2016 г. № 642. Президент России [Электронный ресурс]. – Президент России. URL: http://www.kremlin.ru/acts/bank/41449 (дата обращения: 14.07.2022).
3. Указ Президента Российской Федерации от 10.10.2019 г. № 490. Президент России [Электронный ресурс]. – Президент России. URL: http://www.kremlin.ru/acts/bank/44731 (дата обращения: 14.07.2022).
4. Сэйфнет [Электронный ресурс]. – Национальная технологическая инициатива. URL: https://nti2035.ru/markets/safenet (дата обращения: 15.07.2022).
5. Павлов, А.С. Методика планирования траектории движения группы мобильных роботов в неизвестной замкнутой среде с препятствиями // Системы управления, связи и безопасности. – 2021. – №3. – С. 38-59.
6. O'Grady, R. Performance benefits of self-assembly in a swarm-bot / R. O'Grady, R. Gross, A.L. Christensen, F. Mondada, M. Bonani, M. Dorigo // IEEE/RSJ International Conference on Intelligent Robots and Systems. – 2007. – P. 2381-2387.
7. Dorigo, M. Swarmanoid: A Novel Concept for the Study of Heterogeneous Robotic Swarms / M. Dorigo, D. Floreano; L.M. Gambardella, F. Mondada, S. Nolfi, T. Baaboura // IEEE Robotics & Automation Magazine. – 2013. – Vol. 20, № 4. – P. 60-71.
8. Oh, H. Morphogen diffusion algorithms for tracking and herding using a swarm of kilobots. / H. Oh, A.R. Shiraz, Y. Jin // Soft Computing. – 2018. – Vol. 22, № 6. – P. 1833-1844.
9. Holland, J. Evolving Collective Behaviours in Simulated Kilobots / J. Holland, C. O'Riordan // Symposium on Applied Computing SAC'18. – 2018. P. 1-8.

10. Dimidov, C. Random walks in swarm robotics: an experiment with kilobots / C. Dimidov, G. Oriolo, V. Trianni // International Conference on Swarm Intelligence. – 2016. – P. 185-196.
11. Brambilla, M. Swarm robotics: a review from the swarm engineering perspective / M. Brambilla, E. Ferrante, M. Birattari, M. Dorigo // Swarm Intelligence. – 2013. – Vol. 7, № 1. – P. 1-41.
12. Ziyan продемонстрировала рой из 10 дронов-бомбардировщиков вертолетного типа [Электронный ресурс]. – Planet today. URL: https://planet-today.ru/novosti/armiya/armiimira/item/104438-ziyan-prodemonstrirovala-roj-iz-10-dronov-bombardirovshchikov-vertoletnogo-tipa (дата обращения: 14.07.2022).
13. Intel Lights Up the Night with 500 «Shooting Star» Drones [Электронный ресурс]. – Intel. URL: http://www.intel.com/content/www/us/en/technology-innovation/videos/drone-shooting-star-video.html (дата обращения: 01.08.2022).
14. Официальный сайт Amazon Robotics LLC [Электронный ресурс]. – Amazon Robotics LLC. URL: https://www.amazonrobotics.com/ (дата обращения: 01.08.2022).
15. Официальный сайт Alibaba Group [Электронный ресурс]. – Alibaba Group. URL: https://www.alibabagroup.com/en/global/home (дата обращения: 18.07.2022).
16. Zakiev, A. Swarm Robotics: Remarks on Terminology and Classification / A. Zakiev, T. Tsoy, E. Magid // Interactive Collaborative Robotics (ICR 2018). – 2018. – P. 291-300.
17. Petrenko, V.I. Path Planning Method in the Formation of the Configuration of a Multifunctional Modular Robot Using a Swarm Control Strategy / V.I. Petrenko, F.B. Tebueva, A.S. Pavlov, V.O. Antonov, M.S. Kochanov // 7th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS 2019). – 2019. – Vol. 166. – P. 165-170.
18. Li, S. The internet of things: a survey / S. Li, L.D. Xu, S. Zhao // Information Systems Frontiers. – 2015. – Vol. 17, № 2. – P. 243-259.
19. Zikratov, I.A. Securing swarm intellect robots with a police office model / I.A. Zikratov, I.S. Lebedev, A.V. Gurtov, E.V. Kuzmich // IEEE 8th International Conference on Application of Information and Communication Technologies (AICT). – 2014. – P. 1-5.
20. Басан, А.С. Анализ и разработка средств обеспечения безопасности для систем группового управления автономными мобильными роботами / А.С. Басан, Е.С. Басан, О. Б. Макаревич // Вопросы кибербезопасности. – 2017. – Т. 5, № 24. – С. 42–49.
21. Юрьева, Р.А. Иммунологические принципы принятия решения в мультиагентных робототехнических системах / Р.А. Юрьева, И.И. Комаров, И.И. Викснин // Глобальный научный потенциал. – 2015. – Т. 5, № 50. – С. 87-91.
22. Zikratov, I.A. Trust and Reputation Mechanisms for Multi-agent Robotic Systems / I.A. Zikratov, I.S. Lebedev, A.V. Gurtov // International Conference on Next Generation Wired/Wireless Networking. – 2014. – P. 106–120.
23. Юрьева, Р.А. Метод и модель выявления и идентификации угроз нарушения информационной безопасности мультиагентных робототехнических систем: дис. ... канд. техн. наук // Санкт-Петербург Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. 2017. 132 с.
24. Strobel, V. Managing byzantine robots via blockchain technology in a swarm robotics collective decision-making scenario: Robotics track / V. Strobel, E.C. Ferrer, M. Dorigo // International Conference on Autonomous Agents and Multiagent Systems. – 2018. – Vol. 1. – P. 541-549.
25. Петренко, В.И. Анализ рисков нарушения информационной безопасности в роевых робототехнических системах при масштабировании численности агентов / В.И. Петренко, Ф.Б. Тебуева, А.С. Павлов, И.В. Стручков // Прикаспийский журнал: управление и высокие технологии. – 2022. – №2. – С. 92-109.
26. Пшихопов, В.Х. Разработка интеллектуальной системы управления автономного подводного аппарата / В.Х. Пшихопов, Ю.В. Чернухин, А.А. Федотов // Известия ЮФУ. Технические науки. – 2014. – Т. 3, № 152. – С. 87-101.
27. Юдинцев Б.С. Синтез нейросетевой системы планирования траекторий для группы мобильных роботов // Системы управления, связи и безопасности. – 2019. – № 4. – С. 163-186.

Павлычев А.В.
ФГАОУ ВО «Дальневосточный федеральный университет»,
директор Центра информационной безопасности,
pavlychev.av@dvfu.ru

РАЗРАБОТКА ЭФФЕКТИВНОГО СПОСОБА ВЫЯВЛЕНИЯ СЛОЖНЫХ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Аннотация: В исследовании рассматривается способ выявления сложных компьютерных инцидентов, осуществляемых злоумышленниками с высоким потенциалом путем эксплуатации уязвимостей информационных систем. Способ основан на анализе записей в системных журналах операционной системы Microsoft Windows с использованием методов машинного обучения.

Функционирование любой программы, как вредоносной, так и легитимной, можно представить в виде уникального набора записей в системных журналах операционной системы, которые можно рассматривать в качестве признаков объекта. При исследовании достаточного количества образцов программного обеспечения можно выявить значения признаков, характерные для работы злоумышленника. С использованием методов машинного обучения строится модель, позволяющая выявлять объекты, подвергшиеся несанкционированному воздействию.

Эффективность описанного способа в рамках исследования составила 89%.

Ключевые слова: выявление компьютерных инцидентов, системные журналы Microsoft Windows, машинное обучение.

Современные геополитические вызовы диктуют новые требования к киберустойчивости цифровых сервисов, предназначенных для полноценного обеспечения интересов личности, общества и государства.

Указом Президента Российской Федерации от 2 июля 2021 г. № 400 утверждена Стратегия национальной безопасности Российской Федерации. Информационная безопасность впервые выделена в качестве одного из стратегических национальных приоритетов, направленных на обеспечение и защиту национальных интересов Российской Федерации. В стратегии целью обеспечения информационной безопасности определено укрепление суверенитета Российской Федерации в информационном пространстве.

Согласно указа Президента Российской Федерации от 1 мая 2022 г. N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», в каждом органе государственной власти и субъекте критической информационной инфраструктуры должно быть создано структурное подразделение, осуществляющее функции по обеспечению информационной безопасности, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

Актуальные угрозы и вопросы безопасности Российской Федерации в информационном пространстве озвучены Президентом России на заседании Совета безопасности России, прошедшем 20 мая 2022 г.

Государственная политика в области информационной безопасности сегодня включает следующие направления:

- обеспечение информационной безопасности отраслевых критически важных объектов, от которых напрямую зависит обороноспособность нашей страны, стабильное развитие экономики и социальной сферы;
- повышение защищённости информационных систем и сетей связи в государственных органах;
- снижение рисков, связанных с использованием зарубежных программ, вычислительной техники и телекоммуникационного оборудования.

В условиях фактически объявленной России кибервойны наибольшую опасность для цифрового суверенитета представляют злоумышленники с высоким потенциалом - профессиональные политически мотивированные хакеры из недружественных государств.

Согласно изученным аналитическим отчетам, в первом полугодии 2022 года количество инцидентов информационной безопасности в России выросло практически на четверть в сравнении с аналогичным периодом 2021 года. Наибольшее число инцидентов с разным уровнем критичности связано с применением хакерами вредоносного программного обеспечения (далее – вредоносного ПО). Наблюдается значительный рост инцидентов, связанных с эксплуатацией уязвимостей. Повышается скорость применения эксплойтов для проведения атак на ресурсы российских компаний.

Складывающаяся политическая обстановка говорит о дальнейшем росте хакерских атак на российскую информационную инфраструктуру с использованием новых видов кибероружия.

Указанные обстоятельства свидетельствуют о высокой актуальности проводимого исследования, целью которого является разработка эффективного способа выявления сложных компьютерных инцидентов с использованием методов машинного обучения.

Для достижения поставленной цели в рамках исследования поставлен ряд задач:

- Исследование структуры и содержания системных журналов информационных систем с точки зрения информационной безопасности;

- Проведение анализа сложных компьютерных инцидентов на предмет оставления следов в системных журналах информационной системы, подвергшейся несанкционированному воздействию;
- Разработка автоматизированного метода обработки данных системных журналов информационных систем, формирование набора данных для дальнейшего исследования;
- Изучение основных методов машинного обучения для решения задач в области информационной безопасности и выбор оптимального алгоритма машинного обучения с учетом полученного набора данных;
- Применение к полученным данным выбранного алгоритма машинного обучения и подбор оптимальных параметров для получения максимальной точности модели;
- Интерпретация полученных результатов и оценка эффективности рассматриваемого способа выявления компьютерных инцидентов.

Одной из важнейших задач информационной безопасности является борьба с вредоносным ПО и, в частности, подзадача по его обнаружению. В свете текущих тенденций развития вредоносных программ, все более актуальными становится задача создания эффективного средства обнаружения неизвестного вредоносного ПО.

Несмотря на существование множества видов вредоносного ПО, все они оставляют следы своей деятельности в операционной системе.

Одним из способов выявления компьютерных инцидентов является исследование файлов журналов различных информационных систем, в том числе системных журналов операционной системы на предмет выявления скрытых закономерностей и различных аномалий.

Несмотря на курс России на импортозамещение, в настоящее время операционная система Microsoft Windows установлена на подавляющем большинстве рабочих мест как обычных пользователей, так и в органах власти, предприятиях промышленности, транспорта, обороны, организациях финансового сектора и иных объектах критической информационной инфраструктуры.

В операционной системе Microsoft Windows ведутся журналы, которые регистрируют пользовательские события и работу системных и прикладных программ на компьютере. Журнал событий представляет собой бинарный файл специального формата (с расширением EVTX), схожий с файлом базы данных.

Журналы событий Windows содержат ряд дескрипторов, позволяющих объединять события в такие категории, как «информационные» и «критические». Отдельные идентификаторы указывают на конкретные типы событий, а последние версии Windows имеют отдельные файлы журналов событий для различных приложений и служб.

Набольший интерес для исследователей информационной безопасности представляет журнал Security (Безопасность) операционной системы Windows (Рис. 1).

	Уровень	Дата и время	Источник	Код события	Категория задачи	Описание	Имя файла
0	Сведения	16.02.2021 11:54:35	Microsoft-Windows-Security-Auditing	5145	Detailed File Share	Выполнена проверка сетевой папки на предмет во...	Security.csv
1	Сведения	16.02.2021 11:54:34	Microsoft-Windows-Security-Auditing	5158	Filtering Platform Connection	Платформа фильтрации IP-пакетов Windows разреш...	Security.csv
2	Сведения	16.02.2021 11:54:34	Microsoft-Windows-Security-Auditing	5158	Filtering Platform Connection	Платформа фильтрации IP-пакетов Windows разреш...	Security.csv
3	Сведения	16.02.2021 11:54:31	Microsoft-Windows-Security-Auditing	4689	Process Termination	Выполнен выход из процесса.\r\n\r\nСубъект:\r\...	Security.csv
4	Сведения	16.02.2021 11:54:31	Microsoft-Windows-Security-Auditing	5156	Filtering Platform Connection	Платформа фильтрации Windows разрешила подключ...	Security.csv

Рис. 1. Пример набора записей исследуемого объекта в журнале Security

Согласно официальной документации Microsoft журнал Security включает в себя 422 возможных события, каждому из которых присваивается уникальный код (EventID), начиная со значения 1100 и заканчивая значением 8191.

В рамках исследования с использованием Банка данных угроз ФСТЭК России выбран ряд уязвимостей операционных систем Windows, которые широко используются хакерскими группировками для компрометации целевых информационных систем:

CVE-2017-0144 / BDU:2017-01099 (CVSS v3.0 Base Score 9.8 HIGH) - уязвимость протокола SMBv1 операционной системы Microsoft Windows, позволяющая нарушителю выполнить произвольный код («EternalBlue»);

CVE-2020-0796 / BDU:2020-01005 (CVSS v3.0 Base Score 10 HIGH) - уязвимость реализации сетевого протокола Server Message Block (SMBv3) операционных систем Windows, позволяющая нарушителю выполнить произвольный код;

CVE-2021-1675 / BDU:2021-03322 (CVSS v3.0 Base Score 9.8 HIGH) – уязвимость операционных систем Windows, связанная с небезопасным управлением привилегиями, позволяющая нарушителю повысить свои привилегии («PrintNightmare»);

CVE-2021-24084 / BDU:2021-00932 (CVSS v3.0 Base Score 5.5 MEDIUM) - уязвимость диспетчера мобильных устройств Windows Mobile Device Management операционных систем Windows, позволяющая нарушителю получить несанкционированный доступ к защищаемой информации;

CVE-2021-36934 / BDU:2021-03913 (CVSS v3.0 Base Score 7.8 HIGH) - уязвимость операционных систем Windows, связанная с недостатками разграничения доступа, позволяющая нарушителю повысить свои привилегии («SeriousSAM» или «HiveNightmare»);

CVE-2021-40444 / BDU:2021-04442 (CVSS v3.0 Base Score 7.8 HIGH) - уязвимость механизма MSHTML браузера Internet Explorer, связанная с неверным управлением генерацией кода, позволяющая нарушителю выполнить произвольный код;

CVE-2021-40449 / BDU:2021-05018 (CVSS v3.0 Base Score 7.8 HIGH) - уязвимость компонента Win32k (Win32k.sys) операционной системы Windows, связанная с использованием памяти после её освобождения, позволяющая нарушителю повысить свои привилегии;

CVE-2022-21882 / BDU:2022-00596 (CVSS v3.0 Base Score 7.8 HIGH) - уязвимость компонента Win32k (Win32k.sys) операционных систем Windows, позволяющая нарушителю повысить свои привилегии;

CVE-2022-29072 / BDU:2022-02366 (CVSS v3.0 Base Score 7.8 HIGH) - уязвимость библиотеки 7z.dll файлового архиватора 7-Zip, позволяющая нарушителю повысить свои привилегии;

CVE-2022-30190 / BDU:2022-03226 (CVSS v3.0 Base Score 7.8 HIGH) - уязвимость утилиты сбора диагностических данных и устранения неполадок Microsoft Support Diagnostics Tool операционных систем Windows, связанная с ошибками при обработке вызываемого URL-адреса, позволяющая нарушителю выполнить произвольный код с привилегиями вызывающего приложения («Follina»).

На специально подготовленной инфраструктуре проведена эксплуатация указанных уязвимостей. После успешного применения вредоносного ПО осуществлен сбор и анализ записей журналов Security скомпрометированных рабочих станций. Установлено, что каждый эксплойт оставил уникальный набор записей в системных журналах (Рис. 2).

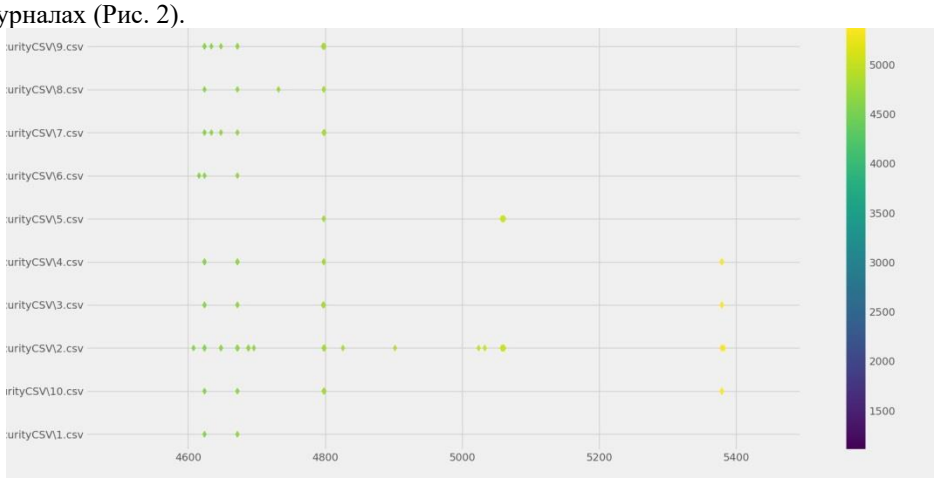


Рис. 2. Сравнительный анализ наборов записей в журналах Security

Для решения следующей задачи исследования разработана формализованная модель выявления признаков функционирования вредоносного ПО в исследуемой системе.

Пусть $Sec = \{Sec_1, \dots, Sec_p\}$ - множество булевых функций, где p – количество всех возможных событий, отображаемых в журнале Security операционной системы Windows (значение p является постоянной величиной и равняется 422).

Каждый элемент множества Sec имеет следующий смысл: функция Sec_i имеет значение 1, тогда и только тогда, когда за время выполнения программы происходило i-е событие из множества Sec, множества всех возможных событий журнала Security.

Определим любой элемент множества U, множества всех возможных программ как набор следующих векторов.

Каждый элемент U_i из множества U имеет вид:

$$U_i = \left\{ \begin{bmatrix} Sec_{1,i} \\ \dots \\ Sec_{p,i} \end{bmatrix} \right\}, i = \overline{1,n}. \quad (1)$$

Пусть $\varphi(U_i)$: $U_i \to \{0,1\}$ — функционал, обозначающий выполнение программы U_i и приводящий либо к безопасному состоянию системы (легитимное программное обеспечение), либо небезопасному состоянию (вредоносное программное обеспечение).

На следующем этапе исследования проведен эксперимент, в ходе которого на специально подготовленном стенде осуществлялся запуск как вредоносного программного обеспечения, так и легитимного программного обеспечения с дальнейшим сбором и обработкой журналов Security операционной системы.

В соответствии с разработанной моделью сформирован набор данных (датасет), содержащий уникальные наборы значений EventID журналов Security (Рис. 3)

1100	1101	1102	1104	1105	1108	4608	4609	4610	4611	...	6416	6417	6418	6419	6420	6421	6422	6423	6424	8191
0	1	0	0	0	0	1	0	0	0	...	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	0	0	0	...	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	0	0	0	...	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	0	0	0	...	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	1	0	0	0	...	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	0	0	0	...	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	0	0	0	...	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	0	0	0	...	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	0

Рис. 3. Пример уникальных наборов значений EventID журналов Security, полученных по результатам проведенного эксперимента

Ввиду значительных объемов событий в системных журналах необходимо применение автоматизированных методов обработки данных. Для решения данной задачи возможно использование методов машинного обучения.

Машинное обучение представляет собой метод анализа данных, который автоматизирует построение аналитических моделей. Это ветвь искусственного интеллекта, основанная на идее, что системы могут учиться на данных, выявлять закономерности и принимать решения с минимальным вмешательством человека.

Машинное обучение доказало свою эффективность в решении различных аналитических задач и все чаще используется для обнаружения угроз и автоматического устранения их, прежде чем они смогут нанести ущерб. Разработанные алгоритмы быстро сканирует большие объемы данных и анализирует их с помощью статистики.

В рамках проводимого исследовании основным подходом является Data Mining - выявление скрытых закономерностей и взаимозависимостей в больших наборах данных для поддержки принятия решений.

В технологии Data Mining гармонично объединены строго формализованные методы и методы неформального анализа, т.е. количественный и качественный анализ данных.

Большинство аналитических методов, используемые в технологии Data Mining – это известные математические алгоритмы и методы. Ввиду развития современных технологий данные методы широко применяются не только в теоретических исследованиях, но и для решения практических задач.

В рамках исследования изучен ряд прикладных способов обнаружения компьютерных инцидентов с использованием алгоритмов машинного обучения.

1. Деревья решений.

Дерево решений - логический алгоритм классификации, решающий задачи классификации и регрессии. Дерево решений – это метод машинного обучения, основанный на рекурсивной древовидной структуре. Дерево решений состоит из ряда элементов: корневого и промежуточного узла, пути и конечного узла. Корневой и промежуточный узел дерева представляет объект или атрибут. Каждый путь расхождения дерева представляет возможные значения родительского узла (объекта). Конечный узел соответствует прогнозируемой категории или классифицированному атрибуту. Результирующее дерево далее представляется в виде правил «если-то».

Данный метод используется в системе обнаружения и предотвращения вторжений SNORT. Авторы статьи «Using decision trees to improve signature- based intrusion detection» в своем эксперименте заменили правила SNORT с использованием модели дерева решений. Хотя авторы не приводят никаких количественных показателей, исследование выявило существенное ускорение с использованием алгоритма дерева решений, а время обработки правил резко сократилось.

2. Случайный лес.

Случайный лес – один из примеров объединения классификаторов в ансамбль. Для задачи классификации выбирается решение по большинству результатов, выданных классификаторами, а в задаче регрессии - по их среднему значению.

Таким образом, случайный лес представляет собой усреднение над решающими деревьями, при обучении которых для каждого разбиения признаки выбираются из некоторого случайного подмножества признаков.

Случайный лес имеет применение, например, для измерения объема спама и для обнаружения вторжений. Для тестирования метода по обнаружению вторжений использовался набор данных NSL-KDD. На данном наборе метод показал точность обнаружения вторжений 69,7% и 80,2%.

3. Байесовская сеть.

Байесовская сеть – это направленный ациклический граф, каждой вершине которого соответствует случайная переменная, а дуги графа кодируют отношения условной независимости между этими переменными. Узлы, представляющие потомка, зависят от родительских узлов, и каждый узел поддерживает состояния формы условной вероятности и случайной величины.

Байесовскую сеть можно использовать для обнаружения аномалий, а известные сигнатуры и шаблоны атак также можно сравнивать с потоковыми данными для известных атак. В статье «A framework for an adaptive

intrusion detection system using Bayesian network» авторы описывают создание системы обнаружения вторжений с использованием байесовской сети. Для моделирования системы использовался набор данных KDD с девятью его атрибутами. Модель обеспечила уровень обнаружения атак на уровне 99%.

4. Кластеризация.

Это метод обучения без учителя, в котором мера сходства используется для группировки данных. Алгоритмы кластеризации могут обучаться на данных, полученных в результате аудита, при этом оператору не требуется явное описание различных классов атак.

Авторы статьи «Intrusion signature creation via clustering anomalies» демонстрируют применение обнаружения сигнатур в реальном времени с использованием алгоритма кластеризации. Нормальный и аномальный сетевой трафик был создан схемой кластеризации на основе плотности, известной как Simple Logfile Clustering Tool (SLCT). Используются две схемы кластеризации: во-первых, схема для обнаружения обычных сценариев и сценариев атаки, во-вторых, другая схема используется для контролируемого определения нормального трафика. Для проверки модели использовался набор данных KDD. Для неизвестных атак (в том числе с использованием уязвимостей «нулевого дня») достигнута точность от 70% до 80%.

5. Нейронные сети.

Нейронная сеть (или искусственная нейронная сеть) строится по аналогии работы человеческого мозга. Сеть имеет структуру слоев, ввод данных активирует нейрон второго слоя сети, что, в свою очередь, выводит на следующий уровень иерархии и так далее. Вывод производится последним слоем сети. Функция, которая преобразует несколько входных параметров в один выходной называется искусственным нейроном. Одним из основных недостатков нейронной сети является большое количество времени, необходимого для обучения.

Автор статьи «Artificial neural networks for misuse detection» описывает модель нейронной сети, которая использует многокатегориальный классификатор для обнаружения аномалий. Данные классифицируются либо как обычный трафик, либо как вредоносный трафик. Для генерации данных использовался сетевой монитор RealSecure со встроенными сценариями атак. Предварительная обработка данных выполнялась с использованием девяти выбранных параметров: код ICMP, тип ICMP, адрес источника, адрес назначения, номер протокола, порт источника, порт назначения, длина необработанных данных и тип необработанных данных. Исследователи сообщают о частоте ошибок 0,058 и 0,070 во время сценариев обучения и тестирования. Точность алгоритма составила 93% на этапе тестирования.

6. Метод опорных векторов.

Метод опорных векторов считается наиболее часто используемым и успешным методом машинного обучения для задач кибербезопасности, особенно для средств обнаружения вторжений. Метод опорных векторов классифицирует и разделяет два класса данных по обе стороны от гиперплоскости. Точность классификации точек данных может быть повышена за счет увеличения расстояний между гиперплоскостями. Точки данных, лежащие на границе гиперплоскости называются опорными векторными точками. Метод опорных векторов, как и нейронные сети, требует много памяти для обработки и времени для обучения.

Подробное сравнение метода опорных векторов и искусственной нейронной сети провели авторы статьи «Application of SVM and ANN for intrusion detection». Сравнение проводилось на наборе данных KDD, на котором метод опорных векторов показал лучшие результаты.

В рамках исследования объектом изучения с помощью методов машинного обучения является набор данных, содержащий булевые функции, соответствующие наступлению определенного события и записанные в журнал Security. Построенная модель должна предсказывать, является ли программа с заданным набором признаков вредоносной (значение 1), либо легитимной (значение 0).

С учетом набора изучаемых данных и специфики решаемой задачи алгоритмом машинного обучения для анализа в рамках исследования выбран «случайный лес».

В качестве инструмента использовалась библиотека Scikit-learn, содержащая класс RandomForestClassifier.

Указанный алгоритм содержит следующие основные входные параметры:

n_estimators - число деревьев в «лесу»;

max_features - число признаков для ветвления;

max_depth - максимальная глубина дерева;

min_samples_split - минимальное число объектов, необходимое для того, чтобы узел дерева мог разделиться;

min_samples_leaf - минимальное число объектов в листьях;

bootstrap - использование для построения деревьев подвыборки с возвращением.

В рамках очередной задачи исследования осуществлен перебор различных параметров модели. Результаты сравнительного анализа приведены на Рис. 4.:

n_estimators	param_min_samples_split	param_min_samples_leaf	param_max_features	param_max_depth	param_bootstrap	mean_test_score	rank_test_score
700	2	2	log2	11	True	0.777778	1
300	18	39	log2	2	True	0.444444	2
800	39	44	sqrt	4	True	0.444444	2
200	39	44	sqrt	1	True	0.444444	2
1000	50	28	sqrt	4	True	0.444444	2
700	50	23	log2	2	True	0.444444	2
600	39	34	log2	13	True	0.444444	2
800	50	39	log2	1	True	0.444444	2
1000	7	12	sqrt	2	True	0.444444	2
700	23	12	sqrt	8	True	0.444444	2

Рис. 4. Результаты работы алгоритма с различным набором параметров

С использованием полученных результатов осуществлен поиск значений параметров, при которых эффективность модели является максимальной (Рис. 5).

```
{'bootstrap': True,
 'max_depth': 2,
 'max_features': 'log2',
 'min_samples_leaf': 2,
 'min_samples_split': 2,
 'n_estimators': 100}

classifier_best.score(x_train, y_train)

1.0

classifier_best.score(x_test, y_test)

0.8888888888888888
```

Рис. 5. Результат работы по выбору оптимальных параметров модели

Итоговая эффективность модели на тренировочной выборке составила 100%, а на тестовой выборке – 89%. Измерение эффективности модели производилось с помощью F-меры, которая гармонично учитывает как ложноположительные, так и ложноотрицательные значения классификатора. Такие значения как точность (recall) и полнота (precision), составили 80% и 100% соответственно (Рис. 6.).

```
'Hyperparameter Tuned Random Forest recall score'

0.8

'Hyperparameter Tuned Random Forest precision score'

1.0

'Hyperparameter Tuned Random Forest f1 score'

0.888888888888889
```

Рис. 6. Итоговые значения эффективности модели

Таким образом, в рамках исследования разработан классификатор, позволяющий с эффективностью 89% выявлять признаки сложных компьютерных инцидентов на основании анализа записей журналов операционной системы. Все задачи, поставленные в рамках исследования, решены, а цель – достигнута.

Исследование проведено при финансовой поддержке Минобрнауки России («Грант ИБ МТУСИ») № 40469-23-2021-К.

СПИСОК ЛИТЕРАТУРЫ

1. Атаки на российские компании во 2-м квартале 2022 года [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/analytics/reports/2880/, свободный (дата обращения: 02.08.2022).
2. R. Badhwar, The CISO’s Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms // Springer. – 2021. – P. 279–285.
3. N. Dutta, N. Jadav, S. Tanwar, Cyber Security: Issues and Current Trends // Springer. – 2021. – P. 129–141.
4. CIS Microsoft Windows Desktop Benchmarks: Securing Microsoft Windows Desktop An objective, consensus-driven security guideline for the Microsoft Windows Desktop Operating Systems [Электронный ресурс]. – Режим доступа: https://www.cisecurity.org/benchmark/microsoft_windows_desktop/, свободный (дата обращения: 12.08.2022).
5. Markus Ring, Daniel Schlör, Sarah Wunderlich, Dieter Landes, Andreas Hotho, Malware detection on windows audit logs using LSTMs // Computers & Security. – 2021. – Vol. 109. – P. 1-12.
6. Joseph Rabaiotti, Counter Intrusion Software: Malware Detection using Process Behaviour Classification and Machine Learning [Электронный ресурс]. – Режим доступа: URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.2417 &rep=rep1&type=pdf свободный (дата обращения: 10.07.2022).

7. Банк данных угроз безопасности информации [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/vul, свободный (дата обращения: 20.07.2022).
8. Zico J. Kolter, Marcus A. Maloof, Learning to Detect Malicious Executables in the Wild // Journal of Machine Learning Research. – 2006. – Vol. 7. – P. 2721-2744.
9. Павлычев А.В., Солдатов К.С., Сказин В.А. Выявление сетевых аномалий в системных журналах операционной системы Microsoft Windows с использованием методов машинного обучения // Доклады Томского государственного университета систем управления и радиоэлектроники. 2021. Т. 24. № 4. С. 27-32.
10. Farah Jemili, Montassar Zaghdoud, Mohamed Ben Ahmed, A framework for an adaptive intrusion detection system using Bayesian network // Intelligence and Security Informatics, IEEE. – 2007.
11. C. Kruegel, T. Toth, Using decision trees to improve signature-based intrusion detection // 6th International Workshop on the Recent Advances in Intrusion Detection, West Lafayette. – 2003. – P. 173–191.
12. Gilbert R. Hendry, Shanchieh Jay Yang, Intrusion signature creation via clustering anomalies // SPIE Defense and Security Symposium, International Society for Optics and Photonics. – 2008.
13. Cannady, Artificial neural networks for misuse detection // Proceedings of the 1998 National Information Systems Security Conference, Arlington, VA. – 1998. - P. 443.
14. Shu He, Gene Moo Lee, Sukjin Han, Andrew B. Whinston, How would information disclosure influence organizations' outbound spam volume? Evidence from a field experiment // Journal of Cybersecurity. – 2016. – Vol. 2. – P. 99-118.
15. Sean Miller, Curtis C.R. Busby-Earle, Multi-Perspective Machine Learning a Classifier Ensemble Method for Intrusion Detection // The 2017 International Conference on Machine Learning and Soft Computing. – 2017. - P. 7-12.
16. Wun-Hwa Chen, Sheng-Hsun Hsu, Hwang-Pin Shen, Application of SVM and ANN for intrusion detection // Computers & Operations Research. – 2005. – Vol. 32. – No. 10. – P. 2617-2634.
17. Bernhard Schölkopf, Robert C. Williamson, Alex Smola, John Shawe-Taylor, John Platt, Support vector method for novelty detection // Advances in Neural Information Processing Systems. – 2000. – P. 582-588.

Плаван А.И.
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики»,
аспирант,
aleksej-plavan@ya.ru

ОБНАРУЖЕНИЕ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА НА ОСНОВЕ ФИЛЬТРАЦИИ ЛИНЕЙНОГО ПРЕОБРАЗОВАНИЯ ТРАФИКА ПО КРИТЕРИЮ МИНИМУМА СРЕДНЕКВАДРАТИЧЕСКОЙ ОШИБКИ

Аннотация: в работе описывается идея применения линейного фильтра, оптимального пол критерию минимума среднеквадратичной ошибки, для обработки сетевого трафика с целью выявления аномального поведения. Сетевой трафик представляется в виде смеси случайного процесса с определенной корреляционной функцией и случайного процесса, представляющего погрешность измерений. По корреляционным функциям этих процессов определяется импульсная характеристика фильтра и ожидаемая ошибка фильтрации. При использовании фильтра вычисляется среднеквадратическая ошибка и сравнивается с ее ожидаемым значением. Отклонение значения ошибки является признаком наличия в фильтруемом трафике аномального процесса.

Ключевые слова: сетевой трафик, линейная фильтрация, среднеквадратическая ошибка, корреляция, самоподобие, коэффициент Херста, обнаружение аномалий.

На сегодняшний день обмен информацией через Интернет является неотъемлемой частью современной жизни. Различные телекоммуникационные сети организованы в предприятиях, государственных и частных предприятиях, банках, образовательных учреждениях – все они для качественного и своевременного предоставления различных услуг вынуждены хранить, передавать и обрабатывать огромные объемы информации. Для этого организуются телекоммуникационные сети различных уровней: отдельных рабочих отделов, предприятий, городов, стран и наконец все они объединяются через глобальную сеть — Интернет.

Пакеты, передаваемые по сетям, или трафик, часто становятся целью злоумышленников, ведь в них можно обнаружить пароли для доступа к разным ресурсам и другие ценные данные. Для противодействия им создаются сложные многоуровневые системы защиты информации. В состав этих систем входят различные средства защиты информации: антивирусы, межсетевые экраны, системы обнаружения и предотвращения вторжений, системы предотвращения утечек данных (DLP), криптографические средства защиты и др.

Системы обнаружения вторжений обычно являются аппаратно-программными или чисто программными решениями, которые автоматизируют процесс контроля протекающих в компьютерной сети или системе событий, а также самостоятельно анализируют данные события с целью поиска признаков проблем безопасности. Так как количество различных способов и типов организации несанкционированного доступа в чужие компьютерные сети только увеличивается, системы обнаружения атак стали необходимым компонентом инфраструктуры безопасности большинства организаций.

Один из принципов, на которых основаны системы обнаружения вторжений и некоторые другие средства защиты, состоит в том, что невозможно получить доступ к трафику извне, не повлияв на сам трафик, то есть, не установив соединение с некоторым сервером и не послав пакеты с некоторыми данными. Возникновение нового источника трафика приводит к изменению общего состояния и значений статистических характеристик сети.

Обнаружить постороннюю активность в сети можно с использованием инструментов для анализа трафика. При тестировании на проникновение анализ трафика является одним из важнейших этапов [1]. Анализ трафика позволяет выявить проблемы в работе сети (в том числе вызванные несанкционированной активностью), восстановить потоки данных и определить паттерны использования сети клиентами, осуществлять сбор статистики для развития и модернизации системы.

В телекоммуникационных и компьютерных сетях в качестве потока событий рассматривается случайная последовательность пакетов данных (образованная несколькими разными источниками), поступающих на обрабатывающее эти пакеты устройство. Данную последовательность и называют трафиком.

Трафик в телекоммуникационной сети можно рассматривать как случайный процесс, причем существует несколько интерпретаций:

1. Случайный поток событий: моменты поступления пакетов на вход обрабатывающего устройства рассматриваются как моменты поступления заявок, длительность обработки пакетов как длительность обработки заявки (Рис. 1). Следует заметить, что в реальных сетях интенсивность трафика может достигать очень высоких значений, и использование такого подхода непосредственно может быть затруднительно.

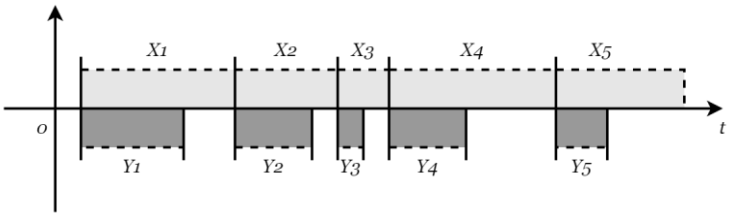


Рис. 1. Случайный поток событий

2. Случайный временной ряд: зависимость количества пакетов (или байт), пришедших на вход обрабатывающего устройства, в последовательные фиксированные одинаковые промежутки времени, от этих временных отсчетов (Рис. 2). Временной ряд обычно рассматривается в определенном временном масштабе, при этом значения внутри одного временного интервала суммируются.

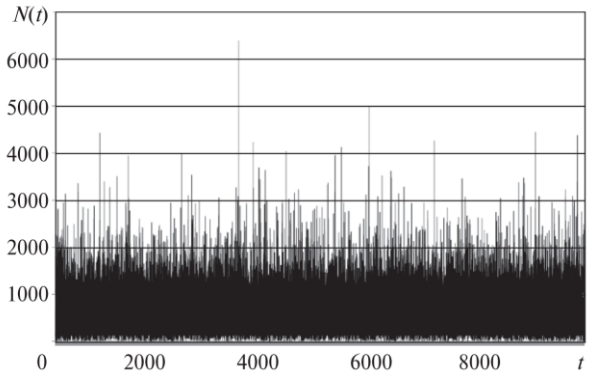


Рис. 2. Случайный временной ряд

Очевидно, что эти два представления взаимосвязаны между собой. Чем меньше интервалы между поступлениями пактов, тем больше пакетов поступит на вход обрабатывающего устройства в один временной промежуток, и тем больше будет соответствующее значение временного ряда. Можно перейти от случайного потока событий к временному ряду следующим образом: строится новая ось времени, деления на которой отмечаются в долях секунд, размер которых соответствует масштабу агрегации, затем подсчитывается количество поступлений пакетов (или сумма длин поступающих пакетов в байтах) между двумя последовательными временами на этой оси. Полученные значения образуют временной ряд. В дальнейшем будем рассматривать случайные процессы, представляющие трафик в одном из этих вариантов, с учетом того, какой из них удобнее использовать с рассматриваемым в текущий момент инструментом.

Случайным процессом называется случайная функция времени. Функция называется случайной, если в результате эксперимента она принимает тот или иной вид, причем заранее не известно, какой именно. Конкретный вид, который принимает случайный процесс в результате эксперимента, называется реализацией случайного процесса [2].

Характеристики случайного процесса в отличие от числовых характеристик случайных величин представляют собой неслучайные функции. Среди них для оценки случайного процесса широко применяются функции математического ожидания и дисперсии случайного процесса, а также корреляционная функция случайного процесса. Дисперсия случайного процесса характеризует разброс или рассеивание реализаций относительно функции математического ожидания. Корреляционной функцией случайного процесса называется функция двух переменных, которая каждой паре моментов времени сопоставляет корреляционный момент соответствующих сечений процесса.

Случайный процесс называется стационарным, если любые его вероятностные характеристики не зависят от сдвига начала отсчета времени. Для стационарного случайного процесса математическое ожидание и дисперсия постоянны, а корреляционная функция зависит лишь от разности моментов времени $\tau = t_2 - t_1$ и является функцией одного аргумента.

По мере развития сетевых технологий, обнаружилось, что соседние и близко расположенные отсчеты случайного процесса, представляющего сетевой трафик, имеют устойчивые корреляционные

связи. Из этого следует, что Интернет-трафик обладает свойством самоподобия или фрактальности, то есть сохраняет свои статистические характеристики при рассмотрении в разном временном масштабе. Впервые это было показано в [3], в дальнейшем эта тема исследовалась во многих работах [4–6]. Самоподобные процессы, обладающие долговременной зависимостью, как правило, характеризуются одномерными распределениями с «тяжелыми хвостами». Самоподобие Интернет-трафика не позволяет применять стандартные методы теории массового обслуживания и рассматривать трафик как случайную величину, обладающую гауссовским распределением, поскольку для распределений с тяжелыми хвостами характерные бесконечные дисперсия и математическое ожидание.

Основным методом изучения фрактальной структуры временных рядов является R/S-анализ, или метод нормированного размаха. Он был разработан английским гидрологом Гарольдом Эдвином Хёрстом. Коэффициент Херста может принимать значения от 0 до 1, при этом его значение говорит о следующем [7]:

- Если коэффициент >0,5, последовательность считается персистентной, обладающей фрактальными свойствами, значения коррелированы и имеют распределение «с тяжелыми хвостами».
- Если коэффициент равен 0,5, последовательности считаются независимыми величинами без явно выраженной корреляции.
- Если коэффициент <0,5, то такая последовательность считается антиперсистентной, то есть любая тенденция стремится смениться противоположной.

Для Интернет-трафика типовое значение коэффициента Херста составляет 0,65-0,8 или более [3].

Для описания трафика, обладающего свойством самоподобия и фрактальности, за прошедшее с момента обнаружения таких свойств время были созданы различные стохастические моделей. Они применяются для анализа производительности различных протоколов, алгоритмов или топологий сети, для воссоздания трасс трафика, приближенных к реальным, при имитационном моделировании в симуляторах трафика или в тестовых сетях. Существует множество разновидностей таких моделей [8], но в настоящее время нельзя выделить какую-то одну из них, как наиболее подходящую для о моделирования реалистичного самоподобного Интернет-трафика. К таким моделям относятся:

- Регрессионные модели (AR, MA, ARMA, ARIMA, FARIMA)
- Фрактальное броуновское движение
- Фрактальный гауссовский шум
- Фрактальное движение Леви
- On/Off модель
- Мультифрактальные модели
- Модели на основе вейвлетов
- Пакетный процесс Пуассона-Парето (PPBP)
- Пуассоновский процесс, управляемый марковской цепью (MMPP)
- M/G/∞-модель

Исследователи также предлагают множество новых моделей: в [9] предложена модель на основе сплайнов, в [10] рассматривается модифицированная alpha-beta On/Off модель, в которой учитываются короткие всплески интенсивности, в [11] предлагается модель на основе смеси распределений с тяжелыми хвостами. В целом можно сказать, что единого устоявшегося подхода к моделированию реалистичного трафика пока что не сложилось, и что анализ самоподобного сетевого Интернет-трафика и создание его реалистичной модели представляет интерес в области исследования телекоммуникационных сетей.

Для выявления посторонней активности в сетевом трафике существует несколько подходов: на основе обнаружения аномалий, обнаружения злоупотреблений и использование нейросетей. Подход на основе обнаружения аномальной активности состоит в создании профиля нормального поведения системы, включающий в себя определенный набор признаков и последующее сравнение текущего состояния системы с этим профилем. Профиль может быть создан для каждого временного периода, для которого характерны определенные значения параметров, например рабочий день, ночь, выходные и т.п. Подход на основе злоупотреблений включает в себя сравнение трафика с заранее определенными сигнатурами, свойственными для того или иного типа атак. Нейросетевой подход предполагает извлечение набора признаков из трафика, обучение модели на размеченных данных, валидацию модели на тестовых данных и последующее применение модели к трафику по принципу «черного ящика». Достоинства и недостатки обозначенных подходов подробно описаны в [12]. Зачастую применение того или иного подхода предполагает предварительную классификацию потоков данных

в трафике, идентифицируемых по пяти признакам: *адрес источника, порт источника, адрес назначения, порт назначения, используемый протокол*. Идентификация потоков теряет в производительности на больших объемах данных, то же самое происходит с методиками на основе сигнатур, особенно извлекаемых из содержимого пакета, а также с подходами на основе захвата трафика [13]. Статистические подходы, применяемые к трафику в целом, не вдаваясь в подробности отдельных пакетов выглядят более привлекательными.

В данной работе предлагается использовать методику, основанную на применении линейного фильтра Винера к процессу, представляющему сетевой трафик. Фильтр должен быть согласован по статистическим свойствам с ожидаемым в данный период времени трафиком, характерным для нормального профиля работы сети. Интенсивность трафика в сети можно выразить как аддитивную смесь $x(t) = s(t) + n(t)$, где $s(t)$ — процесс, представляющий нормальный трафик, $n(t)$ — шум (погрешность) измерений, определяющий ожидаемый разброс (дисперсию) значений оцениваемой величины. В качестве $s(t)$ можно рассматривать последовательность интервалов между прибытиями пакетов, количество поступивших пакетов за единицу времени (в различных масштабах долей секунд), суммарный объем байт за единицу времени или иные процессы, которые можно извлечь из трафика. Для применения фильтра данный процесс должен быть в широком смысле стационарным и обладать нулевым средним.

При оптимальной линейной фильтрации возникает ошибка оценивания (фильтрации), которая равна нулю, только в том случае, если энергетические спектры двух процессов не перекрываются [14]. Во временной области это значит, что процессы должны быть некоррелированными, то есть их взаимная корреляционная функция должна быть равна нулю при любых значениях временного сдвига. В реальности она будет иметь очень малые, но все же ненулевые значения, поэтому ошибка оценивания также будет отлична от нуля. Значение этой ошибки может быть получено при фильтрации *«нормального»* трафика. в момент, когда сеть функционирует в штатном режиме и аномальный трафик отсутствует.

Суть подхода состоит в том, что возникновение аномальной составляющей в фильтруемом трафике неизбежно приводит к изменению статистических свойств трафика и соответственно к изменению значения ошибки оценивания. Когда отклонение ошибки от ожидаемого значения превышает некоторый заранее заданный порог, это может служить сигналом о появлении в сети аномального процесса, вызванного хакерской сетевой атакой, сбоями в работе сетевого оборудования или изменением конфигурации сети.

Данный подход ориентирован на обнаружение сетевых атак, которые неявно влияют на статистические характеристики сетевого трафика, например сканирование сети, которое может быть первым этапом разведки перед основными действиями злоумышленников, распространение червей, необычные паттерны удаленного доступа и т.д. Резкие всплески интенсивности трафика из-за DoS- и DDoS-атак также должны приводить к изменению характеристик трафика, и соответственно тоже должны быть обнаружены, хотя для детектирования таких атак есть и более очевидные инструменты, основанные на сравнении обнаружении непропорционально большого количества пакетов определенного типа [15]. Данный метод не позволяет обнаруживать атаки уровня хоста, которые эксплуатируют уязвимости конкретного устройства и не связаны с передачей дополнительных данных по сети: вирусы, уязвимости ОС и приложений (переполнение буфера, повышение прав и т.п.), точечный перехват трафика, не влияющий на общую картину (MitM), атаки уровня приложений (php-, sql-инъекции) и т.д.

Импульсная переходная функция фильтра может меняться со временем, так как для разных временных периодов (рабочий день, ночь, выходные) ожидаемые значения статистических характеристик нормального трафика будут отличаться. В работе будет рассматриваться случай, когда характеристика фильтра не меняется со временем, но применение данного подхода для случая адаптивного фильтра также является актуальной задачей.

Оценка нормального трафика на выходе фильтра соответствует выражению (1.1).

$$\hat{s}(t) = \int_0^T h(t-u)x(u)du\,, \tag{1.1}$$

где $\hat{s}(t)$ — оценка процесса $s(t)$ по аддитивной смеси $x(t)$, $h(t)$ — импульсная характеристика фильтра, T — время наблюдения.

В [14] показано, что оптимальная по критерию минимума среднего квадрата ошибки (MSE) $M\{[s(t)-\hat{s}(t)]^2\} \to \min$ импульсная характеристика может быть получена путем решения интегрального уравнения (1.2), ошибка оценивания при использовании такой импульсной характеристики равна (1.3). Уравнение (1.2) также называется уравнением Винера-Хопфа. Предполагается, что случайный процесс, представляющий трафик, является стационарным, по крайней мере в широком смысле. Это накладывает дополнительное ограничение на временной период, в котором может быть использован фильтр с полученной импульсной характеристикой.

$$B_{xs}(\tau) = \int_0^T h(u) B_x(\tau - u) du \,, \tag{1.2}$$

$$\varepsilon_{\min}^2 = B_s(0) - \int_0^T h(u) B_{xs}(u) du \,, \tag{1.3}$$

где $B_{xs}(\tau)$ — взаимная корреляционная функция $x(t)$ и $s(t)$, $B_x(\tau)$ — корреляционная функция последовательности на входе фильтра, $B_s(\tau)$ — корреляционная функция процесса, представляющего трафик.

В [14] также показано, что если рассматривать не сам процесс, представляющий нормальный трафик, а его линейное преобразование (1.4), то формулы интегрального уравнения и ошибки оценивания можно записать как (1.5) и (1.6) соответственно.

$$\lambda(t) = \int_{-\infty}^{\infty} g(t-u) s(u) du \,, \tag{1.4}$$

где $\lambda(t)$ — линейное преобразование процесса, $g(t)$ — параметр линейного преобразования.

$$B_{x\lambda}(\tau) = \int_0^T h(u) B_x(\tau - u) du \,, \tag{1.5}$$

$$\varepsilon_{\min}^2 = B_\lambda(0) - \int_0^T h(u) B_{x\lambda}(u) du \,, \tag{1.6}$$

где $B_{x\lambda}(\tau)$ — взаимная корреляционная функция $x(t)$ и $\lambda(t)$, $B_\lambda(\tau)$ — корреляционная функция линейно-преобразованного процесса, представляющего трафик.

Вид линейного преобразования влияет лишь на выражения корреляционной функции $B_\lambda(\tau)$ и взаимной корреляционной функции $B_{x\lambda}(\tau)$. Если выбрать $g(\tau) = \delta(\tau - t - t_0)$, то эти выражения примут вид (1.7) и (1.8). При этом случай $t_0 > 0$ соответствует экстраполяции или (линейному) предсказанию значений случайного процесса, $t_0 = 0$ его фильтрации, а $-T \le t_0 < 0$ — интерполяции [14].

$$B_\lambda(\tau) = B_s(\tau + t_0) \,, \tag{1.7}$$

$$B_{x\lambda}(\tau) = B_s(\tau + t_0) + B_{sn}(\tau + t_0) \,, \tag{1.8}$$

где $B_{sn}(\tau)$ — взаимная корреляционная функция $s(t)$ и $n(t)$.

Решение интегрального уравнения (1.5) в общем случае может быть весьма затруднительно. Учитывая, что трафик предполагается наблюдать, захватывать и анализировать с использованием программных средств, то есть в системе с дискретным временем, уравнение для определения импульсной характеристики фильтра можно записать в виде (1.9).

$$B_{x\lambda}[n] = \sum_{k=0}^{N} h[k]\, B_x[n-k] = \sum_{k=0}^{N} h[n-k]\, B_x[k] \,, \tag{1.9}$$

Определить импульсную характеристику можно еще более удобным способом, если перейти к рассмотрению векторов и провести аналогичные вычисления записав выражение для оценки процесса на выходе фильтра в матричной форме. Соответствующий корреляционной функции $B_{<a>}$ вектор

будем обозначать как $\mathbf{b}_{<\mathbf{a}>}$. Тогда интегральное уравнение примет вид (1.10), а выражение для ошибки оценивания — (1.11).

$$\mathbf{b}_{\mathbf{x\lambda}} = \mathbf{H} \cdot \mathbf{b}_{\mathbf{x}} = \mathbf{B}_{\mathbf{x}} \cdot \mathbf{h}, \tag{1.10}$$

$$\varepsilon^2_{\min} = \mathbf{b}_{\lambda}[0] - \mathbf{h}^{\mathbf{T}} \cdot \mathbf{b}_{\mathbf{x\hat{\lambda}}}, \tag{1.11}$$

где $\mathbf{H}$ — импульсная характеристика в векторной форме, $\mathbf{B}_{\mathbf{x}}$ — корреляционная матрица последовательности на входе фильтра.

Корреляционная матрица $\mathbf{B}_{\mathbf{x}}$ — тёплицева матрица, получаемая из $\mathbf{b}_{\mathbf{x}}$ путем его циклического сдвига, соответственно являющаяся не вырожденной и имеющая обратную матрицу, отсюда импульсная характеристика может быть получена из выражения (1.12).

$$\mathbf{h} = \mathbf{B}_{\mathbf{x}}^{-1} \cdot \mathbf{b}_{\mathbf{x\hat{\lambda}}}, \tag{1.12}$$

В [16] показано, как можно получить выражение для ошибки независимо от полученной импульсной характеристики **h**. Так как в рассматриваемых в данном исследовании векторах не может быть комплексных значений, и с учетом ранее принятых обозначений, выражение для ошибки примет вид (1.13).

$$\varepsilon^2_{\min} = \mathbf{b}_{\lambda}[0] - \mathbf{b}^{\mathbf{T}}_{\mathbf{x\hat{\lambda}}} \cdot \mathbf{B}_{\mathbf{x}}^{-1} \cdot \mathbf{b}_{\mathbf{x\hat{\lambda}}}, \tag{1.13}$$

Корреляционная функция суммы двух случайных процессов может быть получена как сумма корреляционных функций этих процессов и их взаимных корреляционных функций. Учитывая это, а также (1.7) и (1.8) окончательно получаем выражения (1.14) и (1.15) для получения импульсной характеристики фильтра и ошибки оценивания.

$$\mathbf{h} = (\mathbf{B}_{\mathbf{s}} + \mathbf{B}_{\mathbf{sn}} + \mathbf{B}_{\mathbf{ns}} + \mathbf{B}_{\mathbf{n}})^{-1} \cdot (\mathbf{b}_{\mathbf{s}} + \mathbf{b}_{\mathbf{sn}}), \tag{1.14}$$

$$\varepsilon^2_{\min} = \mathbf{b}_{\mathbf{s}}[0] - (\mathbf{b}_{\mathbf{s}} + \mathbf{b}_{\mathbf{sn}})^{\mathbf{T}} \cdot (\mathbf{B}_{\mathbf{s}} + \mathbf{B}_{\mathbf{sn}} + \mathbf{B}_{\mathbf{ns}} + \mathbf{B}_{\mathbf{n}})^{-1} \cdot (\mathbf{b}_{\mathbf{s}} + \mathbf{b}_{\mathbf{sn}}), \tag{1.15}$$

Таким образом, для реализации фильтра необходимо знать автокорреляционные функции (АКФ) процессов $s(t)$, $n(t)$ и их взаимную корреляционную функцию (ВКФ). Если шум наблюдений $n(t)$ не коррелирован с процессом $s(t)$, это позволяет упростить выражение (1.12) и вычислить импульсную переходную функцию как (1.16) и минимальную ошибку фильтрации как (1.17).

$$\mathbf{h} = (\mathbf{B}_{\mathbf{s}} + \mathbf{B}_{\mathbf{n}})^{-1} \cdot \mathbf{b}_{\mathbf{s}}, \tag{1.16}$$

$$\varepsilon^2_{\min} = \mathbf{b}_{\mathbf{s}}[0] - \mathbf{b}_{\mathbf{s}}{}^{\mathbf{T}} \cdot (\mathbf{B}_{\mathbf{s}} + \mathbf{B}_{\mathbf{n}})^{-1} \cdot \mathbf{b}_{\mathbf{s}}, \tag{1.17}$$

Обнаружение аномалии производится путем сравнения ожидаемой минимальной среднеквадратической ошибки фильтрации, вычисляемой по выражению (1.15) и реальным значением, вычисляемым как $M\{[s(t) - \hat{s}(t)]^2\}$. Существенное отклонение значения ошибки фильтрации служит признаком аномалии. Более удобно использовать не само значение MSE, а ее нормализованное значение — NMSE. Для вычисления значений ожидаемой и реальной нормализованной ошибки в таком случае будут использоваться выражения (1.18) и (1.19) соответственно [16].

$$\varepsilon = \frac{\varepsilon^2_{\min}}{\sigma_s^2}, \tag{1.18}$$

$$\varepsilon = 1 - \frac{\sigma^2_{\hat{s}}}{\sigma_s^2}, \tag{1.19}$$

где σ_s^2 — дисперсия ожидаемого процесса, $\sigma_{\hat{s}}^2$ — дисперсия оценки процесса.

Для проверки методики было произведено моделирование такого фильтра на языке программирования Python. Сперва было произведено оценивание ошибки фильтрации трафика и сравнение ее с ожидаемым значением для смеси процесса с шумом оценивания, имеющими разные АКФ. Рассматривалось три варианта форма АКФ: экспоненциальная вида (1.20), треугольная вида (1.21) и некоррелированная (в виде дельта -импульса).

$$R(\tau) = \sigma^2 e^{-\frac{|\tau|}{\tau_0}}, \tag{1.20}$$

$$R(\tau) = \begin{cases} \sigma^2 \left(1 - \dfrac{|\tau|}{\tau_0}\right), |\tau| \le \tau_0 \\ 0, |\tau| > \tau_0 \end{cases}, \tag{1.21}$$

где σ^2 — дисперсия случайного процесса, τ_0 — время корреляции.

Для каждого случая было проведено 20 экспериментов. На первом этапе были сгенерированы по 20 случайных последовательностей длиной 50000 отсчетов для каждой заданной формы АКФ. Закон распределения случайного процесса во всех случаях гауссовский.

Реализации последовательностей были сгенерированы по методике авторегрессии (для экспоненциальной АКФ) и скользящего среднего (для треугольной АКФ) [17]. Результаты генерации представлены на графиках (Рис. 3). Сверху показаны первые 1000 отсчетов одной из реализаций, снизу выборочные АКФ для всех последовательностей, и заданная корреляционная функция (выделенная пунктирной черной линией). Графики слева относятся к последовательностям с экспоненциальной АКФ, справа — с треугольной.

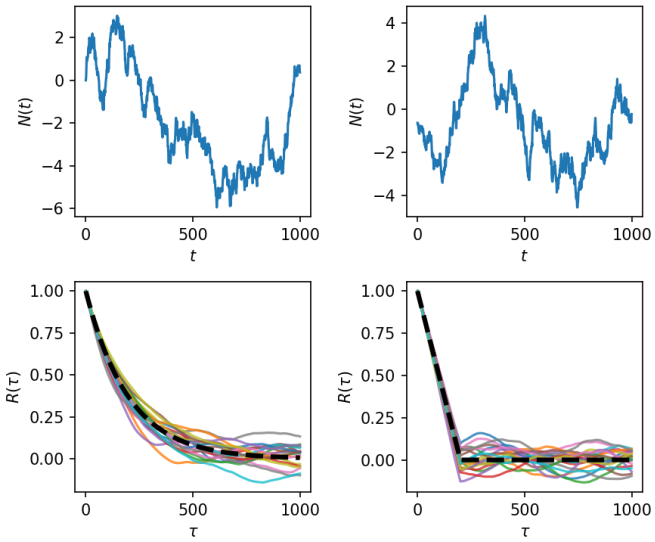


Рис. 3. Сгенерированные последовательности с заданными корреляционными функциями

Для каждого из трех случаев было получено ожидаемое значение минимальной среднеквадратической ошибки по формуле (1.17). Была произведена линейная фильтрация смеси последовательностей с рассматриваемыми АКФ и вычислены реальные значения нормализованной среднеквадратической ошибки. Значения ожидаемых и реальных ошибок для каждой последовательности приведены на графике на Рис. 4. По оси абсцисс отмечены ожидаемые значения ошибки фильтрации, вычисленные по формуле (1.18) а по оси ординат — реальные значения нормализованной среднеквадратической ошибки, вычисленные по формуле (1.19). Пунктиром отмечена линия $y = x$, к которой, при идеальной согласованности фильтра, должны приближаться все точки на графике. В этом случае значение ожидаемой ошибки совпадает с реальным. Условные обозначения для графиков на (Рис. 4) и (Рис. 5) приведены в (Табл. 1).

Табл. 1. Условные обозначения

№ п/п	Форма АКФ $s(t)$	Форма АКФ $n(t)$	Форма АКФ $a(t)$	Символ
1	Экспоненциальная	Треугольная	-	□
2	Дельта-импульс	Экспоненциальная	-	○

№ п/п	Форма АКФ $s(t)$	Форма АКФ $n(t)$	Форма АКФ $a(t)$	Символ
3	Треугольная	Дельта-импульс	-	
4	Экспоненциальная	Треугольная	Дельта-импульс	
5	Дельта-импульс	Экспоненциальная	Треугольная	
6	Треугольная	Дельта-импульс	Экспоненциальная	

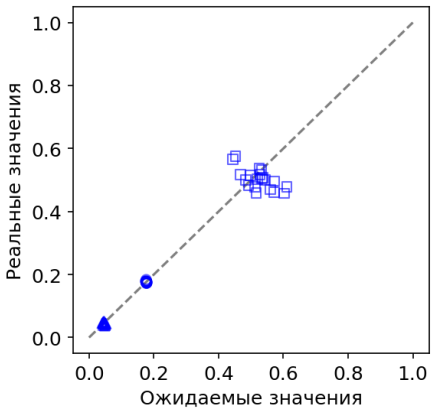


Рис. 4. Ошибки фильтрации процесса $x(t) = s(t) + n(t)$

По графику видно, что ближе всего реальная ошибка оказывается к ожидаемой в случае некоррелированного шума (№ 3 в Табл. 1), в этом же случае ошибка имеет минимальное значение. В случае (№ 2 в Табл. 1), когда трафик некоррелирован, а шум имеет экспоненциальную АКФ ожидаемое и реальное значение также совпадают, значение ошибки чуть выше. Если же и $s(t)$, и $n(t)$ имеют АКФ определенной формы (№ 1 в Табл. 1), то для разных реализаций значения ожидаемой и реальной ошибки расходятся в небольших пределах, в общем значение ошибки осциллирует возле значения 0,5. Это объясняется большей схожестью АКФ шума с АКФ ожидаемого случайного процесса в области $0 \le \tau \le \tau_0$, так как при моделировании использовались одни и те же параметры и между процессами $s(t)$ и $n(t)$ возможно возникновение нежелательной взаимной корреляции.

Затем к полученным на предыдущем шаге реализациям смеси нормального трафика с шумом был добавлен аномальный процесс с определенной АКФ. В этом случае так же была произведена линейная фильтрация и получены реальные значения ошибки. Ожидаемые значения ошибки совпадают со значениями из предыдущих расчетов, поскольку характеристики аномального процесса не учитываются при синтезе фильтра. График ошибок представлен на Рис. 5.

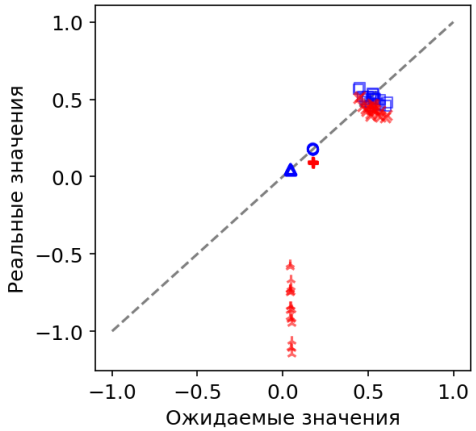


Рис. 5. Ошибки фильтрации процесса $x'(t) = s(t) + n(t) + a(t)$

По графику видно, что сильнее всего значения полученной реальной ошибки отличаются от ожидаемых для случая (№ 6 в Табл. 1), когда аномалия имеет экспоненциальную АКФ. В этом случае явно можно говорить о наличии аномального процесса в наблюдаемых процессах. В случаях (№ 4 в Табл. 1) и (№ 5 в Табл. 1) отклонение ошибки меньше, значение ошибки уменьшилось на небольшую величину. Для такой ситуации трафик является подозрительным и подлежит более детальному анализу со стороны специалистов.

Для определения статистической значимости наблюдаемого отклонения ожидаемой ошибки от реальной (с аномалией и без) был применен t-критерий Стьюдента для зависимых выборок (1.22), при этом оценивание значения ошибки фильтрации процесса выполнялось для одних и тех же сгенерированных реализаций процесса с заданной АКФ. В данном случае нулевая гипотеза H_0 состоит в том, что математическое ожидание в двух выборках совпадает. Для того, чтобы предложенный метод обнаружения атак корректно распознавал аномалии, необходимо, чтобы в случаях (№ 1, 2, 3 в Табл. 1) нулевую гипотезу нельзя было отвергнуть, а в случаях (№ 4, 5, 6 в Табл. 1) она отвергалась. Уровень значимости принимается равным 0,05. Результаты представлены в (Табл. 2).

$$t = \frac{M_d}{\sigma_d / \sqrt{n}}, \tag{1.22}$$

где M_d — средняя разность значений, σ_d — стандартное отклонение разностей, n — количество наблюдений.

Табл. 2. Значения t-критерия Стьюдента

№ п/п	Значение критерия	H_0
1	1,3963	Не отвергается
2	0.5721	Не отвергается
3	1.3541	Не отвергается
4	5.2698	Отвергается
5	82.9944	Отвергается
6	23.2774	Отвергается

По результатам вычисления t-критерия Стьюдента все отклонения можно считать статистически значимыми, следовательно отклонение реального значения нормализованной среднеквадратической ошибки может служить признаком наличия аномальной составляющей в случайном процессе, представляющем сетевой трафик. Для применения в реальной системе возможно определить численный диапазон возможных значений ошибки фильтрации, для большей производительности.

В данной работе был рассмотрен способ применения линейного фильтра, оптимального по критерию минимума среднеквадратической ошибки, к случайному процессу, выделенному из сетевого трафика, совместно с ожидаемым шумом (погрешностью) измерений. Получено ожидаемое (эталонное) значение ошибки фильтрации для процессов с заданными корреляционными свойствами. Для последовательности, обработанной фильтром, вычисляется среднеквадратическая ошибка, которая затем сравнивается с последовательностью с заданной АКФ. Отклонение полученного значения от эталонного служит признаком наличия аномалии в фильтруемой последовательности. Были вычислены ожидаемые и реальные значения ошибки для различных комбинаций процессов с треугольной, экспоненциальной АКФ, и без корреляции. Значимость отклонения значений ошибки была проверена с помощью t-критерия Стьюдента для зависимых выборок. Во всех случаях отклонение при наличии аномалии является статистически значимым.

В рамках дальнейшей работы необходимо рассмотреть следующие вопросы:

1. Найти более устойчивый и производительный алгоритм генерации случайных последовательностей с заданными характеристиками (АКФ), с возможностью применения в системах имитационного моделирования.
2. Определить критерии выделения временных периодов, в рамках которых трафик в сети сохраняет свои статистические свойства, а также рассмотреть случай адаптивной фильтрации.
3. Исследовать влияние взаимной корреляции между случайным процессом и шумом и аномалией на значения ошибки фильтрации.
4. Рассмотреть случай экстраполяции и интерполяции с использованием оптимальной фильтрации. Данный вариант использования может применяться при первоначальном определении нормального профиля трафика в сети.

СПИСОК ЛИТЕРАТУРЫ

1. Смирнов Г.Е. Анализ стандартов и методик тестирования на проникновение / Г.Е. Смирнов, С.И. Макаренко // Системы управления, связи и безопасности. 2020. № 4. С. 44–72.
2. Васильев К.К. и др. Теория электрической связи / под ред. Васильев К.К. Ульяновск: УлГТУ, 2008. 452 с.

3. Leland W.E. On the self-similar nature of Ethernet traffic (extended version) / W.E. Leland, M.S. Taqqu, W. Willinger, D.V. Wilson // IEEE/ACM Transactions on Networking. 1994. Т. 2, № 1. С. 1–15.
4. Шелухин О.И. Причины самоподобия телетрафика и методы оценки показателя Херста // Электротехнические и информационные комплексы и системы. 2007. Т. 3, № 1. С. 1.
5. Лебедев Н.А. Оценка степени самоподобия современного интернет-трафика и анализ полученных экспериментальным путём данных / Н.А. Лебедев, С.Д. Ерохин // Телекоммуникации И Информационные Технологии. 2017. Т. 4, № 1.
6. Петров В.В. То, что вы хотели знать о самоподобном телетрафике, но стеснялись спросить // М.: МЭИ, ИРЭ. 2003.
7. Карташевский В.Г. Основы теории массового обслуживания. Учебное пособие для вузов // М.: Горячая линия - Телеком, 2015. 126 с.
8. Шелухин О.И. Мультифракталы. Инфокоммуникационные приложения // М.: Горячая линия - Телеком, 2011. 576 с.
9. Strelkovskaya I. Modeling of Self-similar Traffic / I. Strelkovskaya, I. Solovskaya, N. Severin // Proc. of the 4th International Conference on Applied Innovations in IT, (ICAIIT). 2016. № 40. С. 4.
10. Sarvotham S. Network and user driven alpha-beta on–off source model for network traffic / S. Sarvotham, R. Riedi, R. Baraniuk // Computer Networks. 2005. Т. 48, № 3. С. 335–350.
11. Song Luo, Realistic Internet Traffic Simulation Through Mixture Modeling and a Case Study / Luo Song, G.A. Marin // Proceedings of the Winter Simulation Conference, 2005. Orlando, FL. USA: IEEE, 2005. С. 2408–2416.
12. Шелухин О.И. Обнаружение вторжений в компьютерные сети [сетевые аномалии] / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова // М: Горячая линия-Телеком, 2018. 220 с.
13. Гетьман А.И. Анализ сетевого трафика в режиме реального времени: обзор прикладных задач, подходов и решений / А.И. Гетьман, Е.Ф. Евстропов, Ю.В. Маркин // Препринт ИСП РАН. 2015. Т. 28. С. 1–52.
14. Б.Р. Левин. Теоретические основы статистической радиотехники. Книга вторая. 2-е-е изд. // М.: Советское радио, 1975. Т. 2. 392 с.
15. Антипов А. Методы защиты от DDoS нападений [Электронный ресурс]. 2003. URL: https://www.securitylab.ru/analytics/216251.php (дата обращения: 13.07.2022).
16. Haykin S.S. Adaptive filter theory. 4th ed. // Upper Saddle River, N.J: Prentice Hall, 2002. 920 с.
17. Быков В.В. Цифровое моделирование в статистической радиотехнике // М.: Советское радио, 1971. 328 с.

Плугатарев А.В.
Юго-Западный государственный университет,
аспирант,
aplugatarev@bk.ru

АЛГОРИТМ ИСПОЛЬЗОВАНИЯ МЕТАДАННЫХ ДЛЯ ИСПРАВЛЕНИЯ ОШИБОК АУТЕНТИФИКАЦИИ ПРИ СЕТЕВОМ ВЗАИМОДЕЙСТВИИ

Аннотация: Работа посвящена проблеме контроля аутентичности передаваемых по открытым каналам связи данных в распределённых системах. Целью исследования является создание модели определения источника сообщений в приёмнике, позволяющей на основе анализа характеристик распределения времени поступления сообщений повысить достоверность определения источника. Идентификация источника сообщений происходит на основе статистического анализа значений метаданных, которыми в данном исследовании и являются интервалы времени между поступившими сообщениями. Определение источника производилось с помощью методов кодирования в режиме сцепления блоков, которые обеспечивают более высокую достоверность идентификации для сообщений небольшой длины, характерных для указанного типа сетей. С помощью численного моделирования были определены закономерностей изменения характеристик времени поступления сообщений в случае возникновения ошибки идентификации. Так же сформулированы критерии принятия решения в случае невозможности проведения идентификации на основе обработки содержимого идентификационных полей. Итогом проведенных исследований является разработка модели аутентификации, основанной на анализе времени поступления сообщений на приёмник. Результат экспериментальных исследований показал возможность при помощи разработанной модели повысить достоверность определения аутентичности источника сообщений, снижения числа переспросов, возникающих при обнаружении ошибок, уменьшении размеров дополнительных полей идентификаторов в каждом сообщении.

Ключевые слова: удалённое взаимодействие, обработка информации, метаинформация, аутентификация.

Большинство современных информационных систем, в которых происходит обмен данными между её субъектами, спроектированы так, что, необходимым условием является использование механизмов контроля целостности и аутентичности передаваемых данных. Традиционным методом определения источника поступающих в приёмник информационных сообщений является введение в состав таких сообщений специальных полей, содержащих в явном или закодированном виде идентификатор источника. Размер полей служебной информации в таких методах должен быть минимальным для сокращения избыточности данных и повышения пропускной способности коммутационного канала. Таким образом, можно утверждать, что механизмы аутентификации требуют использования ресурсов информационной системы, которые по своей сути не направлены на непосредственное выполнение задач, выполняемых данной системой [1].

К методам проверки подлинности информационного сигнала выдвигаются различные требования к надёжности и ресурсным затратам, в зависимости от задач, для которых система была спроектирована. Как правило, все промышленные информационные системы выдвигают высокие требования к надёжности, и к экономии вычислительных ресурсов и ресурсов хранения данных. Как следствие, вопрос исследования, механизмов аутентификации актуален, так как с повышением мощностей вычислительной техники и прогрессу мировой сетевой инфраструктуры, возможности злоумышленников получить несанкционированный сетевой доступ возрастают, а ресурсы информационных систем, как правило имеют существенные ограничения, что и требует постоянных исследований в области защиты информации [2].

Главным преимуществом аутентификации при помощи метаданных, является то, что анализ аутентичности происходит на основе «данных о данных», то есть по информации, уже имеющимся в системе, без надобности хранить дополнительные массивы данных. Особо актуален данных вопрос для сетевых каналов с низкой пропускной способностью. Механизмы неявной аутентификации постепенно входят в нашу жизнь, их применяют всё больше крупных корпораций. Однако полностью данный механизм пока не может заменить явную аутентификацию, и лишь на начальном этапе отсеивает явные попытки несанкционированного доступа, и подтверждает явную подлинность пользователей, что, однако, уже позволяет значительно снизить информационную избыточность методов контроля целостности и аутентичности и повысить пропускную способность канала [3].

Особенно это актуально в системах, где на размер пакета по ряду причин, будь то низкая пропускная способность канала или необходимость в небольшом времени отклика, накладываются значительные ограничения. Если в протоколах, где размер единицы сетевого взаимодействия составляет несколько килобайт, а один – два байта дополнительной информации незначительно скажутся на общем объёме информации, то для протоколов, в которых размер блока ограничен несколькими десятками байтов, дополнительные поля будут оказывать существенное влияние на пропускную способность канала. Примером таких протоколов могут быть протоколы обмена данными между устройствами интернета вещей, сенсорных сетей, протоколы радиоидентификации, протоколы управления реальными технологическими процессами. В таких системах использование метаданных информационных пакетов может существенно повысить защищённость процесса информационного обмена между субъектами [4].

Краткий обзор экспериментальных научных исследований показал, что проблеме экономии ресурса и повышения достоверности определения источника сообщений при помощи нестандартных методов посвящено множество работ. Исследованиями в методологической области аутентификации занимались такие авторы как Македонский С. А., Коржик В. И., Приходько Н. В, Kang M. J., O. Riva. В своих исследованиях, данные авторы исследуют качественные значения различных видов аутентификации, в том числе и неявных методов. Приводятся сравнительные характеристики, и обоснование для применения того или иного метода для определённого круга задач. Все значимые теоретические разработки методов оценки ошибок неявной аутентификации получали практическую реализацию и проводились соответствующие экспериментальные исследованиях [5-8].

Исследователи экспериментируют с различными данными и различными методами определения порогового значения обнаружения ошибки. Данные исследования интересны тем, что используют вероятностные способы определения пороговых значений ошибки, и для этих целей используются массивы динамических цифровых данных. Однако, эти исследования ограничены для аутентификаций типа человек-система [9]. Был разработан протокол аутентификации для коммутации устройств интернета вещей, совмещающий классическую криптографию и анализ метаданных, что отлично иллюстрирует увеличение ёмкости канала передачи данных при использовании метаинформации. А схожий метод проверки подлинности для мобильных устройств, основывается на анализе поведенческих факторов; после обучения системы, работает в фоновом режиме и вычисляет подозрительную активность. Однако, данные методы требуют сбора информации, и вычислительных ресурсов, а предлагаемый метод основывается на метаинформации о пакетах придачи данных.

Методы, которые более применимы для модели, рассматриваемой в данном диссертационном исследовании информационных систем, описаны в работах [10-11]. Авторы работы [10] определяют оптимальное признаковое пространство и способы дополнительного определения источника сообщений, позволяющего повысить достоверность отождествления источников с имеющимися записями в базе данных информационной системы, применяемого в сервисе аутентификации. В патенте [11] аутентификация пользователя выполняются автоматически без каких-либо действий пользователя, поскольку доставка паролей не требуется для функционирования системы.

Описываемое диссертационное исследование ставит перед собой следующие цели и задачи:

1. исследование и анализ существующих подходов и методов аутентификации с использованием метаданных;
2. разработка модели определения источника сообщений на основе анализа времени их поступления;
3. разработка метода проверки подлинности сигнала источника сообщений на основе анализа времени их поступления на приёмник, а именно, на анализе характеристик распределения моментов высоких порядков для рядов временных задержек;
4. проведение вычислительного эксперимента, с применением разработанного программного и аппаратного обеспечения и обоснование применимости разработанной модели аутентификации.

Научная новизна исследования состоит в методе повышения достоверности, основанного на аутентификационных кодах сообщений, отличающийся тем, что на основе времени поступления сообщений, позволяет повысить достоверность определения источника сообщений; в модели обмена данными в распределённой информационной системе, которая позволяет формировать временные интервалы для получения оценки аутентичности при использовании характеристик распределения моментов высокого порядка.

Теоретическая значимость работы определяется тем, что показана возможность обнаруживать нарушения аутентичности или целостности информации при передаче данных, основанные на анализе таких метаданных, как время поступления сообщения на устройство-приёмник. Получены результаты

возможности принятия решения об аутентичности источника сигнала на основе коэффициента асимметрии и коэффициента эксцесса при анализе значений временных задержек принятых сообщений.

Практическая значимость работы определяется тем, что проведенные вычислительные эксперименты программных и аппаратных реализаций алгоритмов подтверждают результативность использования времени поступления сообщений на приёмник для аутентификации источника на реальных данных.

Методологической основой исследования являются методы моделирования алгоритмов обнаружения ошибок аутентификации, и вычислительного эксперимента проверки разработанных моделей. Также применяются такие методы и приемы, как научная абстракция, анализ и синтез, методы группировки, сравнения и другие.

Теоретическую основу исследования составляют научные труды в области методологии организации информационной безопасности информационных систем, исследований алгоритмов неявной аутентификации, исследований особенностей проектирования IoT-систем и информационных систем с низкой пропускной способностью.

На защиту данного диссертационного исследования выносятся следующие положения:

1. установлено, что методы контроля аутентификации, основанные на алгоритмах анализа временных интервалов поступления на приёмник единиц сетевого взаимодействия, позволяют значительно снизить информационную избыточность методов контроля целостности и аутентичности, а также повысить пропускную способность канала;
2. алгоритмы вычисления порогового значения вероятности обнаружения ошибки аутентификации, основанные на анализе метаинформации единиц сетевого взаимодействия, повышают вероятность обнаружения несанкционированного доступа к информационной системе;
3. программные и аппаратные реализации алгоритмов контроля аутентификации, основанные на анализе метаданных, значительно снижают время прохождения аутентификации на устройстве-приёмнике и повышают пропускную способность канала.

Диссертационное исследование прошло апробацию результатов на научно-технических конференциях: Современные информационные технологии и информационная безопасность (Курск), Распознавание – 2021 (Курск), Международной научно-технической конференции «Автоматизация» (RusAutoCon-2022)(Сочи), а результаты исследований опубликованы в издательствах перечня ВАК: Безопасность информационных технологий (Национальный исследовательский ядерный университет МИФИ); Известия Юго-западного государственного университета (ФГБОУ ВО «Юго-Западный государственный университет»).

В рамках диссертационного исследования рассматривается система, где источник, генерируя информационные пакеты к сообщениям добавляет значение хеш-функции от этого сообщения, соответственно на стороне приёмника также вычисляется значение хеш-функции от полученных сообщения.

В пределах исследуемой модели, во время сетевого взаимодействия, на приёмник в некоторое временное окно поступает множество сообщений. Так как результат обработки сообщений формируется не для отдельного сообщения, а для пула сообщений целиком, то, используется буферизация полученных N последних по времени поступления на приёмник сообщений. Каждое принятое сообщение получает уникальный порядковый номер i. На первом этапе буферизации сообщений на приёмнике необходимо сформировать цепочки последовательностей сообщений. В процессе сетевого взаимодействия в рамках временного промежутка, ограниченного по количеству принятых сообщений на приёмник, каждое поступившее сообщение n_i содержит имитовставку (кодовую последовательность). Имитовставка сравнивается и имитовставками всех уже пришедших сообщений на приёмник порядковый номер поступления которых меньше i. Условием для включения сообщения в последовательности является полное равенство полученного значения хеш-функции (имитовставки), сформированной из данных предыдущих блоков цепочки содержимого. При совпадении хэша, считаем принятое сообщение продолжением соответственного сообщения, фиксируем временной интервал между n_i и n_{i-1}.

На следующем этапе обработки данных на основе разницы поступления сообщений на приёмник, в буфере устройства, формируется граф сеанса. Формальное представление такого графа выглядит так, что каждый сеанс представляет из себя ориентированный взвешенный граф:

$$G = \{V, R\}, \quad (1)$$

где вершины V – представляют из себя множество сообщений, поступивших на приёмник, а R – множество пар сообщений $v, v' \in V$, соответственно дуга (v, v') – это два сообщения с совпадающей имитовставкой, так что время поступления $t(v_{i-1}) < t(v_i)$.

Новое полученное приёмником, сообщение приёмником n_i добавляет вершину v_i в множество V, соединённую с ребром (v, v') из множества R если имитовставки n_{i-1} и n_i совпадают. Вес получившегося ребра графа определяем по формуле:

$$r_{v_i - v_{i-1}} = t(v_i) - t(v_{i-1}) \quad (2)$$

В итоге, в буфере данных содержится информация об ориентированном графе, вершины которого – сообщения пришедшие на приёмник, а ребра – временная задержка между сообщениями, вершины графов которых соответствуют тем сообщениям, которые это ребро соединяет. Матрица расстояний в получившемся графе сеанса, с длиной цепочки n будет выглядеть следующим образом:

$$M = \begin{Bmatrix} r_{00} & r_{01} & \dots & r_{0n} \\ r_{01} & r_{12} & \dots & r_{1n} \\ & & \dots & \\ r_{n0} & r_{n1} & \dots & r_{nn} \end{Bmatrix} \quad (3)$$

Значение каждого элемента r_{kl} – временная задержка между поступлениями на приёмник сообщения с индексом l и k.

В ситуации, когда с каждым новым поступившем сообщением однозначно определяется его принадлежность к целевому источнику, информация из первого столбца и первой строки удаляется, и дополняется строкой n и столбцом n (в таком случае содержимое матрицы не меняется). Как только появляется сообщение, которое невозможно однозначно идентифицировать, матрица изменяется лишь добавлением строк и столбцов, до тех пор, пока в графе не образуется несколько идущих подряд однозначно аутентифицированных отдельных сообщений.

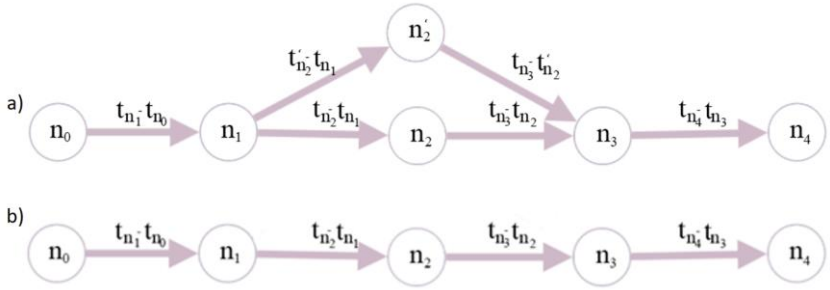


Рис. 1. Пример графов сообщений.

На примере из рисунка 1(а) существует две возможные аутентичные цепочки сообщений длины N=5 из-за того, что в промежуток времени t_3 и t_1 на приёмник поступило два сообщения. При анализе результатов, полученных на основе описанной модели формирования временных интервалов между сообщениями, формируются две цепочки временных задержек (n_0–n_1–n_2'–n_3–n_4 и n_0–n_1–n_2–n_3–n_4, рисунок 1). Возникает задача определения аутентичной цепочки сообщений.

На следующем этапе необходимо зафиксировать все пути графа длиной N – параметра, выбирается для достижения необходимой достоверности. Если такая цепочка одна, то на приёмник поступили сообщения в сеансе однозначно только от целевого источника. В рамках описываемого алгоритма фиксация происходит при модифицированном методе обхода графа в глубину.

В рамках вышеописанной модели задача сравнения двух небольших выборок одинакового размера с одинаковыми элементами за исключением 1-3 последовательных возникает на этапе принятия решения о принадлежности цепочки сообщений целевому источнику.

Исследования [12] характеристик моментов высокого порядка позволяют классифицировать различные законы распределения, в том числе по коэффициентам асимметрии и эксцесса [13]. Учитывая, что сообщения, передаваемые целевым источником, генерируются по модели типа ALOHA, значения временной задержки будут иметь свои характеристики распределения [14].

Также выводы, полученные в результате исследований однородности случайных выборок [15] и аномальных значений выборки, полученных из наборов выборок [16], позволяют использовать моментные характеристики высокого порядка для анализа и сравнения небольших выборок, таких как временные интервалы между сообщениями образуя единую цепь. Учитывая вышесказанное, возникла гипотеза о возможности использования таких характеристик распределения, как коэффициенты асимметрии и эксцесса, для корректной идентификации несанкционированных сообщений в цепочке.

График, построенный в единой системе координат, где по горизонтальной и вертикальной осям отложены соответственно коэффициенты асимметрии и эксцесса, позволяет легко проследить

тенденции смещения коэффициентов для цепочек несанкционированных сообщений. На рис. 3 для наглядности показаны результаты 10^2 экспериментов при N = 32. В цепочке сообщений присутствует одно несанкционированное сообщение.

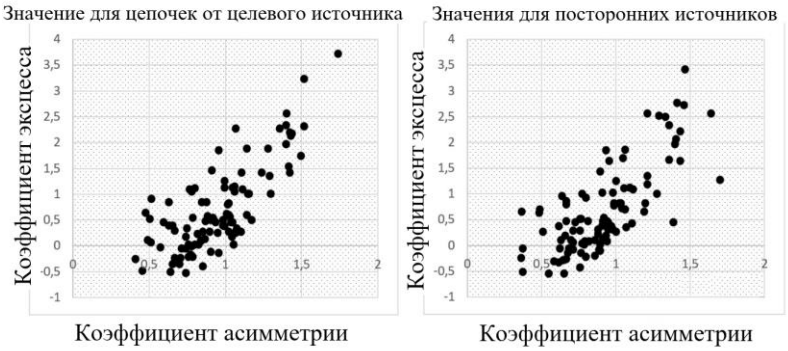


Рис. 2. Примеры значений эксцесса и коэффициента асимметрии для целевых и неавторизованных цепей для 10^2 временных интервалов

На рисунке 2 наглядно показана тенденция к массовому смещению значений в начало координат. Безусловно есть значения для посторонних источников, которые не уменьшаются по всем осям, однако, визуально, общая тенденция просматривается.

Для получения достоверного результата, при котором средняя доля ошибок могла бы характеризовать вероятность возникновения ошибки, в рамках первого эксперимента, в сеанс случайным образом добавлялось одно ложное сообщение, общее число экспериментов для каждого N проводилось в количестве 10^5.

Эксперименты показали, что максимальный процент успешного определения цепочки сообщений от целевого источника в рассматриваемом методе достигается при возрастании N (а именно при N>32) и использовании правила, формализованного как:

$$auth = (K_A > K'_A)\ or\ (K_Э > K'_Э) \qquad (4)$$

где, K_A и $K_Э$ – коэффициенты асимметрии и эксцесса, рассчитанные для цепочки сообщений, которую, согласно обсуждаемому методу, определяем как цепочку сообщений целевого источника, а K'_A и $K'_Э$ – коэффициенты асимметрии и эксцесса, рассчитанные для последовательности сообщений, определяемой как последовательность, включающая сообщения нецелевого источника. Иными словами, цепочкой сообщений целевого источника признаётся цепочка, у которой больше рассчитанный для неё либо коэффициент асимметрии, либо коэффициент эксцесса.

Далее была рассмотрена модель с открытым каналом связи, в котором присутствует множество устройств-источников, с одним приёмником-хабом. В данном случае, наиболее приближенном к реальным системам, критерий на основе характеристик распределения имеет следующий вид:

$$auth = (K_A > K'_A)\ and\ (K'_Э > K'_Э) \qquad (5)$$

Такое правило успешной аутентификации применимо для ситуации, когда соблюдается критерий:

$$| K'_Э | > | 2 \cdot K'_Э | \qquad (6)$$

Общая доля ситуаций, подходящих под критерий (6), составляет примерно 40%. Успешность аутентификации по данному критерию оценивается, как больше 90%. Таким образом, применение данного метода позволит избавится от необходимости аутентификации в примерно 40% случаев. График успешности и доля в системе с 40 устройствами представлен ниже.

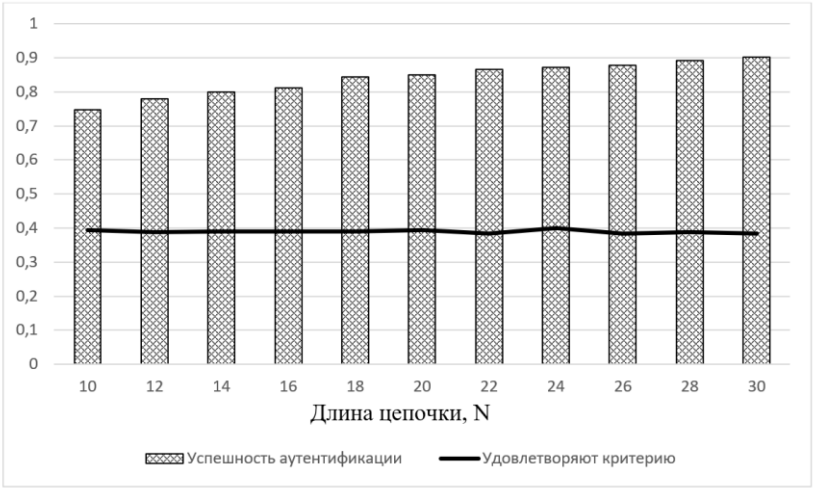


Рис.3. Значения успешной аутентификации.

На рисунке 3 показана доля успешных аутентификаций (5) и доля ситуаций, подходящих под критерий (6). Из графика видно тенденция к возрастанию успешности аутентификации, и достигает вероятности 0,9 при N=30, а доля ситуаций, удовлетворяющих критерию (6), не меняется. Это означает, что максимальной эффективности алгоритм, в распределённой сети с 40 устройствами достигает начиная с N=30.

Основные этапы метода определения источника сообщений на основе анализа времени их поступления могут быть представлены следующим образом:

1. буферизация сообщений и фиксация времени поступления каждого из них на приёмнике: во множестве сообщений от источника выделяются подмножества сообщений, объединённых в сеанс, то есть буферизуются согласно установленному заранее количеству;

2. формирование на основании анализа кодов аутентификации сообщений и временных интервалов сообщений взвешенного графа (1);

3. в случае, когда в графе сеанса присутствует более чем одна цепочка необходимой длины N, находим коэффициенты эксцесса и асимметрии из выборок, представленных весами дуг соответствующих цепочек;

4. считать ту цепочку сообщений от целевого источника, которая удовлетворяет критериям (4-6).

В заключении стоит отметить, что исследования подтвердили возможность использования метаданных, а именно времени поступления сообщений для повышения вероятности определения источника. Применена модель оценки выборок при использовании характеристик моментов высоких порядков (таких как коэффициент асимметрии и коэффициент эксцесса), которая является действенным средством анализа выборок небольшого размера. Показано, что сочетание режима сцепления блоков для аутентификации с использованием анализа времени поступления в сетевой модели типа ALOHA позволяет исключить необходимость аутентификации в примерно в 40 % случаев.

К рекомендациям дальнейших исследований данной тематики можно отнести поиск критериев большей достоверности для цепочек сообщений меньшей длины, и поиск критериев, позволяющий увеличить долю сообщений, которую возможно однозначно аутентифицировать.

СПИСОК ЛИТЕРАТУРЫ

1. Буренин А.Н., Основные проблемы безопасности подсистем обеспечения единым временем элементов систем управления сложными организационно-техническими объектами / Буренин А.Н., Легков К.Е. // T-comm: телекоммуникации и транспорт. 2019. С. 48.
2. Dr. Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martinez, Michael Baucom, Chris Eagle, The late Shon Harris. Gray Hat Hacking: The Ethical Hacker’s Handbook, Fifth Edition. - McGraw-Hill Education, 2018. 640 с.
3. Blerton Abazi, Application of biometric models of authentication in mobile equipment./ Blerton Abazi, Besnik Qehaja, Edmond Hajrizi. // IFAC-PapersOnLineVolume 52, Is. 252019. P. 543-546.
4. Лоднева О.Н., Анализ трафика устройств интернета вещей. / Лоднева О.Н., Ромасевич Е.П. // Современные информационные технологии и ИТ-образование Том 14, № 1. 2018, с. 149 – 169.

5. Македонский С. А., Сухаревская Е. В. Разработка формальной модели исследования систем аутентификации. // ISSN 2305-7815. Вестн. Волгогр. гос. ун-та. Сер. 10, Иннов. деят. 2017. Т. 11. № 3.
6. M. J. Kang and J. W. Kang. “A novel intrusion detection method using deep neural network for in-vehicle network security”, Vehicular Technology Conference, 2016.
7. Безопасность информационных систем [Текст]: учеб. пособие: / Марухленко А.Л., Таныгин М.О., Ефремов М.А., Спеваков А.Г; Юго-Зап. гос.ун-т. Курск, 2019. 210 с.
8. O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos, "Progressive Authentication: Deciding When to Authenticate on Mobile Phones." In USENIX Security Symposium, pp. 301-316. 2012.
9. William Cheung, Sudip Vhaduri. Context-Dependent Implicit Authentication for Wearable Device User. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2020.
10. Исхаков А.Ю., Повышение защищенности сервисов аутентификации путем проведения дополнительной идентификации с использованием оптимального признакового пространства / Исхаков А.Ю., Исхаков С.Ю., Мещеряков Р.В. / В сборнике: Информационные технологии в науке, управлении, социальной сфере и медицине. Сборник научных трудов IV Международной конференции: в 2 частях. Томский политехнический университет. 2017. С. 117-122.
11. Кярккяинен Т., Калево О., Регистрация и аутентификация пользователей без паролей Патент на изобретение RU 2713604 C1, 05.02.2020. Заявка № 2019106197 от 15.09.2017.
12. Жукова Г.Н. / Карта коэффициентов асимметрии и эксцесса в преподавании теории вероятностей и математической статистики. // Научно-методический электронный журнал Концепт. 2015. № 8. С. 56-60.
13. Жукова Г.Н. / Идентификация распределения по коэффициентам асимметрии и эксцесса. // Московский государственный университет печати имени Ивана Федорова.
14. Vangelista Lorenzo. Frequency Shift Chirp Modulation: The LoRa Modulation // IEEE Signal Processing Letters. 2017 Vol. 24, no. 12.Pp. 1818–1821
15. Уразбахтин А.И., Алгоритм проверки однородности выборки и ее репрезентативности исследуемому случайному процессу. / Уразбахтин А.И., Уразбахтин И.Г. // Инфокоммуникационные технологии. 2006. Т. 4. № 3. С. 10-14.
16. Tatyana I. Lapina, Time series forecasting based on data normalization methods/ Tatyana I. Lapina, Ildus G. Urazbahtin // Proceedings Volume 6277, Optical Technologies for Telecommunications 2005; 62770C (2006).

Сергеев Антон Валерьевич
ФГАО УВО
«Национальный исследовательский университет
«Высшая школа экономики»,
Московский институт электроники и математики им. А.Н. Тихонова
(МИЭМ НИУ ВШЭ)
УДК 004.056
Советник, доцент
avsergeev@hse.ru

ПОВЫШЕНИЕ ЭНЕРГОЭФФЕКТИВНОСТИ ПЕРЕДАЧИ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ МЕТОДА СТАТИСТИЧЕСКОЙ МОДУЛЯЦИИ (НА ПРИМЕРЕ QAM) В РАМКАХ КОНЦЕПЦИИ ТАКТИЛЬНОГО ИНТЕРНЕТА

Аннотация: В работе представлен новый эффективный метод совместного кодирования и модуляции, который позволяет улучшить уровень энергоэффективности и энергосбережения в современных беспроводных системах передачи. Метод требует априорного знания о законе распределения входных данных для выставление их в соответствие модуляционным символам наиболее эффективным образом.

Основная идея предлагаемого метода Статистической Модуляции состоит в том, чтобы отображать наиболее часто встречающиеся входные значения потока данных в модуляционные символы с наименьшей энергией. Для оценки величины выигрыша, мы применили данный подход к хорошо известному методу квадратурно-амплитудной модуляции (QAM).

Оценка выигрыша произведена путём моделирования передачи сигнала (MatLab) для AWGN-канала.

Ключевые слова: статистическая модуляция, энергоэффективность, QAM, СКАМ

ВВЕДЕНИЕ

Представленная в 2014 году Международным союзом электросвязи (ITU-T) концепция «Тактильного Интернета» (Tactile Internet) [1] провозгласила ключевой целью на следующие десятилетия (как минимум в перспективе до 2030 года) снижение значений задержки в процессах передачи данных в сетях связи до 1 мс.

Чтобы получить сквозную задержку от отправителя до получателя Тактильного Интернета в 1 миллисекунду и, следовательно, отклик системы в 1 миллисекунду, важно хорошо представлять цепочку (и потоки данных) между источниками данных (например, датчиками) и получателями (например, исполнительными механизмами). На Рис. 1 показан примерный бюджет времени ожидания беспроводной мобильной связи для тактильного Интернета для сценария применения типа «Индустриальный Интернет вещей (IIoT)».

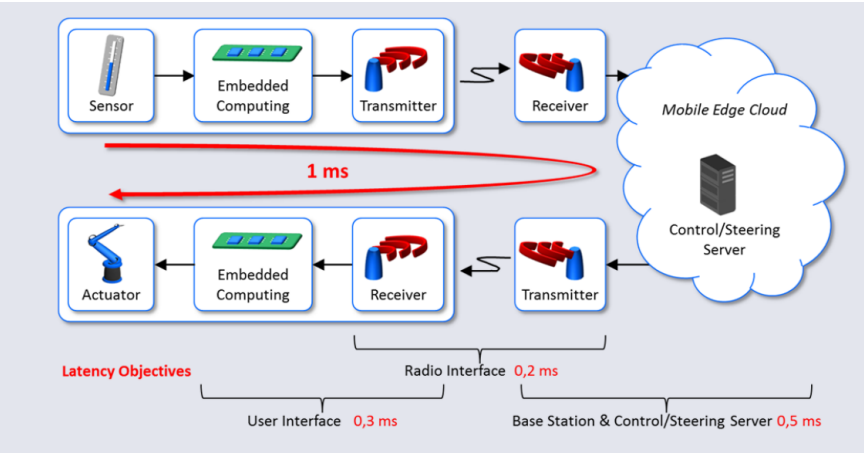


Рис. 1. Оценки задержки (пример) на разных этапах доставки данных в системах IIoT

Основной поток данных устроен следующим образом. Датчик измеряет значение технологических параметров, после данные подлежат предварительной обработки и передаются в IoT-платформу (встроенную или внешнюю систему), управляющую передающим устройством (с радиоинтерфейсом). Отметим, что передающее устройство передает данные через все протокольные уровни OSI на физический уровень, обеспечивая необходимую упаковку и обработку пакетов. То же самое происходит на принимающей стороне, например, на мобильной базовой станции с подключенным. После этого данные передаются на передаются на управляющий сервер. Именно здесь происходит управление системой и, при необходимости, принимаются управляющие решения. Чтобы получить желаемую реакцию системы, решения передаются исполнительному механизму через аналогичную цепочку обратной связи.

Существующие системы связи часто являются частью того, что обычно называют «критической инфраструктурой». Государство и общество возлагает большие надежды на системы связи, требуя, чтобы они были не только доступны и надежны, но и защищены от внешнего воздействия, обеспечивая высокий уровень безотказности. Тактильный Интернет, особенно со сверхнизкой сквозной задержкой, предъявляет дополнительно к этому серьезные требования для системы связи по времени доставки сигнала. При этом, встаёт вопрос и о выполнении криптографических процедур, а также операциях обеспечения доверия на очень высоких скоростях. Таким образом безопасность, надежность и доступность систем должны быть обеспечены одновременно.

В современных системах связи, в подавляющем большинстве случаев, процедуры обеспечения безопасности (такие как шифрование, электронная подпись, проверка ключей и сертификатов и т.п.) реализована на верхних уровнях сети. Таким образом, процедуры защиты информации отделены от процедур обеспечения надежной связи на протокольном уровне. Задача передачи данных полностью отделена от задачи обеспечения безопасности. Т.е. злоумышленник, осуществляющий перехват данных, имеет возможность успешно получить и извлечь защищенные пакеты данных, после чего приступить к атаке непосредственно на шифротект (или подпись). В свою очередь. технологии передачи отделены от шифрования и сконцентрированы исключительно в том, чтобы обеспечить высокую скорости передачи.

Чтобы тактильный Интернет обеспечивал безопасную передачу данных с очень низкой сквозной задержкой, защита связи от перехватчиков и злоумышленников должна быть встроена на нижние (на физический и MAC) уровни доступа к сети. Подходящие методы совместного кодирования гарантируют, что только законные получатели смогут обработать защищенное сообщение. Природа защищенного сообщения должна быть такова, что злоумышленник, не обладающий необходимым криптографическим секретом, не сможет декодировать сообщение уже на физическом уровне, и не получит доступ к данным в принципе.

Другой важной проблемой, с которой сталкивается Тактильный Интернет, будет идентификация и аутентификаций пользователей или, если быть точным, оконечных устройств. Существующие методы разделения аутентификации и физической передачи не обеспечивают низкую сквозную задержку, а также предоставляют злоумашленникам дополнительные возможности для планирования и реализации атак. Таким образом, реализация методов Тактильного Интернета возможна при встраивании процедур аутентификации в процессы физической передачи данных.

Исходя из вышесказанного концепция Тактильного Интернета предъявляет исключительно высокие требования к системам связи. Новые требования касаются, в основном энергоэффективности (т.к. речь идёт о встраиваемых системах с низким уровнем энергопотребления и длительным сроком автономного функционирования) и задержки (в силу требований по очень высокой скорости реакции).

Один из методов повышения энергоэффективности передачи данных, а также снижения задержки (за счет отказа от предварительной компрессии данных) представлен в следующем разделе.

УЛУЧШЕНИЕ ЭНЕРГОЭФФЕКТИВНОСТИ ПРИ ПЕРЕДАЧЕ СООБЩЕНИЯ С ИСПОЛЬЗОВАНИЕМ МЕТОДА СТАТИСТИЧЕСКОЙ МОДУЛЯЦИИ (НА ПРИМЕРЕ QAM)

В главе представлен новый эффективный метод совместного кодирования и модуляции, который позволяет улучшить уровень энергоэффективности и энергосбережения в современных беспроводных системах передачи. Метод требует априорного знания о законе распределения входных данных для выставление их в соответствие модуляционным символам наиболее эффективным образом.

Основная идея предлагаемого метода Статистической Модуляции состоит в том, чтобы отображать наиболее часто встречающиеся входные значения потока данных в модуляционные

символы с наименьшей энергией. Для оценки величины выигрыша, мы применили данный подход к хорошо известному методу квадратурно-амплитудной модуляции (QAM): наиболее часто встречающиеся входные символы были отображены в точки созвездия с меньшей энергией. В результате средняя энергия, необходимая для передачи данных, значительно снизилась, что позволяет увеличить расстояние между точками созвездия QAM при сохранении уровня средней энергии. Таким образом, достигается улучшение соотношения вероятности ошибки на бит (BER) к отношению сигнал-шум (SNR) по сравнению со стандартной квадратурной модуляцией, которая не учитывает вероятности входных символов.

В исследовании проведено сравнение новую SQAM и традиционную QAM модуляции для случая экспоненциального распределения входных символов. Наши эксперименты и теоретические вычисления показывают, что SQAM для экспоненциального входа показывает до 3 Дб выигрыш по критерию BER-SNR.

Данный подход может быть применён для улучшения соотношения BER-SNR и уменьшения энергопотребления передающей системы. Список потенциальных областей применений содержит M2M связь, приложения индустриального интернета вещей, мобильные устройства и другие сценарии, критичные к вопросам энергопотребления, времени жизни батареи и задержке передачи данных.

Квадратурно-амплитудная модуляция (КАМ)

Квадратурно-амплитудная модуляция (КАМ) – один из наиболее используемых видов модуляции для передачи данных в телекоммуникационных системах различного назначения. Основная причина – более высокий уровень спектральной эффективности по сравнению с простыми методами модуляции, например, QPSK. На практике наиболее распространены КАМ с 16 и 64 точками в созвездии [2, 3], т.н. КАМ16 (QAM16) и КАМ64 (QAM64).

Алгоритм модуляции и демодуляции КАМ можно описать следующим образом:

1. Получение значений, которые распределены по равномерному закону распределения. Значения ранжируются от 0 до $M - 1$.
2. Сопоставление точек к созвездию М-КАМ и получение сигнала, который имеет две несущие, сдвинутые по фазе на 90 градусов, модулируется, и результирующий выход состоит из амплитудных и фазовых колебаний.
3. Передача сигнала и добавление шумов.
4. Получение сигнала и декодирование созвездия методом ближайшего соседа (Используется промежуточная точка между двумя символами в качестве порога обнаружения).

Оценка средней энергии для КАМ

Рассмотрим типичную схему модуляции КАМ-16 [3] , в которой алфавит задан как

$$\alpha_{QAM16} = \begin{Bmatrix} \pm 1 \pm i & \pm 1 \pm 3i \\ \pm 3 \pm i & \pm 3 \pm 3i \end{Bmatrix}$$

Каждая точка в созвездии является символом. КАМ16 использует 16 символов.

Средняя мощность в общем стандартном созвездии М-КАМ, в котором распределение вероятностей входных значений равномерно, вычисляется следующим образом [3]:

$$E_s = \sum_{i=0}^{K-1} \sum_{j=0}^{K-2} p_{i*K+j}((2i - K + 1)^2 + (2j - K + 1)^2) \qquad (1)$$

Где $\bar{p}$ это вероятность каждого символа, и $K = \sqrt{M}$.

Рассчитаем значение средней энергии:

$$E_s = E\left[\left|\alpha_{QAM16}\right|^2\right] = E\left[Re\left|\alpha_{QAM16}\right|^2\right] + E\left[Im\left|\alpha_{QAM16}\right|^2\right] = 2E\left[R\left|\alpha_{QAM16}\right|^2\right] = \frac{2 * 2}{4}(1^2 + 3^2) = 10$$

Как видно, средняя энергия созвездия равна $E_{QAM16} = 10$.

Модель шума

Пускай полученный символ y имеет форму[2]:

$$y = k\sqrt{E_s}s + n$$

Где $k = \sqrt{\frac{1}{\frac{2}{3}(M-1)}}$ это нормирующий фактор. Значение $k = \frac{1}{\sqrt{10}}$ для $M = 16$ (КАМ-16). s это передающий символ и n это шум. Предполагается, что в канале накладывается аддитивный белый гауссовский шум, имеющий функцию плотности вероятности,

$$p(x) = \frac{1}{\sqrt{\pi\sigma^2}} e^{\frac{-x+\mu}{\sigma^2}}$$

, где $\mu = 0$ и $\sigma = \frac{N_0}{2}$.

Функция плотности вероятности для символа: $\alpha = 1 + i$

$$p(x) = \frac{1}{\sqrt{\pi\sigma^2}} e^{\frac{-x+\sqrt{\frac{E_s}{10}}}{N_0}}$$

BER-SNR

В данной работе была использована следующая функция теоретической вероятности ошибок на бит (BER) для равномерного распределения КАМ-16 [2]:

$$\mathrm{P_s} = \frac{3}{2\sqrt{\mathrm{M}}}\mathrm{erfc}\left(\sqrt{\frac{\sqrt{\mathrm{M}}\mathrm{E_b}}{10\mathrm{N_0}}}\right)$$

Где $\mathrm{erfc(x)} = \frac{2}{\sqrt{\pi}}\int_{\mathrm{x}}^{\infty} \mathrm{e}^{-\mathrm{r}^2}\mathrm{dx} = 1 - \mathrm{erf}\,(\mathrm{x})$, где $\mathrm{erf(x)}$ является функцией ошибки (также называется функцией ошибки Гаусса).

В работе изменялось отношение сигнал-шум $\frac{\mathrm{E_b}}{\mathrm{N_0}}$ и производилось моделирование передачи данных через канал с AWGN.

Статистическая модуляций SQAM

Большинство современных систем передачи данных исходят из предположения, что распределение символов данных, поступающих на вход блока модуляции, близко к равномерному распределению. Это предположение основывается, обычно, на том факте, что перед кодированием и модуляцией, передаваемые данные подвергаются пред-обработке (сжатию, шифрованию и т.п.) приводящим к «выравниванию» вероятностей символов информационного потока.

Основное вопрос работы – как изменится эффективность модуляции (на примере КАМ), если (а) предположить, что поступающие символы имеют распределение отличное от равномерно и (б) если модуляционная схема учитывает этот факт.

Важным параметром, который необходимо оценить при этом, является средняя энергия сигнала после модуляции. Ниже этот параметр оценивается для КАМ при «равномерном и экспоненциальном распределении входных символов».

Основная идея статистического КАМ (СКАМ) [4,5,6] для экспоненциального распределения состоит в том, чтобы отображать наиболее частые входные символы в точке на созвездии КАМ с наименьшей энергией передачи. В результате средняя энергия системы передачи значительно снижается, поскольку значения символов после модуляции с низкой энергией передаются более часто, чем значения с более высоким уровнем энергии. Визуализация работы схемы показано на Рис. 2.

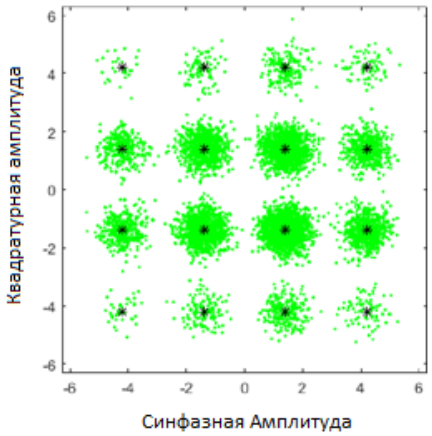


Рис. 2. Экспоненциальное распределение в статистической КАМ (SQAM) с наложенным шумом. Точки – переданные символы после передачи по зашумленному канала, звезды (*) – точки созвездия QAM. Видно, что наибольшая концентрация точек возникает у центральных символов созвездия, с минимальной энергией.

Базовые теоретические аспекты подхода были рассмотрены в работах [6, 7], отдельно от работ [4,5]. Вопросы поиска оптимального распределения входных символов для СКАМ (в общем случае) решены в [8]. В [9, 10] представлены перспективные варианты использования подхода для улучшения характеристик передачи по оптоволоконной связи.

Для корректности сравнения двух модуляционных схем (СКАМ и КАМ) необходимо выровнять среднюю энергию передачи. Средняя энергия СКАМ может быть увеличена за счет увеличения расстояния между точками в созвездии.

Используем формулу (1) для вычисления средней энергии для созвездия СКАМ-16:

$$10 = \sum_{i=0}^{K-1}\sum_{j=0}^{K-2} p_{i*K+j}(A^2(2i-K+1)^2 + A^2(2j-K+1)^2)$$

$$= A^2 \sum_{i=0}^{K-1}\sum_{j=0}^{K-2} p_{i*K+j}(A^2(2i-K+1)^2 + A^2(2j-K+1)^2)$$

Где A – коэффициент растяжения созвездия. Значение A можно получить, зная распределение вероятностей символов: $\frac{10}{\sum_{i=0}^{K-1}\sum_{j=0}^{K-2} p_{i*K+j}(A^2(2i-K+1)^2+A^2(2j-K+1)^2)}$

Эта формула зависит от вероятности каждого символа, но вероятность символов может зависеть от экспоненциального распределения, которое имеет свои характеристики. Если известно распределение, то можно высчитать коэффициент A для СКАМ.

Табл. 1. Символы для СКАМ16, энергия, бинарное представление

Входные символы	**Входные бинарные символы**	**КАМ символы**		**Энергия**
		Re	**m**	
0	0000	-1	1	2
1	0001	1	1	2
2	0010	-1	-1	2
3	0011	1	-1	2
4	0100	-1	3	10
5	0101	1	3	10
6	0110	-1	-3	10
7	0111	1	-3	10
8	1000	1	-3	10
9	1001	1	3	10
10	1010	-1	3	10
11	1011	-1	3	10
12	1100	3	3	18
13	1101	3	3	18
14	1110	-3	3	18
15	1111	-3	3	18

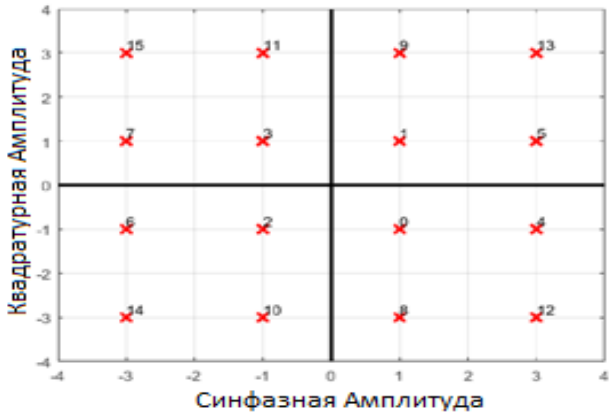


Рис. 3: Созвездие для СКАМ16

Генерация распределения

Одна из важных практических задач для верификации модели является генерация входных значений, которые распределены экспоненциально. Одной из задач в данной работе являлось генерация распределения от 0 до $M-1$.

Обратим внимание на равномерное распределение. С помощью функции обратного преобразования можно получить экспоненциальное распределение из равномерного: $-\frac{1}{\lambda}ln(U)$, где λ это характеристика экспоненциального распределения, U это равномерно распределённая величина от a до b. Запишем неравенство:

$$0 \leq -\frac{1}{\lambda}ln(U) < M$$

Упростим:

$$1 \geq U > e^{-\lambda M}$$

Отсюда можно сделать вывод, что для решения поставленной задачи необходимо генерировать равномерное распределение $U[e^{-\lambda M}, 1]$, далее пользуясь формулой перехода из равномерного получаем распределение, которое очень похоже на экспоненциальное.

Практические результаты

На вход подается распределение, выглядящее как экспоненциальное. Входное распределение показано на Рис. 4. В то же время, если значение λ окажется большим, тогда распределение напоминает равномерное, выигрыш от предложенной схемы моделирования не будет.

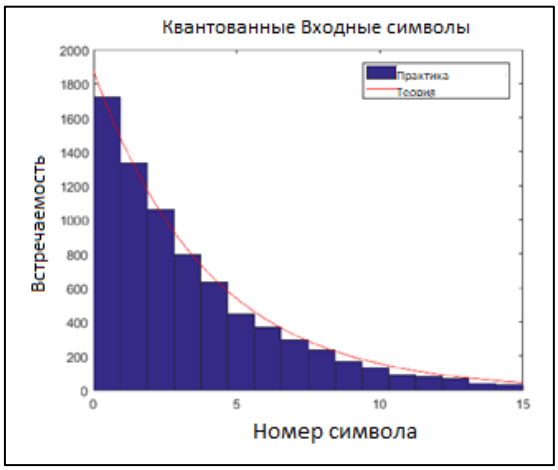


Рис. 4: Квантованные символы

Код Matlab для генерации сигнала КАМ16/СКАМ моделирует передачу по каналу. Сначала передаются значения через аддитивный белый гауссовский шум, потом производится демодуляция на приемнике, после этого подсчитывается неправильное количество переданных бит и строится кривая зависимости битовых ошибок от отношения сигнала к шуму.

Результаты показаны на Рис. 5. Графики зависимостей ошибки на бит и отношение сигнал к шуму, полученные в результате моделирования, хорошо согласуются с теоретическими формулами.

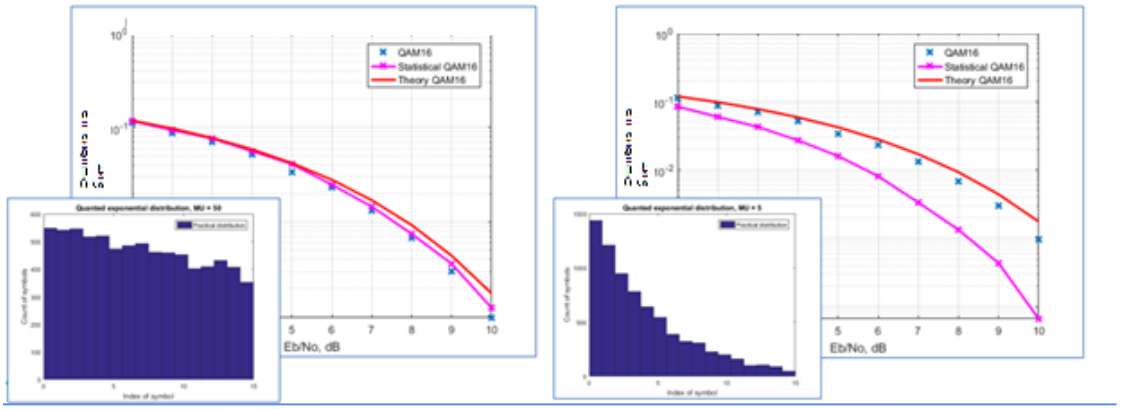


Рис. 5: Зависимость ошибки на бит и отношение сигнал-шум для разных распределений

Заключение

В разделе приведены результаты выигрыша предложенного метода статистической модуляции, учитывающей вероятности символом входного потока пао сравнению с «традиционной» схемой.

Оценка производилась для схемы квадратурно-амплитудной модуляции с 16 точками в созвездии (КАМ16) для равномерно и экспоненциально распределённых входных символов.

Оценка обеих методов (КАМ16 + равномерно-распределённые входные символы и СКАМ16 + экспоненциально распределённый вход) была произведена по критерию BER-SNR для AWGN-канала методом имитационного моделирования. Эксперименты показали, что при равных средних затратах на энергию, **выигрыш для СКАМ по скорости битовых ошибок составляет до 5 Дб**. Выигрыш достигается за счёт более частой передачи символов с низкой энергией, чем с высокой. При этом, если входной сигнал меняется на равномерный (при сохранении отображения точек СКАМ), проигрыша также не наблюдается.

СПИСОК ЛИТЕРАТУРЫ

1. The Tactile Internet, ITU-T Technology Watch Report / Geneva, 2014
2. J. R. Barry, Springer Science & Business Media / J. R. Barry, E. A. Lee, and D. G. – Springer, 3rd ed., ISBN-10: 1461349753, 855 pages, 2012.
3. Скляр Б., Цифровая связь: Теоретические основы и практическое применение / Издательский дом Вильямс, 2004.
4. A. Sergeev, Joint source coding and modulation for low-complexity video transmission / A. Sergeev, A. Turlikov, and A. Veselov - Proc. of the XII International Symposium On Problems Of Redundancy In Information And Control Systems, 2011
5. A. Sergeev, Statistical Modulation for Low-Complexity Video Transmission / A. Sergeev, A. Turlikov - Proc. of International Symposium on Wireless Personal Multimedia Communications, WPMC, 2008
6. G. D. Forney, Multidimensional constellations. Introduction, figures of merit, and generalized cross constellations / G. D. Forney, L.-F. Wei - IEEE journal on selected areas in communications, vol. 7, no. 6, pp. 877–892, 1989.
7. F. R. Kschischang and S. Pasupathy, Optimal nonuniform signaling for gaussian channels, IEEE Transactions on Information Theory, vol. 39, no. 3, pp. 913–929, 1993.
8. I. Arasaratnam, Discrete-time nonlinear filtering algorithms using gauss–hermite quadrature / I. Arasaratnam, S. Haykin, and R. J. Elliott - Proceedings of the IEEE, vol. 95, no. 5, pp. 953–977, 2007
9. T. Fehenberger, On probabilistic shaping of quadrature amplitude modulation for the nonlinear fiber channel / T. Fehenberger, A. Alvarado, G. Bocherer, and N. Hanik, - Journal of Lightwave Technology, vol. 34, no. 21, pp. 5063–5073, 2016
10. P. Poggiolini, The gn-model of fiber non-linear propagation and its applications / P. Poggiolini, G. Bosco, A. Carena, V. Curri, Y. Jiang, and F. Forghieri - Journal of lightwave technology, vol. 32, no. 4, pp. 694–721, 2014.

Симахин Е.А.
Национальный исследовательский ядерный университет «МИФИ»,
Инженер 1й категории отдела по ПДИТР и ТЗИ
EASimakhin@mephi.ru

ИССЛЕДОВАНИЕ КОМПРОМЕТИРУЮЩЕГО ИЗЛУЧЕНИЯ ИНТЕРФЕЙСОВ ПЕРЕДАЧИ ДАННЫХ LCD МОНИТОРОВ

Аннотация: При обработке информации интерфейсы передачи данных излучают информативные электромагнитные волны в окружающее их пространство. В целях обеспечения защиты информации от перехвата и последующего восстановления, специалисты в области информационной безопасности проводят исследования объектов информатизации (ОИ) на предмет побочного электромагнитного излучения (ПЭМИ) интерфейсов передачи данных. С учетом сложности и, как следствие, больших временных затрат, выполнение такого вида работ требует не только квалифицированных специалистов, но и обеспечение автоматизации технического процесса. В данном докладе представлены основные положения проводимого исследования, автоматизированный метод определения эффективной ширины спектра информативных широкополосных сигналов жидкокристаллических (ЖК) мониторов, краткое описание комплекса обнаружения и измерения ПЭМИ, содержащего разработанный метод. Также при проведении исследования компонентов архитектуры интерфейса DisplayPort, влияющих на распределение энергии ПЭМИ в спектре, определено, что помехоустойчивость линий основного канала зависит от настроек конфигурации интерфейса DisplayPort – DPCD. Такая зависимость обуславливает возможность изменения конфигурации программными средствами и таким образом позволяет существенно влиять на качество проведения инструментальных испытаний по оценке защищенности обрабатываемой информации. По результатам исследования предложены порядок анализа необходимой информации для применения подходов и порядок применения инструментальных действий при подготовке к лабораторным исследованиям высокоскоростного интерфейса передачи данных DisplayPort.

Ключевые слова: информационная безопасность, побочное электромагнитное излучение, жидкокристаллический монитор.

1. Актуальность темы исследования

При больших временных затратах, требуемых для анализа, отсутствие методов обнаружения информативных частот, определения эффективной ширины спектра, измерения мощности сигналов интерфейсов передачи данных, их автоматизации и средств анализа приводит к ограничениям или запрету в эксплуатации, в частности, для внутренних дифференциальных интерфейсов современных ЖК мониторов и интерфейса DisplayPort. Также, это приводит к неточностям или ошибкам при расчете зон разведдоступности, в пределах которых возможен перехват средством разведки ПЭМИ с требуемым качеством, и, как следствие, при формировании системы защиты ОИ.

Для преодоления данных недостатков требуется разработать методы и средства анализа ПЭМИ интерфейсов передачи данных ЖК мониторов, повышающие точность и полноту их результатов при уменьшении трудозатрат на проведение аттестационных испытании ОИ.

2. Степень разработанности темы

Научное сообщество ведет активную работу в направлении защиты информации от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН). Так, отечественные ученые предлагают методы применения защиты от утечки за счет ПЭМИ [1], [2], например, способ программной защиты изображения монитора от утечки за счет ПЭМИ, основанный на программной псевдослучайной перестройке рабочей частоты следования кадров дисплея [2]. Исследуется возможность уменьшения зоны разведдоступности за счет методов экранирования [3], [4]. Разрабатываются методы оценки возможности перехвата полезного сигнала [5-7]. Так, для восстановления информации за счет ПЭМИ видеотракта с требуемым качеством авторы [6] использовали программируемую логическую интегральную схему, не предназначенную для такого вида работ, и специализированный пакет программного обеспечения.

В работах [8-13] обсуждается методология формирования технического канала ПЭМИН и моделирование угроз безопасности информации относительно элементов технических средств ОИ, в частности ЖК мониторов. Исследуется распространение ПЭМИ устройств автоматизированных рабочих мест [9], возможности злоумышленника [10]. Предлагается методика оценки коэффициентов ослабления уровней ПЭМИ [11]. Авторы [12] представили методику оценки рисков при

функционировании вредоносных программных средств, предложена схема формирования комплекса защитных мер и определена формула расчета величины, показывающей степень значимости возникающего ущерба. Вместе с этим разрабатываются программно-аппаратные комплексы и полезные модели обнаружения, измерения и анализа ПЭМИ интерфейсов передачи данных [13], [14], позволяющие автоматизировать процессы специальных исследований. Проводятся исследования канала утечки информации за счет ПЭМИН, формируемого при помощи Soft Tempest – специализированного программного обеспечения, воздействующего на интерфейсы передачи данных [15], [16].

Зарубежные коллеги также проводят исследования в данном направлении, особенно в части методов восстановления информации не только в теоретических аспектах моделирующих критические условия эксплуатации, но и в реальных условиях эксплуатации [17], [18]. Работы, касающиеся возможности и примеров восстановления информации, в основном направлены на изучение интерфейсов передачи данных современных устройств, компонентом которых является ЖК дисплей [19-21]. Также исследователи предлагают методы анализа ПЭМИ в области противодействия и защиты информации [22-24]. Например, в [23] авторами анализируется степень защищенности от утечки за счет ПЭМИН, которой должно удовлетворять помещение с компьютерной инфраструктурой соответствующей требованиям стандарта CISPR22 EMC «Оборудование информационных технологий. Характеристики радиопомех. Пределы и методы измерения».

Из проведенного анализа видно, что наиболее интересующим научное сообщество средством вычислительной техники (СВТ) является современный ЖК монитор. Основной причиной этого является высокая степень возможности восстановления информации относительно других интерфейсов передачи данных. Совокупность исследований по данной тематике и наличие неконтролируемого распространения информативного сигнала от ЖК монитора через физическую среду до технического средства, осуществляющего перехват информации, подтверждают актуальность реализации и разработки методов защиты информации от утечки по каналу ПЭМИН.

3. Цель и задачи работы

Цель исследования – разработка методов и средств анализа ПЭМИ интерфейсов передачи данных ЖК мониторов.

Для достижения поставленной цели необходимо:

1. Разработать автоматизированный метод оценки эффективной ширины спектра широкополосных сигналов ПЭМИ в частности внутренних интерфейсов ЖК монитора;
2. Разработать автоматизированный комплекс обнаружения и измерения ПЭМИ СВТ включающий автоматизированный метод анализа побочных электромагнитных излучений широкополосных сигналов;
3. Провести анализ архитектуры интерфейса передачи данных DisplayPort;
4. Сформировать рекомендации к оценке ПЭМИ для интерфейса DisplayPort.

4. Научная новизна

Научная новизна заключается в:

- Разработке метода определения эффективной ширины спектра информативных широкополосных сигналов, в частности внутренних интерфейсов ЖК монитора;
- Разработке автоматизированного комплекса обнаружения и измерения энергетических характеристик побочных электромагнитных излучений интерфейсов передачи данных СВТ, включающий автоматизированный метод анализа побочных электромагнитных излучений широкополосных сигналов;
- Обоснованных рекомендациях к оценке ПЭМИ высокоскоростного интерфейса передачи данных DisplayPort.

5. Теоретическая и практическая значимость работы

Теоретическая значимость работы состоит в развитии методов анализа обнаружения ПЭМИ интерфейсов передачи данных ЖК мониторов.

Практическую значимость работы заключается в применении разработанного комплекса обнаружения и измерения энергетических характеристик побочных электромагнитных излучений интерфейсов передачи данных СВТ, включающий автоматизированный метод анализа побочных электромагнитных излучений широкополосных интерфейсов LVDS и RSDS, а также рекомендациях для анализа побочных электромагнитных излучений высокоскоростного интерфейса передачи данных DisplayPort.

6. Методология и методы исследования

Теоретическая и методологическая база основывалась на современных трудах, публикуемых научными изданиями в области защиты информации от утечки за счет побочных электромагнитных излучений и наводок. Требования к измерительным комплексам и методу автоматизации обнаружения, предложенные в работе, исследовались путем анализа архитектуры ЖК мониторов и способов передачи видеоинформации. Производились математические расчеты для корректного построения алгоритма взаимодействия с измерительным оборудованием и последующее тестирование разработанной методики на реальном объекте информатизации. Для решения поставленных задач применялся математический аппарат теории вероятности, математического анализа, теории множеств.

7. Положения, выносимые на защиту

На защиту выносятся следующие положения:

1) метод определения эффективной ширины спектра информативных широкополосных сигналов;

2) программная реализация комплекса обнаружения и измерения побочных электромагнитных излучений и наводок;

3) рекомендации к анализу побочных электромагнитных излучений высокоскоростного интерфейса передачи данных DisplayPort.

8. Степень достоверности и апробация результатов

Все результаты работы докладывались на следующих конференциях и семинарах:

1) 2-nd Scientific Conference on Fundamental Information Security Problems in terms of the Digital Transformation (FISP-2020);

2) 2021 International Siberian Conference on Control and Communications (SIBCON);

3) 2021 IEEE 32nd International Conference on Microelectronics (MIEL);

4) Белорусско-российская научно-техническая конференция «Технические средства защиты информации», 2021;

5) Белорусско-российская научно-техническая конференция «Технические средства защиты информации», 2022;

6) Международный московский IEEE-семинар по электронным и сетевым технологиям (MWENT-2022).

9. Краткое содержание диссертации с упором на результаты, полученные за период реализации научного проекта в рамках гранта

9.1 Метод определения эффективной ширины спектра информативных широкополосных сигналов

Для определения эффективной ширины спектра широкополосного сигнала первоначально требуется измерить значения мощности и соответствующих частот во всем исследуемом диапазоне частот. Для этого в каждой полосе обзора на этапе обнаружения вычисляется среднеквадратичное отклонение значения мощности P_σ, детектор трассы пиковый (MAX). После измерения из массива полученных данных $[f_i, P_i]$, выделяются подмассивы $[f_j, P_j]$ такие, что для каждого элемента подмассива значение мощности превышает значение P_σ. Значению полосы обнаруженных сигналов ΔF присваивается значение равное разности максимальной и минимальной частот в каждом подмассиве.

Исходя из практических результатов анализа эффективной ширины спектра информативных широкополосных сигналов ручным методом полоса сигнала, как правило, намного больше требуемой полосы пропускания фильтра промежуточной частоты. Таким образом, во входных данных искомому сигналу соответствует некоторое множество значений частот. В том случае, если исследователю не известны параметры передаваемого сигнала, то объективный критерий объединения полученных значений и их соответствия искомому сигналу отсутствует. В целях уменьшения количества полученных значений удовлетворяющих условиям первичного отбора применяется операция минимизации количества частот. Алгоритм минимизации заключается в следующем:

1) исходя из формы огибающей искомых информативных широкополосных сигналов ЖК мониторов, полученной путем применения в модулирующем преобразовании функций Бесселя, изначально требуется минимизировать разрывы между компонентами искомого сигнала. В связи с тем, что на этапе обнаружения полезного сигнала нет необходимости точного определения его энергетических характеристик, то для объедения разрывов можно использовать фильтрацию скользящего среднего с задержкой фильтра либо использовать встроенную в анализатор спектра и

сигналов функцию «Smoothing», принимающей на вход процент сглаживания. Опытным путем было установлено, что корректное объединение с полосой фильтра промежуточной частоты равной 120 кГц возможно в диапазоне от 1% до 1,5% сглаживания. При меньших значениях эффект сглаживания не дает требуемого результата. При больших значениях искомые сигналы на высоких частотах полностью смешиваются с индустриальными шумами;

2) далее для каждой полосы обзора рассчитывается константное значение частотного расстояния между двумя точками измерения численно равное выражению $\Delta F_{SPAN} / SWP$,

где ΔF_{SPAN} - ширина полосы обзора, Гц;

SWP - количество точек измерения в одной полосе обзора;

3) далее итеративно для значений f_j каждой полосы обзора, начиная с первой частоты, рассчитывается разница между первоначальной частотой и последующей. Если выражение $\left\lceil (f_{j+1} - f_j) / (\Delta F_{SPAN} / SWP) - 1 \right\rceil$ равно нулю, то это значит, что частоты находятся рядом и принадлежат одному сигналу, если же не равно нулю, то частоты не принадлежат одному сигналу. Сравнение для каждого сигнала проводится до момента, пока результат алгоритма не будет равен нулю. В тот момент, когда нашлась такая частота, определяется значение полосы широкополосного сигнала.

9.2 Программная реализация комплекса обнаружения и измерения побочных электромагнитных излучений и наводок

С технической точки зрения, задача анализа ПЭМИ требует реализации двух алгоритмов:

1) обнаружение информативных частот интерфейсов передачи данных;

2) измерение мощности сигнала и индустриальных шумов на обнаруженных частотах.

Реализация алгоритма обнаружения является наиболее важной задачей, поскольку любая ошибка при обнаружении частот делает этап измерений полностью неприменимым для проведения дальнейшего анализа (Рис.1).

Рис.1. Основные задачи анализа ПЭМИ

Тем не менее, для удобства пользования и переносимости, полученных при анализе данных, комплексу необходимо обладать следующим функциональными и нефункциональными характеристиками:

1) обеспечение взаимодействия с файловой системой;

2) удобство графического интерфейса;

3) детектирование изменения электромагнитного поля в реальном времени;

4) настройка основных параметров приема оборудования.

В соответствии со схемой представленной на рисунке 1, и установленными требованиями функциональная схема управляющей программы должна иметь структуру, представленную на рисунке 2 (Рис.2).

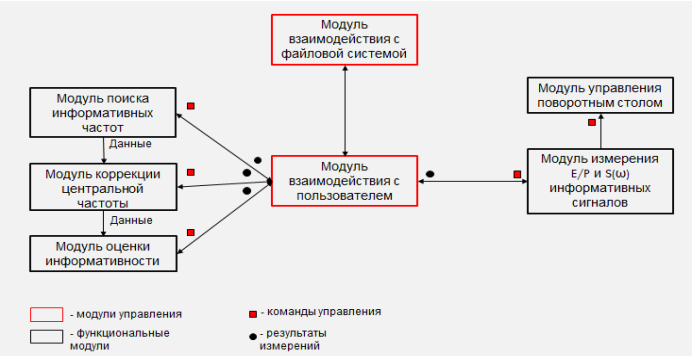


Рис. 2. Функциональная схема управляющей программы

Основным компонентом управляющей программы является модуль взаимодействия с пользователем, позволяющий оператору комплекса в реальном времени отслеживать измеряемые энергетические характеристики интерфейсов передачи данных и тем самым проводить анализ ПЭМИ (Рис. 3). Анализ проводится в автоматическом и ручном режимах.

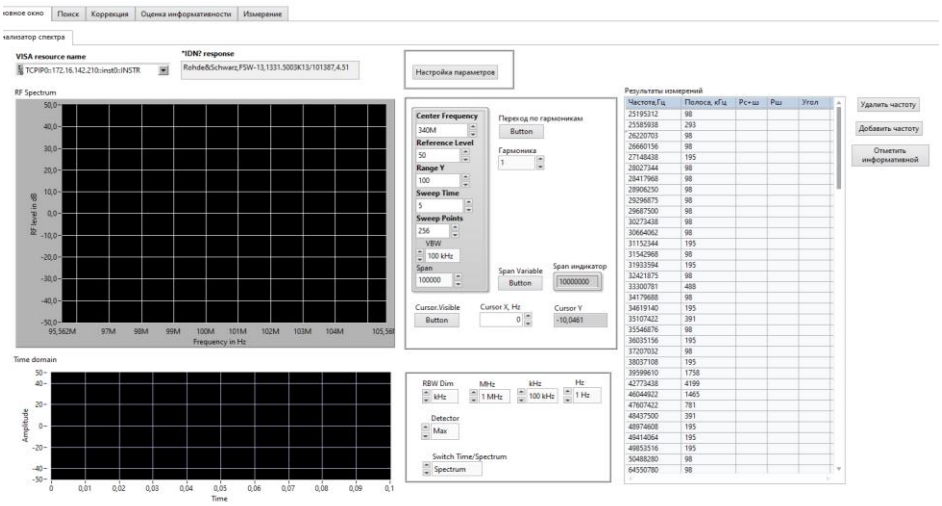


Рис. 3. Модуль взаимодействия с пользователем

Также, данный модуль обладает следующим функционалом:

1) автоматическое определение используемого измерительного оборудования;

2) взаимодействие с настройкой основных параметров измерительного комплекса;

3) возможность быстрого анализа ПЭМИ СВТ с помощью прохода по частотам гармоник исследуемых интерфейсов передачи данных;

4) установление маркера на максимальное значение напряженности/мощности сигнала в полосе обзора;

5) просмотр и редактирование полученных значений после проведения последней операции, а также итеративно на каждом шаге;

6) переход между операциями этапов обнаружения и измерения.

В целях переносимости результатов проведённой работы с комплексом реализована модель взаимодействия оператора с файловой системой операционной системы (Рис. 4) следующим образом:

1) реализована возможность сохранения проекта в целом с созданием отдельных директорий с наименованием по умолчанию «Измерения №»;

2) реализованы возможности открытия/закрытия проекта исследований;

3) реализована возможность открытия нового проекта измерения с учетом сохранения старого по решению оператора комплекса.

В основной директории проектов с проведенными измерениями дополнительно хранится файл настроек анализатора спектра и сигналов, выставленных по умолчанию – «default.txt». Данный файл необходим для первоначального запуска измерительного оборудования или аварийного останова вследствие непредвиденной программной или аппаратной ошибки, совершенной не по вине оператора комплекса.

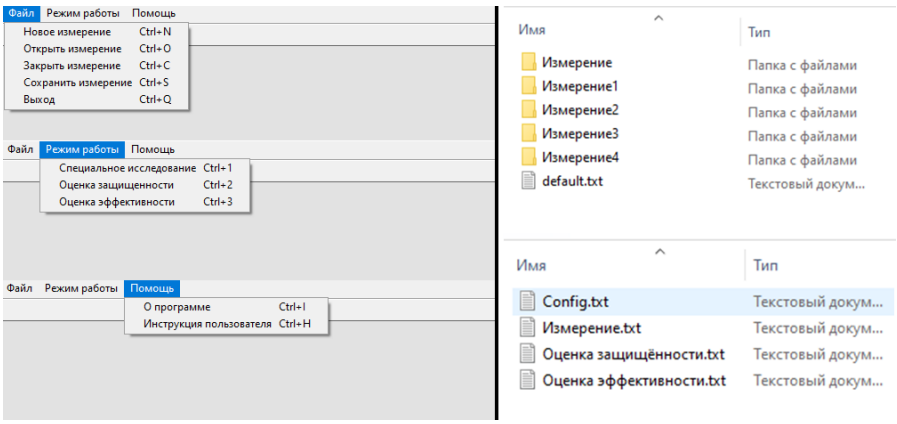


Рис. 4. Работа с файловой системой

Дополнительно реализована защита от некорректной настройки входных параметров для работы измерительного оборудования по всем настраиваемым параметрам.

9.2.1 Обнаружение информативных частот

Базовый принцип обнаружения информативных частот сигналов ПЭМИ состоит из следующих этапов:

1) первоначальный поиск возможных частот информативных сигналов;

2) уточнение центральных частот информативных сигналов (только для узкополосных сигналов);

3) отсеивание неинформативных частот.

Основной задачей этапа поиска является подготовка первичного списка частот, удовлетворяющих критериям отсева, и соответствующих им значений мощности для их дальнейшей обработки (Рис. 5). В случае широкополосных сигналов добавляется значение эффективной ширины спектра. Для решения этой задачи используется поиск относительно некоторой константной величины: порогового значения и шумовой обстановки. Также оператору доступно формирование собственного списка частот вручную.

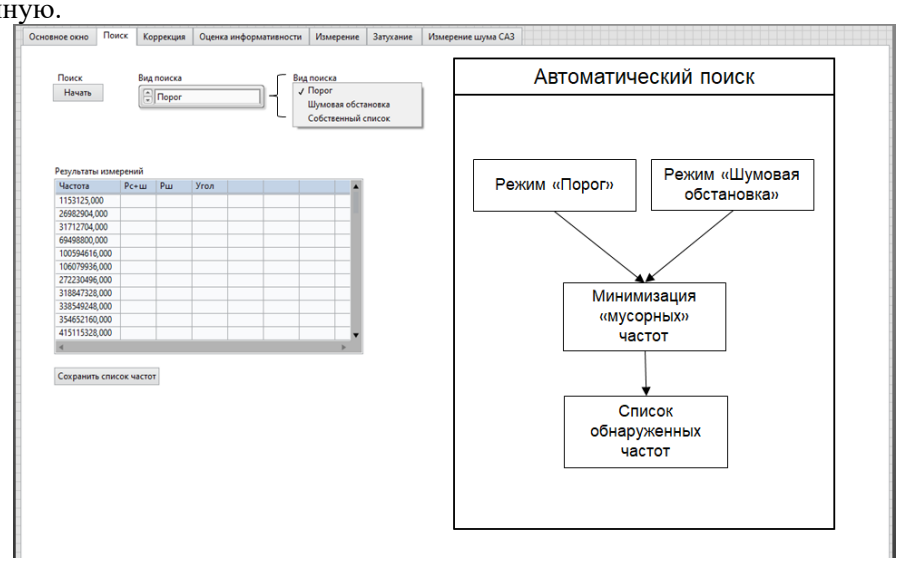


Рис. 5. Окно и общий алгоритм поиска

Алгоритм относительно порогового значения работает следующим образом:

1) уровень порогового значения определяется как совокупность среднего значения мощности электромагнитного шума в полосе обзора и константного значения, установленного оператором. Программный комплекс проводит обработку данных и отсекает все частоты, соответствующая мощность которых не превышает константное значение мощности на этой же частоте;

2) алгоритм выполняется итеративно для каждой полосы обзора в исследуемом диапазоне частот.

Алгоритм относительно шумовой обстановки работает следующим образом:

1) оператором устанавливаются базовые настройки для проведения поиска сигналов;

2) проводятся два последовательных измерения без включенного СВТ и с включенным тестовым сигналом на исследуемый интерфейс;

3) далее итеративно для каждой полосы обзора вычитаются мощности на одинаковых частотах из двух измеренных массивов. В том случае, если разница превышает 3 дБ, то записываем его в список. Данное допущение необходимо, чтобы не учитывать при формировании первичного списка частот частоты, принадлежащие индустриальному шуму.

Ввиду того, что при использовании таких методов появляется большое количество точек измерения в каждой полосе, то в комплексе реализована операция минимизации количества частот, описанная в пункте 9.1. Дополнительно, для поиска частот информативных узкополосных сигналов предварительно определяется центральная частота каждого обнаруженного сигнала.

Алгоритм формирования собственного списка состоит в следующем:

1) оператором начальная частота F_0 большая минимальной частоты $F_{\min}$ и шаг по частоте $step$;

2) далее сформируется список частот, при условии, что последняя частота не превышает максимальную частоту $F_{\max}$.

9.2.2 Коррекция центральных частот сигналов

Несмотря на использование операции минимизации, это не решает задачу определения центральной частоты сигналов. Для точного определения используется операция коррекции центральных частот, алгоритм которой работает следующим образом:

1) исходя из определённой на этапе поиска полосы сигнала ΔF выбирается ширина полосы обзора, превышающая максимальную полосу в 2 раза;

2) в целях достижения точности измерений устанавливается полоса фильтра RBW с меньше полосой пропускания, чем при поиске сигналов;

3) далее проводится уточнение по имеющемуся списку частот.

Общий вид окна программы при операции коррекции, алгоритм и пример результата представлен на рисунке 6 (Рис. 6).

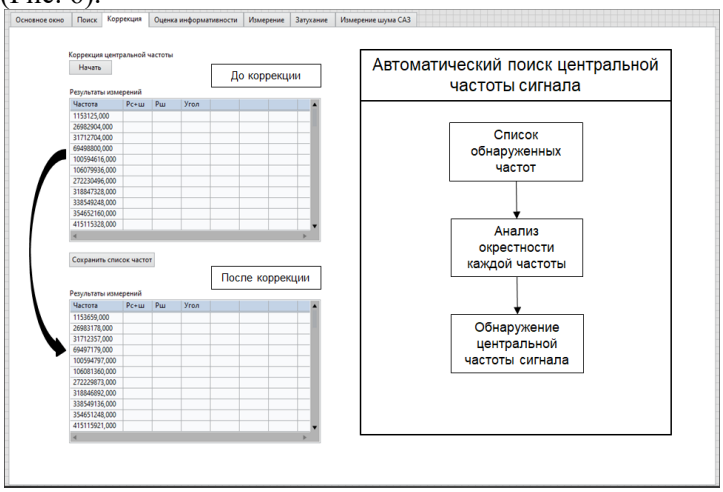


Рис. 6. Окно и общий алгоритм оценки информативности

9.2.3 Отсеивание неинформативных частот

Проверка информативности обнаруженных частот сигналов предназначена для удаления просочившихся неинформативных частот путём либо вычисления коэффициента корреляции по Критерию Пирсона относительно формы огибающей информативного сигнала либо по энергетической составляющей, что представлено на рисунке 7 (Рис.7).

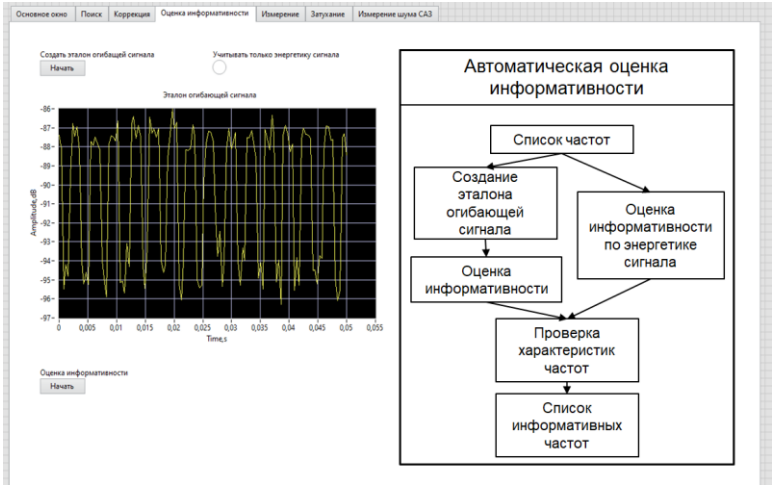


Рис.7. Окно и общий алгоритм оценки информативности

Алгоритм, учитывающий форму огибающей информативного сигнала оценивается следующим образом:

1) с помощью встроенной в драйвер оборудования функций проводим оценку огибающей спектра во временной области. Поскольку синусоидальный сигнал можно представить в виде вещественной и мнимой частей, связанных между собой преобразование Гильберта, то для выделения модуля комплексной функции приведем ее к полярному виду. Модуль полярной функции соответствует значению мощности в точке принадлежащей огибающей спектра сигнала;

2) далее по всем частот, полученным после операции коррекции центральных частот проводим проверку на информативность с помощью вычисления коэффициента корреляции по Критерию Пирсона относительно формы огибающей информативного сигнала.

Алгоритм, учитывающий энергетику сигнала аналогичен методу поиска информативных сигналов относительно шумовой обстановки.

В целях проверки достоверности результатов используется критерий кратности информативных частот. Для этого устанавливается номер гармоники n для первой частоты $F_{ТАКТОВАЯ}$ и максимальная ошибка по частоте равная половине полосы фильтра RBW взятого при коррекции. Если все частоты попадают в диапазон $F_{ТАКТОВАЯ} * n \pm (\Delta F_{RBW} / 2)$, то оценка информативности выполнена корректно. В противном случае, требуется дополнительный анализ оператора.

9.2.4 Измерение энергетических характеристик сигнала

Задача измерения на обнаруженных частотах проводится в 2 этапа:

1) проведение измерения мощности индустриальных шумов;

2) проведение измерения максимальной мощности сигнала.

Для определения максимального уровня мощности сигнала используется дополнительный анализ диаграммы направленности с помощью поворотного стола. Общий вид окна программы при операции измерения и пример результата представлен на рисунке 8 (Рис. 8).

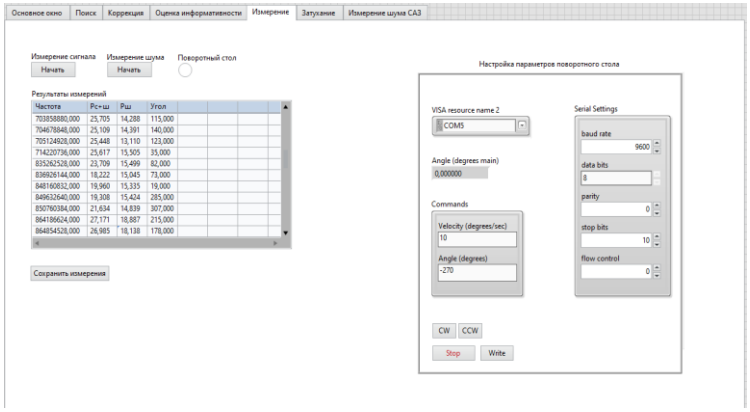


Рис. 8. Окно программы при операции измерения

9.3 Анализ архитектуры интерфейса DisplayPort

В рамках проекта проанализированы компоненты архитектуры интерфейса DisplayPort, характеристики среды распространения сигнала от источника к приемнику и алгоритм формирования транспортных блоков данных. При проведении исследования компонентов архитектуры интерфейса, влияющих на распределение энергии ПЭМИ в спектре, определено, что помехоустойчивость линий основного канала зависит от настроек конфигурации интерфейса DisplayPort – DPCD. С учетом наличия управляющих команд в открытом доступе установлено, что программными средствами возможно изменить конфигурацию и таким образом существенно влиять на качество проведения инструментальных испытаний по оценке защищенности обрабатываемой информации. По результатам исследования предложен порядок анализа необходимой информации для применения подходов и разработан порядок применения инструментальных действий при подготовке к лабораторным исследованиям (Рис. 9) и (Рис.10).

Рис. 9. Порядок анализа необходимой информации

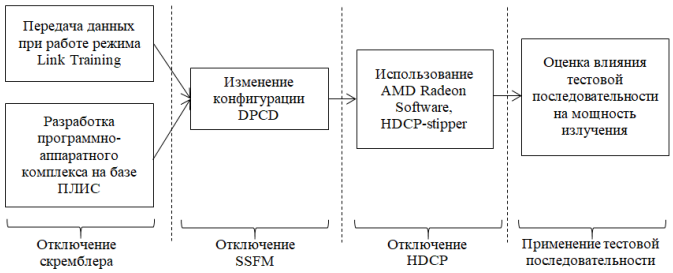


Рис.10. Последовательность применения инструментальных действий

10. Рекомендации и перспективы дальнейшей разработки темы.

Дальнейшее исследование анализа ПЭМИ интерфейсов передачи данных СВТ следует проводить в направлении разработки программ, реализующих формирование тестовых последовательностей для различных вариаций конфигураций исследуемых интерфейсов. Например, как показало исследование алгоритма работы интерфейса DisplayPort, в зависимости от количества активных линий и количества бит на один пиксель меняется количество информации передаваемое за единицу времени, что указывает на разнообразие тестовых режимов работы ЖК монитора. Также актуальной является задача формирования тестовой последовательности для интерфейсов DVI и HDMI различных версий – в данный момент различными программными средствами обеспечивается тест на половину (4 бит / 5 бит) передаваемого блока данных.

СПИСОК ЛИТЕРАТУРЫ

1. Дворников С. В. Методы предотвращения утечки информации из контролируемых помещений за счет побочных электромагнитных излучений и наводок / С. В. Дворников // Интеграция наук. – 2018. – № 7(22). – С. 134-136.
2. Авдеев В.Б. Способ программной защиты видеодисплейной информации от перехвата по каналу побочных электромагнитных излучений / В. Б. Авдеев, Д. В. Асотов, Н. Г. Денисенко, А. Н. Катруша // Телекоммуникации. – 2014. – № 1. – С. 19-22.
3. Петигин А.Ф. Применение радиоэкранирующих тканей для защиты информации от утечки за счёт побочных электромагнитных излучений // REDS: Телекоммуникационные устройства и системы. - 2015. -№5, том. 4. – С. 428-431.
4. Орлова Е. А. Ослабление побочных электромагнитных излучений ПЭВМ / Е. А. Орлова // Актуальные научные исследования в современном мире. – 2021. – № 6-6(74). – С. 80-84.
5. Хорев. А.А. Оценка возможности обнаружения побочных электромагнитных излучений видеосистемы компьютера / А.А. Хорев // Специальная техника. – 2011 – № 1. – С. 47-49.
6. Иванов А.В. Применение технологии SDR (Software Defined Radio) для восстановления сигналов побочных электромагнитных излучений видеотракта / А. В. Иванов, И. А. Огнев, Е. Е. Никитина, Л. В. Меркулов // Безопасность цифровых технологий. – 2021. – № 4(103). – С. 72-90. – DOI 10.17212/2782-2230-2021-4-72-90.
7. Хорев А. А. Побочные электромагнитные излучения видеосистем средств вычислительной техники / А. А. Хорев // Защита информации. Инсайд. – 2014. – № 1(55). – С. 52-59.
8. Авсентьев О. С. Исследование условий возникновения технических каналов утечки информации по побочным электромагнитным излучениям на объектах информатизации / О. С. Авсентьев, А. О. Авсентьев, А. Г. Вальде // Вестник Воронежского института МВД России. – 2017. – № 3. – С. 22-31.
9. Антипов Д. А. Исследование направленности побочного электромагнитного излучения от персонального компьютера / Д. А. Антипов, А. А. Шелупанов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2018. – Т. 21. – № 2. – С. 33-37. – DOI 10.21293/1818-0442-2018-21-2-33-37.
10. Авсентьев, О. С. Имитационная модель канала утечки информации по побочным электромагнитным излучениям объектов информатизации органов внутренних дел / О. С. Авсентьев, А. Г. Кругов // Охрана, безопасность, связь. – 2017. – № 1-2. – С. 13-19.
11. Авдеев В. Б. Мажорирующая оценка коэффициентов ослабления уровней побочных электромагнитных излучений технических средств / В. Б. Авдеев, А. Н. Катруша // Спецтехника и связь. – 2013. – № 5. – С. 36-41.
12. Белоножкин В. И. Методика оценки и регулирования рисков при функционировании программных средств, формирующих технический канал утечки информации за счет

программно управляемых побочных электромагнитных излучений / В. И. Белоножкин, Ю. А. Дергачев, А. С. Турчин // Информация и безопасность. – 2020. – Т. 23. – № 1. – С. 51-66.
13. Kagin I. I. Development of a Software Package for the Analysis of Compromising Emanation Using LabVIEW / I.I. Kagin, E.A. Simakhin, S.G. Arabian, L.N. Kessarinskiy, A.P. Durakovskiy // 2021 International Siberian Conference on Control and Communications (SIBCON) – 2021 – С. 1-5 – DOI: 10.1109/SIBCON50419.2021.9438939.
14. Марков В. П. Автоматизированный комплекс для определения величины затухания сигнала / В. П. Марков, А. В. Данеев // Информационные технологии и математическое моделирование в управлении сложными системами. – 2020. – № 2(7). – С. 46-55. – DOI 10.26731/2658-3704.2020.2(7).46-55.
15. Скрыль С.В. Технология Soft Tempest как объект функционального моделирования / С. В. Скрыль, Е. В. Вайц, С. С. Никулин // Безопасность информационных технологий. – 2022. – Т. 29. – № 1. – С. 125-144. – DOI 10.26583/bit.2022.1.11.
16. Яресько А. П. Канал утечки информации по каналу, образуемый Soft Tempest или мягкий ПЭМИН / А. П. Яресько, А. Н. Соколов // Безопасность информационного пространства: Сборник материалов XV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых – 2016. – С. 250-252.
17. Lee H. S. Information Recovery Using Electromagnetic Emanations From Display Devices Under Realistic Environment / H. S. Lee, D. H. Choi, K. Sim and J. Yook // IEEE Transactions on Electromagnetic Compatibility – 2019. – vol. 61, no. 4 – С. 1098-1106 – DOI: 10.1109/TEMC.2018.2855448.
18. Efendioglu H. S. Identification of Computer Displays Through Their Electromagnetic Emissions Using Support Vector Machines / H. S. Efendioglu, U. Asik, C. Karadeniz // International Conference on INnovations in Intelligent SysTems and Applications (INISTA) – 2020 – С. 1-5 – DOI: 10.1109/INISTA49547.2020.9194634.
19. De Meulemeester P. Reconstructing Video Images in Color Exploiting Compromising Video Emanations / P. De Meulemeester, B. Scheers, G. A. E. Vandenbosch // Proceedings International Symposium on Electromagnetic Compatibility – 2020, – С. 1-6 – DOI: 10.1109/EMCEUROPE48519.2020.9245775.
20. Lee H. S. An information recovery technique from radiated electromagnetic fields from display devices / H. S. Lee, D. H. Choi, K. Sim and J. Yook // Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC) – 2016. – С. 473-475 – DOI: 10.1109/APEMC.2016.7522772.
21. De Meulemeester P. Quantitative Approach to Eavesdrop Video Display Systems Exploiting Multiple Electromagnetic Leakage Channels / P. De Meulemeester, B. Scheers, G. A. E. Vandenbosch // IEEE Transactions on Electromagnetic Compatibility – 2020 – vol. 62, no. 3 – С. 663-672 – DOI: 10.1109/TEMC.2019.2923026.
22. Galvis J. Denoising of Video Frames Resulting From Video Interface Leakage Using Deep Learning for Efficient Optical Character Recognition / J. Galvis, S. Morales, C. Kasmi, F. Vega // IEEE Letters on Electromagnetic Compatibility Practice and Applications – 2021 – vol. 3, no. 2 –С. 82-86. – DOI: 10.1109/LEMCPA.2021.3073663.
23. Popescu M. Estimate of minimum attenuation level for a TEMPEST shielded enclosure / Popescu, V. Bîndar, R. Craciunescu, O. Fratu // 2016 International Conference on Communications (COMM) – 2016 – С. 513-518 – DOI: 10.1109/ICComm.2016.7528278.
24. Bergsma H. Using an in-line uninterruptable power supply as TEMPEST ‘filter’ for naval vessels," 2015 IEEE International Symposium on Electromagnetic Compatibility (EMC) – 2015 – С. 1106-1110 – DOI: 10.1109/ISEMC.2015.7256323.

Смирнов С.И.
МИРЭА – Российский технологический университет, аспирант
smirnov_si@mirea.ru

МЕТОДИКА ПРОВЕДЕНИЯ РАССЛЕДОВАНИЯ КИБЕРИНЦИДЕНТА НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА СОБЫТИЙ БЕЗОПАСНОСТИ ДОМЕНА

Аннотация: В статье обоснована актуальность в необходимости создания методики, направленной на проведение расследования кибератак современности. Сформулированы основные понятия в области расследования киберинцидента, а также описаны этапы методики на основе интеллектуального анализа событий безопасности домена. Методика позволяет качественно выявлять вредоносные действия злоумышленника, который применяет современные техники и инструменты при горизонтальном перемещении в домене.
Ключевые слова: киберинцидент, целевая таргетированная атака, информационная система, расследование инцидента информационной безопасности, горизонтальное перемещение в домене.

1. Введение

Последние геополитические события серьезно переформатировали IT-отрасль. С конца февраля этого года российские организации подвергаются беспрецедентным по своему размаху и интенсивности кибератакам. Нынешняя ситуация требует незамедлительной реакции и приведения информационных систем (ИС) в режим усиленной защиты.

Практика реагирования на современные инциденты информационной безопасности (ИБ) показывает, что за последнее десятилетие количество техник и инструментов, которые используют злоумышленники при целевых атаках на ИС организаций, ежедневно увеличивается [1].

Согласно отчету компании Positive Technologies [2] шифровальщики остаются самым популярным вредоносным программным обеспечением, среди которых можно выделить Avaddon, AvosLocker, Babuk, Conti (Ryuk), DoppelPaymer, REvil. Они были использованы в шести из каждых десяти кибератак на организации. Помимо кражи информации, атаки вымогателей приводили к сбоям в работе государственных IT-систем.

Как показывает практика расследований киберинцидентов, злоумышленник с большей долей вероятности может быть обнаружен на этапе горизонтального перемещения в сети [3]. В настоящее время в области обнаружения компьютерных атак преобладают методы на основе сигнатурного анализа признаков атаки.

Примеры программных инструментов, используемые современными злоумышленниками на каждом этапе целевой атаки (согласно матрице MITRE ATT&CK [4]), представлены из отчета [5] (Рис. 1).

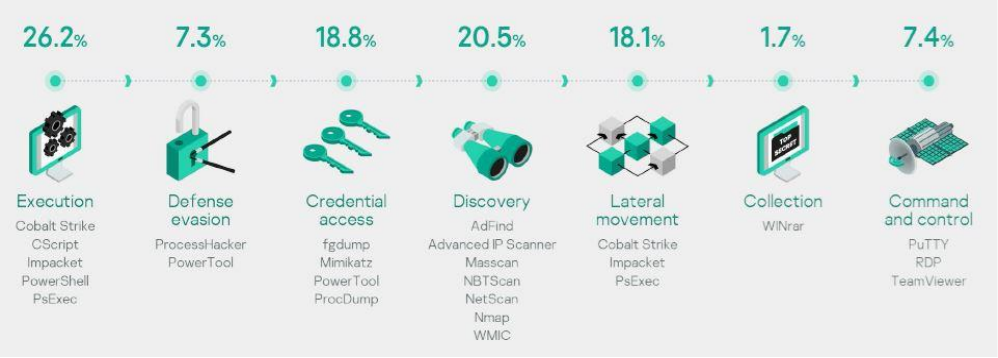


Рис. 1. Примеры программных инструментов, используемые злоумышленниками в настоящее время

Процесс проведения расследования киберинцидента рассмотрен в виде двух циклов (Рис. 2). Первый – это обнаружение следов злоумышленника и его дальнейшее сдерживание, а также восстановление работоспособности ИС. Второй цикл – это рекомендации и выводы, полученные специалистами в ходе расследования инцидента ИБ, которые позволят избежать новых кибератак на ИС организации. Такое понимание процесса расследования инцидентов ИБ как непрерывного цикла является критически важной концепцией защиты от современных кибератак.

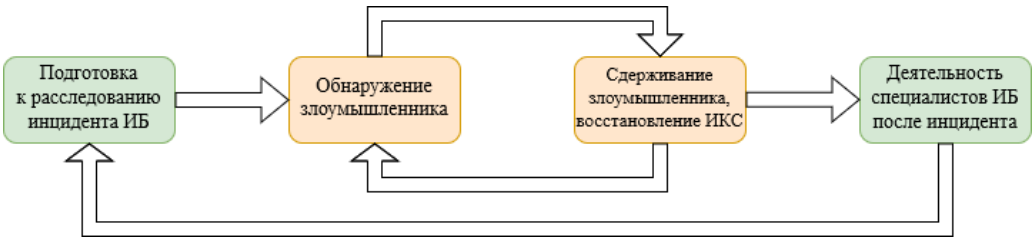


Рис. 2. Жизненный цикл процесса расследования инцидента ИБ

Предлагаемая автором методика затрагивает этапы жизненного цикла процесса расследования инцидента и относится к области ИБ ИС, а также может быть использована компьютерными криминалистами при появлении первых признаков целевых атак.

Новизна методики заключается в применении в ней метода [6] для выявления некой «аномальности» в поведении легитимных пользователей домена посредством интеллектуального анализа событий в различных журналах безопасности домена. Данный анализ построен на факторах поведенческого характера, которые существенно определяют вредоносную аутентификационную активность злоумышленника на этапе горизонтального перемещения в домене. На рис. 3 схематично представлено данное перемещение в ИС.

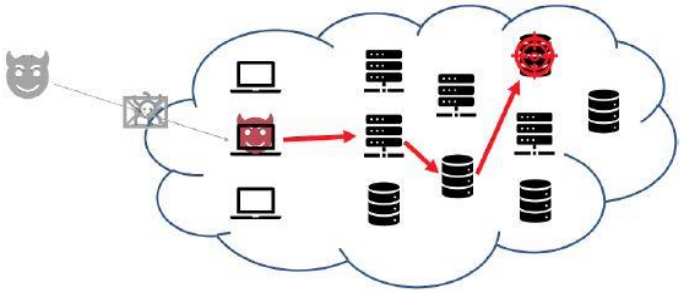


Рис. 3. Пример перемещения злоумышленника в ИС при горизонтальном перемещении в домене

2. Анализ существующих методик проведения расследований киберинцидентов

Специфика решаемой в работе задачи по созданию методики проведения расследования киберинцидента на основе интеллектуального анализа событий безопасности домена требует уточнения некоторых терминов и определений.

Целевая кибератака – это непрерывный процесс несанкционированной активности в инфраструктуре атакуемой информационной системы, удаленно управляемый вручную в реальном времени [7].

Целевая система – информационная система, воздействие на которую может непосредственно привести к наступлению недопустимого для организации события.

Ключевая система – информационная система, без воздействия на которую злоумышленник не сможет развить атаку на целевую систему, или такая система, взлом которой существенно упростит последующий сценарий атаки для компрометации целевых систем.

Инцидент ИБ – появление одного или нескольких нежелательных событий ИБ, которые могут вызвать сбой или нарушение функционирования информационной системы [8].

Криминалистически значимые данные – компьютерная информация, используемая для обоснования выводов криминалистических исследований и позволяющая решить поставленные перед криминалистическим исследованием задачи.

Централизованный сбор, агрегирование журналов ОС Windows – это процесс отправки данных журнала событий на выделенный сервер или службу для хранения, а также для упрощения поиска зловредных событий и их последующего анализа.

Расследование киберинцидента – это совокупность действий специалистов ИБ, направленных на выявление вектора целевой кибератаки, с целью минимизации ущерба и разработки рекомендаций для предотвращения инцидента ИБ в будущем.

Автором проведен анализ существующих методик проведения расследования инцидентов ИБ, описанных отечественными и зарубежными учеными.

Научная работа Овчарова В.А. и Петренко С.А. [9] направлена на расследование ИБ-инцидентов с использованием профилирования поведения динамических сетевых объектов. Профилирование производится на основе сетевого трафика.

В работе [10] приведен процесс управления динамической инфраструктурой сложных систем в условиях целенаправленных атак.

Работа [11] посвящена расследованию компьютерных инцидентов на основе идентификации дискретных событий информационной безопасности и обратного анализа по конечным исходам.

В зарубежной статье [12] представлен подход к обнаружению кибератак на основе APT в реальном времени для SIEM-систем, основанный на причинно-следственном анализе и сопоставлении сгенерированных предупреждений датчиками безопасности.

В диссертации [13] французских исследователей описано применение скрытой марковской модели для обнаружения APT-атак.

Работа [14] посвящена современным методам обнаружения вредоносных программ при APT-атаках.

В руководстве [15] сотрудниками Лаборатории Касперского описаны действия специалистов по реагированию на инциденты ИБ. Данный документ не является универсальной инструкцией по реагированию на всевозможные инциденты ИБ. В нем описаны основные инструменты для: первоначального реагирования, сбора данных, анализа потенциальных угроз и их удаления. Использование интеллектуального анализа событий безопасности авторами в нем не предлагается.

Сотрудники компании Group-IB разработали инструкцию [16] по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания. Недостатком данного документа является возможность его использования только в ИС кредитно-финансовых организаций.

На основе анализа существующих методик при проведении расследования киберинцидентов целевых атак можно сделать вывод о том, что возможности существующих научных и программных решений не удовлетворяют требованиям практики. Необходимо повышать качество обнаружения вредоносных действий злоумышленника с целью минимизации финансового и репутационного ущерба для организаций.

3. Описание методики проведения расследования киберинцидента на основе интеллектуального анализа событий безопасности домена

Предлагаемая автором методика состоит из восьми этапов и схематично представлена на рис. 4.

Этап 1. Сбор журналов событий с контроллера домена и рабочих станций ОС Windows.

Основным журналом безопасности является Security.evtx контроллера домена. В случае, если контроллер выведен из строя, либо в ИС отсутствует домен, необходим централизованный сбор журналов безопасности всех элементов ИС.

Хранение журналов в централизованной системе дает ряд преимуществ по сравнению с локальным хранением данных:

– доступ к записям журналов событий возможен даже в том случае, если исходный сервер отключен, скомпрометирован или выведен из эксплуатации;

– злоумышленникам будет сложнее удалить данные из журналов, которые уже были отправлены на устройство-коллектор;

– расследование и аудит инцидентов становится проще, поскольку все данные о событиях собираются в одном месте;

– данные могут быть проанализированы и сопоставлены более чем в одной системе;

– дальнейшее внедрение и поддержка решений, связанных с масштабируемостью, высокой доступностью и избыточностью становится легче, поскольку они могут быть реализованы на сервере сбора данных;

– осуществление контроля соответствия внутренних и внешних стандартов хранения данных журнала.

Рис. 4 Схема методики проведения расследования киберинцидента на основе интеллектуального анализа событий безопасности домена

Компанией Microsoft, начиная с ОС Windows Microsoft Server 2008 R2 / Vista, был внедрен механизм Windows Event Forwarding, позволяющий серверам Windows (или иным источникам событий) пересылать данные своих журналов на устройство-коллектор с применением функционала WinRM (службы удаленного управления ОС Windows) и использованием так называемых подписок (наборов Xpath-выражений для выбора интересующих журналов и событий на источнике).

Сервера-источники могут отправлять события на устройство-коллектор по запросу последнего (режим «Pull / Collector initiated»), так и без него (режим «Push / Source computer initiated»). Рекомендуется использовать режим «Push / Source computer initiated», поскольку в этом режиме на устройстве-коллекторе служба WinRM слушает входящие соединения, а на серверах-источниках WinRM не находится в режиме прослушивания и только периодически обращается к первому за инструкциями, что уменьшает поверхность потенциальных атак на конечные устройства.

Для шифрования потока, исходящего от источника событий к устройству-коллектору, находящихся в одном домене, и проходящего через службу WinRM используется Kerberos-шифрование SOAP-данных. При этом HTTP-заголовки и соответствующие им метаданные будут передаваться в исходном виде.

Архитектурный подход агрегирования журналов ОС Windows (рис. 4) заключается в использовании правил групповой политики для распределения конфигураций протокола WinRM и переадресации событий на группу компьютеров домена, где каждый клиент будет настроен на пересылку событий на устройство-коллектор.

После сбора журналы могут быть переданы по мере необходимости для дальнейшего анализа или хранения.

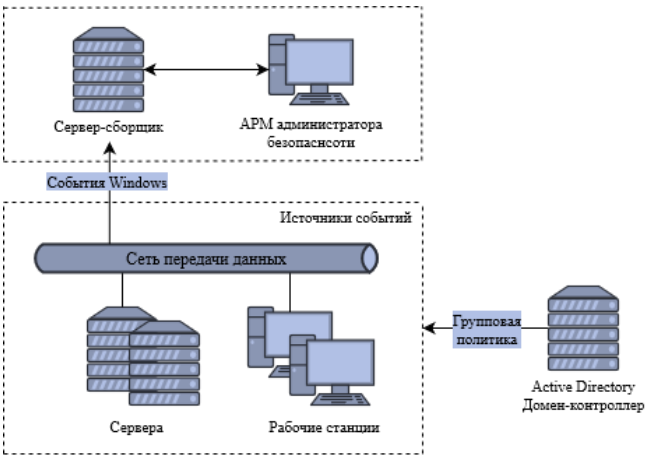


Рис. 4. Архитектура централизованного сбора событий ОС Windows

Для включения сервиса сбора журналов компьютерному криминалисту необходимо выполнить следующие действия:

1. на устройстве-коллекторе включить службу WinRM и установить режим прослушивания на порту TCP:5985 из командной строки, командой: *winrm quickconfig;*
2. на устройстве-коллекторе отключить службу Windows Remote Shell (WinRS), так как данная служба может использоваться злоумышленником на этапе «горизонтального перемещения» при проведении целенаправленной атаки на инфраструктуру. Отключить WinRS можно либо при изменении политики «Конфигурация компьютера / Административные шаблоны / Компоненты Windows / Удаленная оболочка Windows / Разрешить доступ к удаленной оболочке -> Запретить», либо командой: *winrm set winrm/config/winrs @{AllowRemoteShellAccess="false"};*
3. на устройстве-коллекторе необходимо включить службу сборщика событий Windows, чтобы он мог получать журналы событий с устройств-источников, при помощи команды: *wecutil qc*. Вместе с тем в Windows Firewall устанавливается правило, допускающее входящие соединения на устройство-коллектор на порту TCP:5985;
4. аналогично устройству-коллектору на устройствах-источниках необходимо запустить службу WinRM и наряду с этим установить «Тип запуска» в значении «Автостарт»;
5. в случае, если на исходном устройстве установлен Windows Firewall, необходимо позволить ему удаленно управлять журналом событий и отслеживать трафик удаленного мониторинга событий, при помощи редактирования разрешений взаимодействия защитника Windows с приложением или его компонентом «Панель управления / Система и безопасность / Брандмауэр «защитника» Windows / Разрешенные программы -> Удаленный мониторинг событий и Удаленное управление журналом событий»;
6. по умолчанию некоторые журналы доступны только администраторам. Это может вызвать проблемы при получении журналов из других систем. Чтобы избежать этого, на устройствах-источниках необходимо обеспечить доступ к журналам аудита службе WinRM посредством включения встроенной учетной записи NT AUTHORITY в локальную группу чтения журнала событий (Event Log Readers). Прежде, чем переходить к следующему шагу, необходимо перезапустить службы WinRM и EventLog при помощи команд:
Get-Service -ComputerName HOST_NAME -Name WinRM | Restart-Service и *Get-Service -ComputerName HOST_NAME -Name EventLog | Restart-Service* соответственно;
7. для устройств-источников необходимо сконфигурировать групповую политику «Конфигурация компьютера / Административные шаблоны / Компоненты Windows / Пересылка событий / Настроить адрес сервера...», указав в ней адрес устройства-коллектора, а также временной интервал (в секундах), согласно которому источник будет обращаться к сборщику, ожидая новые инструкции, в следующем виде:
Server=http://servername.domain.local:5985/wsman/SubscriptionManager/WEC, Refresh=(временной интервал);
8. На заключительном шаге следует сконфигурировать подписки на сервере-коллекторе. Для этого необходимо открыть программу Event Viewer и выбрать раздел «Подписки -> Создать подписку», в открывшемся окне напротив опции «Source Computer Initiated», что соответствует режиму Push, поставить галочку, после этого добавить интересующие нас устройства или их группы, которые будут присылать события своих журналов на устройство-коллектор и прописать XPath-запрос, необходимый для сбора определенных журналов.

Дополнительно в случае необходимости автором предлагается использовать программный комплекс сбора артефактов операционной системы Linux [17]. Сбор артефактов включает в себя: системную информацию, имя узла, сетевые интерфейсы, последние аутентификации пользователей в систему, данные об автозапуске, содержимое папки /tmp. ОС: Linux.

Этап 2. Выявление пользователей домена с аномальным поведением в домене с помощью программного комплекса обнаружения вредоносной активности в корпоративной сети.

За основу анализа необходимо применять журнал безопасности Security.evtx, который описан в методе обнаружения аномального поведения пользователей с использованием интеллектуального анализа событий безопасности домена [18]. Данный метод основан на знаниях, полученных из модели ассоциированного представления аутентификационных действий злоумышленника в домене [19].

Автором предложены шесть основных факторов, влияющих на коэффициент «аномальности» пользователей домена:

– большое количество попыток аутентификации пользователя домена при атаке методом перебора пароля;

– большое количество аутентификаций одного пользователя (например, локального администратора) к нескольким рабочим станциям в домене;

– особое внимание уделено времени суток (например, в нерабочее время), в которое выявлены аутентификационные действия пользователя домена;

– обнаружение применения нестандартных техник аутентификации пользователя (например, атака Pass-the-Hash, Pass-the-Ticket, Kerberoasting);

– экспериментально определены вредоносные цепочки событий безопасности при удаленном исполнении кода злоумышленником на основе пакета Impacket;

– дополнительно уделено внимание на техники и инструменты злоумышленника для удаленного подключения к различным узлам в домене.

Для определения статистического поведения временных рядов с целью выявления выбросов и точек изменения данных о событиях безопасности в домене используется модель авторегрессии. Исходя из того, что данные, полученные при анализе журналов событий безопасности ОС Windows (Security.evtx, System.evtx, RemoteConnectionManager%4Operational.evtx), могут быть представлены в виде временного ряда и имеют при этом стохастических характер, программную реализацию по обнаружению аномальной активности пользователя в домене решено реализовать на основе алгоритма ChangeFinder [20].

Для экспериментальной апробации предложенного подхода [21] к обнаружению вредоносной активности пользователей домена были смоделированы различные события безопасности, на основе которых был определен критерий оценивания аномалий: нормальная активность пользователя – до 12 баллов; низкий уровень аномальной активности от 13 до 15 баллов; средний уровень аномальной активности от 16 до 17 баллов; высокий уровень аномальной активности – от 17 баллов и выше (Рис. 5).

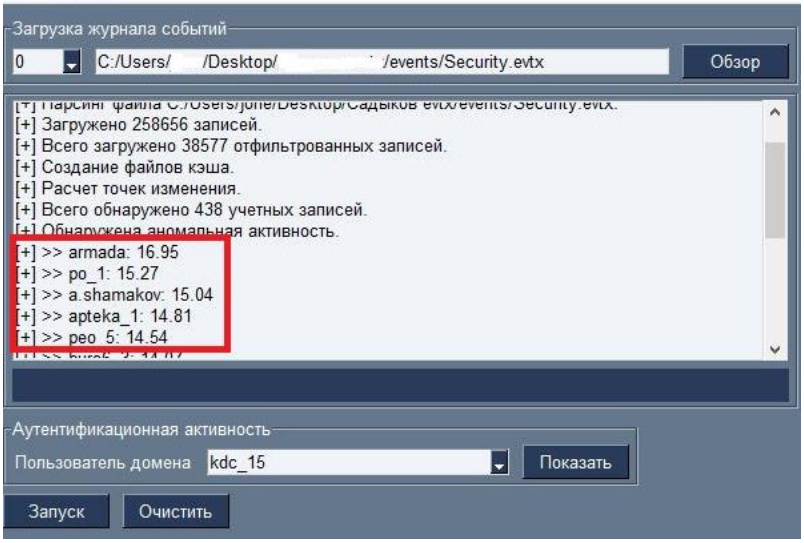


Рис. 5. Скриншот работы программного комплекса обнаружения вредоносной активности в корпоративной сети

Стоит отметить, что точность получаемых на выходе результатов работы программы [22] напрямую зависит от промежутка времени, в течение которого происходил учет данных событий.

Экспериментально выявлено, что для интеллектуального анализа желательно использовать журналы событий, в которых содержится активность пользователей домена как минимум за прошедшую неделю.

Этап 3. Создание и анализ дампов оперативной памяти рабочих станций и серверов домена.

На данном этапе компьютерным криминалистам в первую очередь необходимо создать дампы оперативной памяти (ОП) тех узлов ИС, в которых обнаружена аномальная активность пользователей домена.

При сборе криминалистически значимых данных важным условием для полноты картины об инциденте остается наличие именно дампов ОП (энергозависимых источников). В них содержится ценная информация о процессах, активных и закрытых сетевых соединениях, данных об исполняемых файлах, библиотеках DLL. Она может ускорить процесс расследования инцидента ИБ.

Примером программного обеспечения (ПО), с помощью которого специалисты создают дампы ОП, является бесплатная программа FTK Imager [23]. Она входит в состав набор утилит компьютерной криминалистики Forensic Toolkit (Рис. 6).

Непосредственно для анализа дампа ОП компьютерные криминалисты применяют фреймворки Volatility и Rekall, написанные на языке Python. Они будут работать в любой ОС (Windows, *nix, macOS). Одним из ключевых отличий стоит отметить, что Rekall ввел автоматическое обнаружение и даже создание подходящего профиля для анализируемого образца ОП. Профиль содержит сведения о расположении и формате ключевых структур данных, находящихся в системной памяти, которые имеют решающее значение для возможности интерпретации и анализа данных. А при применении криминалистом ПО volatility на первом шаге необходимо определить и явно указать профиль ОС (модули imageinfo и kdbgscan).

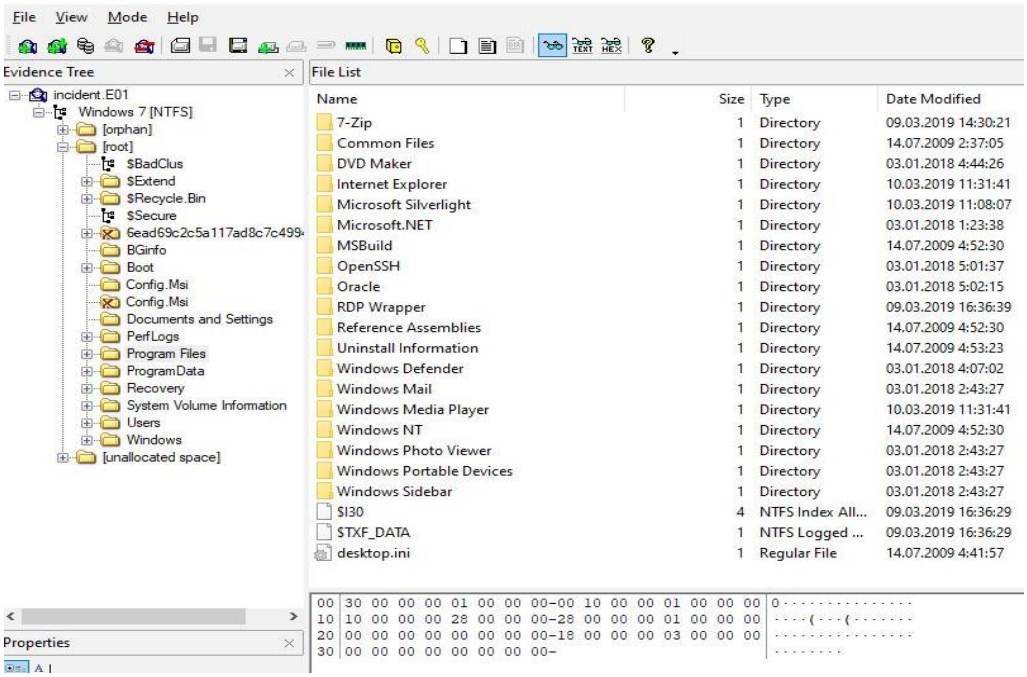


Рис. 6. Скриншот программы FTK Imager

Пример работы модуля imageinfo представлен на рис. 7.

```
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (%путь%/%имя_образа%)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002c430a0L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002c44d00L
                KPCR for CPU 1 : 0xfffff880009ef000L
             KUSER_SHARED_DATA : 0xffffff78000000000L
```

Рис. 7. Выявление версии ОС плагином imageinfo фреймворка volatility

Основные плагины фреймворков Volatility и Rekall сведены в единую таблицу.

Табл. Описание основных плагинов фреймворков Volatility и Rekall

Имя плагина	Краткое описание
Imageinfo	Отображает информацию об анализируемом образце памяти
Pslist	Отображает детали процессов
Pstree	Отображает отношения «родитель-потомок» между процессами
Psxview	Отображает процессы, обнаруженные различными способами, для помощи в идентификации вредоносных процессов
Dlllist	Показывает исполняемый файл, библиотеки DLL и командную строку, используемые для каждого процесса
Services	Отображает информацию о службах, как записано в реестре
Svcscan	Сканирует ОП на предмет служебных объектов
Handles	Отображает информацию о дескрипторах, используемых каждым процессом
Malfind	Анализирует сегменты памяти для поиска внедренного кода
Netstat	Показывает активные соединения по протоколу TCP
Netscan	Сканирует сетевые подключения и сокеты
Printkey	Отображает информацию из ключа реестра
Dlldump	Извлекает DLL из ОП на диск
Procdump	Извлекает память процесса на диск
Timeliner	Отображает объекты на основе временной метки
Autoruns	Соотносит запущенные процессы с ASEP
Filescan	Сканирует файловые объекты в ОП
Cmdscan	Сканирует историю cmd.exe в ОП
Getsids	Показывает идентификаторы безопасности, связанные с определенным процессом

Анализ ОП – это неотъемлемый этап при расследовании киберинцидентов. Специалисты могут использовать несколько инструментов смежной направленности для получения более точного результата при исследовании дампа ОП. Данные, полученные в ходе этого анализа, с высокой долей вероятности положительно повлияют на процесс расследования.

Этап 4. Создание и анализ копий жесткого диска C:\ рабочих станций или серверов домена, в которых обнаружена аномальная активность пользователей домена.

Существует несколько вариантов создания криминалистических копий ОС Windows, которые также возможно создать программой FTK Imager:

– побитовая копия диска (physical), содержащая в себе несколько разделов, включая свободные области, а также нераспределенное пространство;

– побитовая копия определенного раздела (logical), на практике чаще всего криминалисты создают копию диска C:\, включая его свободную область;

– триаж-копия – это набор определенных системных файлов и каталогов (например, журналы событий, pf-файлы, lnk-файлы и др.), сохраняемый в виде контейнера или архива.

На рис. 8 криминалистические копии схематично представлены в виде трех квадратов разных площадей.

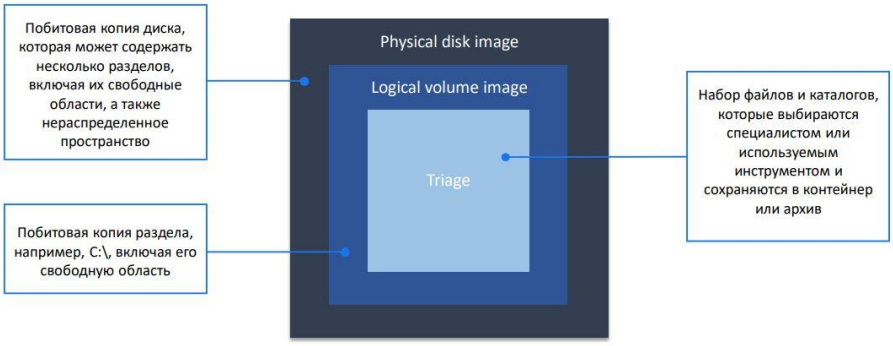


Рис. 8. Схематичное представление криминалистических копий

Стоит отметить, что компьютерные криминалисты работают всегда с копией криминалистической копии с целью не повредить основную.

При анализе специалисту необходимо проанализировать корневые ветки реестра ОС Windows: SAM, SYSTEM, NTUSER.DAT, SOFTWARE, SECURITY, USRCLASS.DAT (рис. 9). Они содержат большое количество полезной информации для поиска артефактов.

SAM	Security Account Manager содержит информацию о локальных пользователях и группах
SYSTEM	Содержит конфигурации сервисов и драйверов аппаратного обеспечения
NTUSER.DAT	Содержит информацию о программах пользователя, последних просмотренных файлах и т.д.
SOFTWARE	Содержит сведения об установленных программах и их конфигурации
SECURITY	Содержит списки контроля доступа
USRCLASS.DAT	Содержит информацию о конфигурациях пользователя

Рис. 9. Корневые ветки реестра ОС Windows

Этап 5. Анализ вредоносного ПО

Для анализа предполагаемых вредоносных файлов специалисты используют «песочницы» (Sandbox). В результате эмуляции действий объекта в изолированной среде становится возможным обнаружение ранее неизвестных угроз, а также получение ключевых индикаторов компрометации. Примером может служить онлайн-платформа AnyRun (Рис. 10).

Рис. 10. Скриншот онлайн-песочницы AnyRun (https://app.any.run)

Для получения результатов анализа в «песочнице» входящими данными могут быть: файл, хеш-сумма файла, ссылка, по которой он был загружен.

Существует большое количество онлайн-сервисов, которые предлагают бесплатный анализ образцов вредоносного ПО и предоставляют автоматические отчеты о его поведении. Категории вредоносных программ включают в себя дропперы, загрузчики, вымогатели, криптомайнеры, средства удаленного доступа/троянские программы, вирусы, черви, шпионское ПО, боты и др.

Наиболее популярными сервисами для анализа вредоносного ПО являются:

– VirusTotal (https://virustotal.com);

– Malware Configuration and Payload Extraction (https://cape.contextis.com);

– Joe Sandbox (https://joesandbox.com).

Каждый из этих сервисов содержит данные из ранее представленных образцов, что позволяет им распределять образцы в разные семейства вредоносных программ.

Для самостоятельного анализа вредоносного ПО существуют несколько методов: статический (проверка без запуска кода) и динамический (код выполняется в контролируемой среде) анализ, а также реверс-инжиниринг (исполняемый файл декомпилируется).

Этап 6. Построение хронологии событий (таймлайна) кибератаки

Существуют различные программные средства с открытым исходным кодом для построения таймлайна целевых атак, которые удовлетворяют современным практикам расследования.

Примерами таких программ являются:

– мощный кроссплатформенный инструмент для построения таймлайна журнала событий Windows и инструмент поиска угроз, созданный японской группой безопасности Yamato Security (https://github.com/Yamato-Security/hayabusa). Он может быть запущен для анализа в реальном времени,

либо путем сбора журналов из нескольких систем в автономном режиме. Выходные данные будут объединены в единую временную шкалу формата CSV для удобного анализа в Excel, Timeline Explorer или Elastic Stack. Имеет более 2200 SIGMA-правил и около 125 правил hayabusa, которые регулярно добавляются; сбор различных статистических данных, сопоставление с MITRE (Рис. 11);

Time	Computername	Eventid	Level	Alert	Details
2021-05-22 05:43:18.227 +09:00	fs01.offsec.lan	4648	informational	Explicit Logon	Source User: FS01$: Target User: admmig
2021-05-22 05:43:22.562 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-22 05:43:49.345 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-22 05:43:50.131 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-22 05:43:50.607 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-22 05:43:50.866 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-23 06:56:57.685 +09:00	fs01.offsec.lan	1102	high	Security log was cleared	User: admmig
2021-05-23 06:57:11.842 +09:00	fs01.offsec.lan	4688	high	Relevant Anti-Virus Event	
2021-05-23 06:57:11.842 +09:00	fs01.offsec.lan	4688	critical	Mimikatz Use	
2021-05-26 22:02:27.149 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:27.155 +09:00	mssql01.offsec.lan	5145	medium	DCERPC SMB Spoolss Named Pipe	
2021-05-26 22:02:27.155 +09:00	mssql01.offsec.lan	5145	critical	CVE-2021-1675 Print Spooler Exploitation IPC Access	
2021-05-26 22:02:29.726 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:29.734 +09:00	mssql01.offsec.lan	5145	medium	DCERPC SMB Spoolss Named Pipe	
2021-05-26 22:02:29.734 +09:00	mssql01.offsec.lan	5145	critical	CVE-2021-1675 Print Spooler Exploitation IPC Access	
2021-05-26 22:02:34.373 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:34.375 +09:00	mssql01.offsec.lan	5145	medium	DCERPC SMB Spoolss Named Pipe	
2021-05-26 22:02:34.379 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:34.379 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:34.380 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-27 05:24:46.570 +09:00	rootdc1.offsec.lan	4768	medium	Possible AS-REP Roasting	Possible AS-REP Roasting
2021-05-27 05:24:46.570 +09:00	rootdc1.offsec.lan	4768	informational	Kerberos TGT was requested	User: admin-test : Service: krbtgt : IP
2021-06-01 23:06:34.542 +09:00	fs01.offsec.lan	4720	medium	Local user account created	User: WADGUtilityAccount : SID:S-1-5-21-1
2021-06-01 23:08:21.225 +09:00	fs01.offsec.lan	4720	medium	Local user account created	User: elie : SID:S-1-5-21-1081258321-3780
2021-06-03 21:17:56.988 +09:00	fs01.offsec.lan	1102	high	Security log was cleared	User: admmig
2021-06-03 21:18:12.941 +09:00	fs01.offsec.lan	4672	informational	Admin Logon	User: admmig : LogonID: 0x322e5b7
2021-06-03 21:18:12.942 +09:00	fs01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-06-04 03:34:12.672 +09:00	fs01.offsec.lan	4104	high	Windows Firewall Profile Disabled	
2021-06-04 04:17:44.873 +09:00	fs01.offsec.lan	1102	high	Security log was cleared	User: admmig

Рис. 11 – Скриншот примера таймлайна утилиты Hayabusa в формате Excel

– функциональность утилиты WELA заключается в создании временной шкалы на основе аутентификаций пользователей по событиям безопасности: 4624, 4634, 4647, 4672, 4776 (Рис. 12);

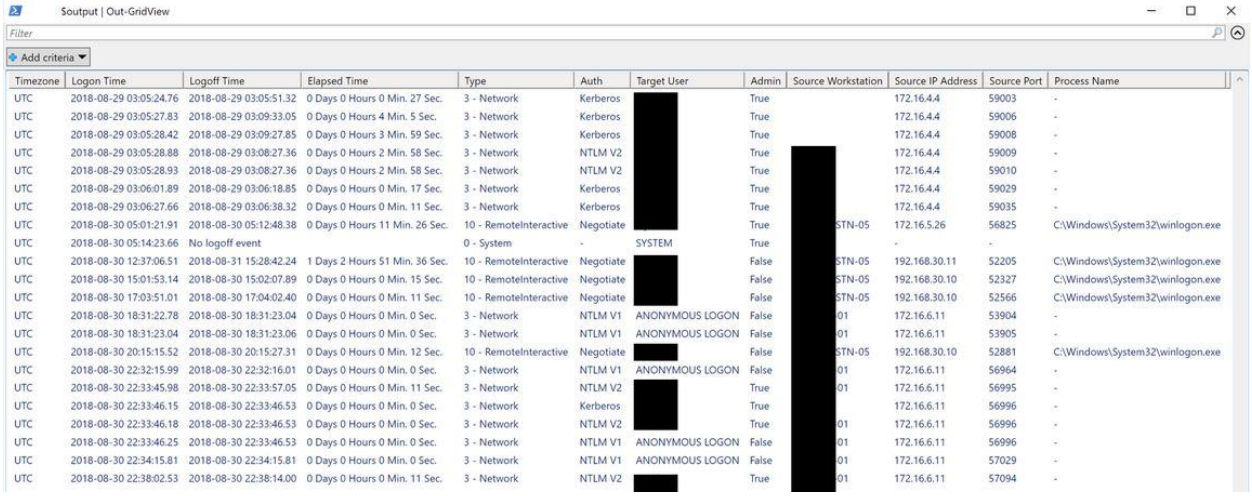


Рис. 12 – Скриншот с таймлайна по событиям безопасности утилиты WELA

– популярными утилитами при расследовании киберинцидентов является набор программ Эрика Зиммермана. Одна из них – это EvtxECmd [24], позволяющая строить дорожную карту событий ОС Windows.

Этап 7. Реагирование на киберинцидент

Цель данного этапа заключается не только в том, чтобы изолировать скомпрометированные машины, но и в недопущении уничтожения артефактов компрометации. Они могут помочь в расследовании киберинцидента. Дело в том, что некоторые угрозы могут не создавать файлов на жестком диске компьютера, а полностью размещают себя в ОП, так как их сложно там обнаружить. Вследствие этого необходимо не допустить отключения питания компьютера.

Криминалистам рекомендуется провести изоляцию зараженных компьютеров в отдельную сеть. На практике выявлялись случаи, когда при APT-атаке некоторые виды угроз отслеживали наличие сетевого соединения. В противном случае начиналось самоуничтожение следов вредоносного ПО на машине «жертвы» [15].

Далее специалисты могут применить два варианта действий: полное восстановление зараженных машин из образа ОС или удаление артефактов посредством Endpoint-антивирусом.

После успешного проведения этапа удаления артефактов необходимо произвести ввод компьютеров в локальную сеть организации. При этом необходимо проводить наблюдение за

состоянием сети и восстановленных машин, чтобы убедиться в том, что APT-атака была полностью устранена.

Этап 8. Выработка рекомендаций и составление отчета об инциденте

Любой инцидент ИБ необходимо завершать составлением отчета, в котором описывается ответы на следующие вопросы:

– каким образом злоумышленник получил доступ к ИС (являлся ли он внешним или внутренним);

– какие ключевые системы были подвержены кибератаке;

– какие пользователи домена были скомпрометированы;

– какие техники и инструменты он использовал (особенно описать его действия при горизонтальном перемещении в домене);

– в какие легитимные процессы была произведена миграция вредоносного ПО;

– подробное описание технического воздействия на ИС организации согласно матрице ATT&CK по 12 категориям тактик (получение первоначального доступа, закрепление в системе, повышение привилегий, уклонение от средств защиты, получение действительных учетных данных пользователей, этап горизонтального перемещения, использование C&C-серверов, утечку данных и др.);

– создание хронологии событий (таймлайна) кибератаки с описанием ответных действий специалистов ИБ организации;

– рекомендации по защите ИС (в том числе ключевых систем) в организации.

Рекомендации по защите ИС включают в себя:

– разделение бизнес-процессов в организации (обратить особое внимание на те компоненты инфраструктуры, которые вовлечены одновременно в несколько бизнес-процессов);

– контроль безопасности конфигурации (чем сложнее будет цепочка кибератаки до целевой системы, тем меньше вероятность успешной компрометации и, следовательно, тем больше вероятность совершения ошибки злоумышленником);

– создание усиленного мониторинга (позволит повысить вероятность обнаружения преступника даже на тех ключевых системах, на которых по каким-либо причинам не были обеспечены усиленные меры защиты или не были установлены обновления).

4. Заключение

Использование методики расследования киберинцидента на основе интеллектуального анализа событий безопасности домена позволяет на раннем этапе обнаружить вредоносную аутентификационную активность злоумышленника в домене. В первую очередь данная методика применима для организации, в которой отсутствует SIEM-система.

В предложенной методике учитываются все основные этапы проведения расследования киберинцидентов современности.

Важным ограничением применения предложенной методики является наличие контроллера домена в ИС организации. Имея информацию о событиях безопасности с контроллера, компьютерные криминалисты могут качественно и оперативно проводить расследование ИБ с целью снижения финансового и репутационного ущерба организации.

Благодарности. Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта № 40469-19/2021-К.

СПИСОК ЛИТЕРАТУРЫ

1. Анализ техник и инструментов, используемых злоумышленником при горизонтальном перемещении в корпоративной сети / С. И. Смирнов, М. А. Еремеев, И. Е. Горбачев [и др.] // Защита информации. Инсайд. – 2021. – № 1(97). – С. 58-61.
2. Отчёт компании Positive Technologies «Актуальные киберугрозы: итоги 2021 года» [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/ (дата обращения: 03.05.2022)
3. Уроки форензики. Расследуем киберинцидент CyberCorp Case 1 / Журнал Хакер (ноябрь 2021) [Электронный ресурс]. – Режим доступа: https://xakep.ru/2021/11/30/cybercorp-case-1/ (дата обращения: 03.05.2022)
4. Матрица MITRE ATT&CK. [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/ (дата обращения: 15.12.2021)
5. Отчет компании Kaspersky «Incident Response Analyst Report 2021» [Электронный ресурс]. – Режим доступа: https://media.kasperskycontenthub.com/wp-

content/uploads/sites/58/2021/09/13133152/Incident-Response-Analyst-Report-ru-2021.pdf (дата обращения: 15.12.2021)
6. Смирнов, С. И. Подход к обнаружению вредоносных действий злоумышленника на основе модели авторегрессии при расследовании киберинцидента / С. И. Смирнов, М. А. Еремеев, И. А. Прибылов // Проблемы информационной безопасности. Компьютерные системы. – 2021. – № 2(46). – С. 41-47.
7. Анатомия таргетированной атаки. [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (дата обращения: 14.05.2022)
8. Инциденты информационной безопасности [Электронный ресурс]. – Режим доступа: https://compnote.ru/otdelit/poryadok-obrabotki-intsidentov-ib/ (дата обращения: 10.05.2022)
9. Расследование ИБ-инцидентов с использованием профилирования поведения динамических сетевых объектов / В. Н. Калинин, А. Г. Ломако, В. А. Овчаров, С. А. Петренко // Защита информации. Инсайд. – 2018. – № 3(81). – С. 58-67.
10. Зегжда, Д. П. Управление динамической инфраструктурой сложных систем в условиях целенаправленных кибератак / Д. П. Зегжда, Д. С. Лаврова, Е. Ю. Павленко // Известия Российской академии наук. Теория и системы управления. – 2020. – № 3. – С. 50-63. – DOI 10.31857/S0002338820020134.
11. Овчаров, В. А. Расследование компьютерных инцидентов на основе идентификации дискретных событий информационной безопасности и обратного анализа по конечным исходам / В. А. Овчаров, П. А. Романов // Труды Военно-космической академии имени А.Ф.Можайского. – 2015. – № 648. – С. 84-89.
12. M. Khosravi and B. T. Ladani, “Alerts Correlation and Causal Analysis for APT Based Cyber Attack Detection” // IEEE Access 8, September 2020. DOI: 10.1109/ACCESS.2020.3021499
13. G. Brogi and E. Di Bernardino, ‘‘Hidden Markov models for advanced persistent threats,’’ Ph.D. dissertation, Caen-Normandy Univ., Caen, Paris, 2017.
14. Tim Niklas Witte, Phantom Malware: Conceal Malicious Actions From Malware Detection Techniques by Imitating User Activity // IEEE Access 8, January 2020
15. Руководство по реагированию на инциденты информационной безопасности / Управление технологических решений, 2017 [Электронный ресурс]. – Режим доступа: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07172131/Incident_Response_Guide_rus.pdf) (дата обращения: 15.05.2022)
16. Суханов, М.А. Инструкция по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания [Электронный ресурс]. – Режим доступа: https://www.group-ib.ru/brochures/Group-IB_dbo_instruction.pdf?ysclid=l37j32czn7 (дата обращения: 16.05.2022)
17. Свидетельство о государственной регистрации программы для ЭВМ № 2022610611 Российская Федерация. Программный комплекс сбора артефактов ОС Linux № 2021681579 : заявл. 19.12.2021: опубл. 13.01.2022 / С. И. Смирнов, Д. А. Изергин, В. С. Нефедов [и др.]. – EDN DIEHWN.
18. Смирнов, С. И. Метод обнаружения аномального поведения пользователя домена на основе интеллектуального анализа событий безопасности / С. И. Смирнов // Защита информации. Инсайд. – 2022. – № 3(105). – С. 56-63. – EDN PTAHCU.
19. Смирнов, С. И. Модель ассоциированного представления аутентификационных действий злоумышленника в домене / С. И. Смирнов, М. А. Еремеев // Защита информации. Инсайд. – 2022. – № 2(104). – С. 50-55. – EDN GPRLTS.
20. Алгоритм ChangeFinder [Электронный ресурс]. – Режим доступа: https://gist.github.com/shunsukeaihara/8080887 (дата обращения: 13.05.2022)
21. Прибылов, И. А. Подход к интеллектуальному анализу аутентификационной активности пользователей домена / И. А. Прибылов, С. И. Смирнов // Актуальные вопросы развития современной цифровой среды : сборник статей по материалам научно-технической конференции молодых ученых, Москва, 14–16 апреля 2021 года. – Волгоград: ИП ЧЕРНЯЕВА ЮЛИЯ ИГОРЕВНА (Издательский дом "Сириус"), 2021. – С. 154-160.
22. Свидетельство о государственной регистрации программы для ЭВМ № 2021614531 Российская Федерация. Программный комплекс обнаружения вредоносной

активности в корпоративной сети: № 2021613300: заявл. 10.03.2021 : опубл. 25.03.2021 / С. И. Смирнов, И. А. Прибылов, Ш. Г. Магомедов, Д. А. Изергин. – EDN MGPSME.
23. FTK Imager [Электронный ресурс]. – Режим доступа: https://accessdata.com/product-download/ftk-imager-version-4-5 (дата обращения: 07.06.2022)
24. Парсер логов EvtxECmd [Электронный ресурс]. – Режим доступа: https://github.com/EricZimmerman/evtx (дата обращения: 09.06.2022)

Трапезников Е.В.
ФГАОУ ВО Омский государственный технический университет, старший преподаватель,
evtrapeznikov@yandex.ru

ОЦЕНКА УРОВНЯ ЗАЩИЩЁННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ МАРКОВСКИХ МОДЕЛЕЙ КИБЕРУГРОЗ

Аннотация: В работе представлено исследование, посвящённое оценки уровня защищенности автоматизированных систем с использование марковских моделей киберугроз. В исследовании представлен анализ современных проблем информационной безопасности, приведен аналитический обзор современных подходов к моделированию процессов защиты информации. На основе представленного обзора, в качестве основы была выбрана марковская модель киберугроз. В исследовании представлено описание марковской модели кибератак. Приведено описание составляющих модели. Определены две метрики безопасности и даны их определения. Сформулирована задача оптимизации средств защиты. Представлен алгоритм сбора и обработки значимых исходных данных об автоматизированной системе. Для проведения имитационного моделирования разработано соответствующее программное обеспечение.

Ключевые слова: марковская цепь, марковская модель киберугроз, кибератаки, уязвимости, оптимизация, алгоритм сбора данных, метрики безопасности.

ВВЕДЕНИЕ

На сегодняшний день защита информации занимает одну из определяющих ролей в обеспечении безопасности автоматизированных систем и является одним из перспективных направлений в исследовании и развитии. С каждым днем появляются все новые и новые угрозы и уязвимости, новые средства защиты информации и программное обеспечение, тестирование которых необходимо до ввода их в эксплуатацию. На фоне этого возникают определенные проблемы. Рассмотрим некоторые из существующих проблем.

Одной из первых проблем является проблема инвестиций в защиту информации. Авторы работ [1; 2] отмечают, что экономический ущерб при потери информации может быть значителен для любого предприятия не зависимо от его организационной формы. Ввиду этого авторы отмечают важность оценки эффективности комплексных мер защиты информации. Также авторами отмечено, что экономическая оценка инвестиционных вложений в систему защиты информации осложняется высокой степенью неопределенности и вероятностным характером основных параметров системы, что зачастую требует дополнительных ресурсов, в том числе и времени. В конечном итоге это может повлечь проблемы несвоевременного реагирования на угрозы информационной безопасности [1].

Следующая немаловажная проблема – оценка защищенности информации. Для того чтобы инвестиции в систему защиты информации были соизмеримы со стоимостью самой информации важно правильно оценить уровень защищенности информации. Подобная оценка порой довольно затруднена из-за быстро меняющихся технологий и часто обнаруживаемых новых угроз кибербезопасности.

В работе [3] авторы провели исследование качественных и количественных методов, связанных с управлением рисками информационной безопасности. Было выделено, что наиболее комплексные подходы включают как количественные методы, так и качественные. Авторы в своей работе выносят предположение, что существующие методы оценки информационной безопасности зачастую ошибочны и в итоге решения по защите информации строятся на эвристике и оптимистических представлениях.

Несколько иной подход к оценке защищенности информации предложен в работе [4]. По мнению авторов этой статьи, подход в оценке должен одновременно быть «абстрактным» (то есть должен предполагать, что уязвимости и источники угрозы могут быть скрыты до начала атаки), а также близким к реальности, поскольку оценка влияет на развитие всей системы защиты информации. Слабая оценка потенциальной угрозы приводит к недостаточным мерам безопасности, а, в свою очередь, завышенная оценка приводит к необоснованным тратам на защиту информации. Авторы цитируемой работы также предлагают некоторый подход в оценке угроз на основе стохастических марковских моде-лей.

После того, как оценка защищенности информации проведена, возникает следующая за ней проблема оптимизации ресурсов, например, средств защиты. На практике обычно эта проблема игнорируется, в связи с тем, что используемые механизмы и средства защиты заранее предписаны нормативно-методическими рекомендациями регуляторов ИБ. С другой стороны, в коммерческом

секторе нет подобных жестких лимитирующих ограничений; собственник информации сам выбирает наиболее удобные с его точки зрения средства кибербезопасности, поэтому задача оптимизации для него становиться весьма актуальной [5; 6].

Упомянем здесь еще одну важную проблему, связанную с обеспечением защиты информации – проблему *оценки рисков* информационной безопасности. *Риск информационной безопасности* – это возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации [7; 8]. Согласно документу [7] менеджмент риска информационной безопасности должен способствовать:

1. идентификации рисков;
2. оценке рисков, исходя из последствий их реализации для бизнеса и вероятности их возникновения;
3. осознанию и информированию о вероятности и последствиях рисков;
4. установлению приоритетов в рамках обработки рисков;
5. установлению приоритетов мероприятий по снижению имеющих место рисков;
6. привлечению причастных сторон к принятию решений о менеджменте риска и поддержанию их информированности о состоянии менеджмента риска;
7. эффективности проводимого мониторинга обработки рисков;
8. проведению регулярного мониторинга и пересмотра процесса менеджмента риска;
9. сбору информации для совершенствования менеджмента риска;
10. подготовке менеджеров и персонала по вопросам рисков и необходимых действий, предпринимаемых для их уменьшения.

В современных исследования используются различные методы к моделированию систем защиты информации, систем анализа и аудита и систем оценки уровня защищенности [9]. Авторы исследований в своих трудах обосновывают правильность своего выбора. Наиболее часто используемые подходы в настоящий момент, которые отражены в соответствующих исследования:

- марковские стохастические модели [10; 11];
- технологии иммунных систем [12];
- байесовская сеть [13];
- нейронные сети [14];
- методы имитационного моделирования атак [15];
- обобщенные модели системы защиты;
- модели, построенные на основе теории графов;
- модели, основанные на теории игр;
- теория надежности.

В результате анализа предметной области была определена следующая **цель исследования** – анализ и выбор математических моделей киберугроз для оценки уровня защищенности информации в автоматизированных системах с возможностью оптимизации и аудита средств защиты информации.

Для решения поставленной цели были определены следующий **задачи:**

1. Определение рационального варианта моделирования системы защиты информации.
2. Определение границ возможности использования марковских моделей киберугроз предложенных А.П. Росенко в качестве базовых для оптимизации системы защиты информации.
3. Определение рационального алгоритма сбора и обработки значимых исходных данных об автоматизированной системе для построения и создания системы защиты с использованием общей системы оценки уязвимостей.
4. Создание комплекса программ, ориентированных на оценку защищенности информации в автоматизированной системе с использованием марковских моделей киберугроз. Экспериментальная апробация.

Объектом исследования в исследовательской работе являются система аудита функционирования защиты информации автоматизированной системы управления информацией в организации и ее оптимизация.

Предметом исследования является комплекс приоритетных показателей, влияющих на систему защиты информации и рисков безопасности, позволяющих осуществлять аудит систем защиты информации, оценку уровня защищенности и возможность оптимизации средств защиты информации, используя математическое моделирование.

При проведении исследований и реализации поставленной цели использовались следующие **методологии и методы исследования:** методы математического моделирования, теория защиты информации, теория алгоритмов, технология баз данных, метод экспертных оценок, технология

разработки программного обеспечения, теория информационной безопасности и методология защиты, проведение вычислительного эксперимента, объектно-ориентированное программирование.

В исследовании были определены следующие **положения, выносимые на защиту**, которые обеспечивают решение задачи оценки уровня защищенности информации в автоматизированных системах с возможностью получения необходимых практических рекомендация по оптимизации средств защиты.

1. Конкретизированы метрики безопасности для оценки уровня защищенности автоматизированных систем, используя аналитическое исследование класса марковских моделей киберугроз, предложенных А.П. Росенко.

2. Метод решения задачи выбора оптимальных конфигураций средств защиты автоматизированной системы путем адаптации численного метода последовательного анализа вариантов для их решения.

3. Алгоритм сбора и обработки значимых исходных данных исследуемой автоматизированной системы с использованием общей системы оценки уязвимостей (CVSSv3) и их последующей агрегаций для вычисления метрик безопасности для создания новых и совершенствования существующих средств защиты информации.

4. Программный комплекс, обеспечивающий оценку уровня защищенности автоматизированной системы, разработанный на основе уточненных моделей и предложенных алгоритмов для информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.

Научная новизна результатов определяется следующие пунктами**:**

1. Впервые получены явные аналитические формулы для вероятностей состояний марковской модели киберугроз, исследованы их долговременные асимптотики.

2. Конкретизированы метрики безопасности и получены явные аналитические формулы для их расчета. Для определения достоверности расчета метрик предложено имитационное моделирование.

3. Для оптимизации системы защиты информации выделены две оптимизационные задачи, принадлежащие классу нелинейных дискретных оптимизационных задач, для решения которых адаптирован численный метод последовательного анализа вариантов.

4. Для оптимизации системы защиты информации разработан алгоритм сбора и обработки значимых исходных данных об автоматизированной системе с использованием общей системы оценки уязвимостей.

5. Предложен комплекс программ, позволяющий автоматизировать процесс оценки уровня защищенности системы защиты информации и ее аудит.

МАРКОВСКАЯ МОДЕЛЬ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

В исследовании представлена модель, которая является обобщением модели, предложенной в работах А.П. Росенко с учетом наших изменений и улучшений, а также западных исследований.

Предположим, что существует информационная система, потенциально подверженную n различным кибератакам с вероятностями соответственно $q_1, q_2, ..., q_n$.

Определим следующие предположения:

1. Любый изменения системы происходят в *дискретные* моменты времени

$$t = 0,1,..., \tag{1}$$

2. В единицу времени существует только одна кибератака.

3. Следующее состояние зависит от предыдущего.

4. Вероятность отражения атак равны соответственно $r_1, r_2, ..., r_n$.

Обозначим состояние компьютерной системы через (рис. 1)

$$s_0, s_1, ..., s_n, \tag{2}$$

1. s_0 – данное состояние характеризует отсутствие кибератаки, оно также называется начальным состоянием или безопасным;

2. s_i –это состояние, в котором происходит *i-ая* кибератака, $i = 1, 2, ..., n$;

3. s_{n+i} - это состояние, в которое переходит система после успешной *i-ой* кибератаки, $i = 1, 2, ..., n$.

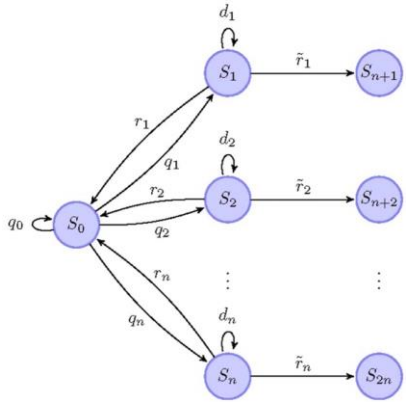


Рис. 1. Диаграмма состояний модели

Если система в момент времени *t* находится в состоянии s_i, то в момент времени *t+1* реализуется один из трех вариантов:

1. атака будет устранена с вероятностью r_i и система перейдет из состояния s_i в начальное состояние s_0;

2. система с вероятностью d_i останется в состоянии s_i;

3. с вероятностью $r_i = 1 - r_i - d_i$ атака успешно завершается и система перейдет в финальное состояние s_{n+i}

Определим составляющие нашей модели в соответствии с диаграммой состояний (рис. 1):

1. $q = (q_1, q_2, ..., q_n)$ –это вектор вероятностей появления кибератаки, формируется в том числе с помощью общей системы оценки уязвимостей (CVSSv3);

2. $r = (r_1, r_2, ..., r_n)$ –это вектор вероятностей отражения киберугрозы, формируется на основе экспертной оценки;

3. $d = (d_1, d_2, ..., d_n)$ – в данном случае это вектор вероятностей задержки кибератаки.

Свершение кибератаки определяет переход системы из одного состояния в следующее состояние. Задержка позволяет показать с какой вероятностей система будет находится в данном состоянии какой либо промежуток времени

Когда система переходит в финальное состояние, что говорит об успешности свершения кибератаки, не предполагается возврат ее к безопасному состоянию.

Матрица переходных вероятностей марковской цепи в нашем случае имеет виде (3).

$$\Pi = \begin{pmatrix} q_0 & q_1 & q_2 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ r_1 & d_1 & 0 & \cdots & 0 & \tilde{r}_1 & 0 & \cdots & 0 \\ r_2 & 0 & d_2 & \cdots & 0 & 0 & \tilde{r}_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ r_n & 0 & 0 & \cdots & d_n & 0 & 0 & \cdots & \tilde{r}_n \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \quad (3)$$

К сожалению, в случае матрицы (3) общего вида вывод явных аналитических формул для вероятностей $p_i(t)$ затруднен ввиду вычислительных трудностей, связанных с возведением матрицы в произвольную степень *t*. Поэтому в исследовании были определены несколько частных случаев:

1. *Случай отсутствия защиты:* $r_i = 0, i = 1, 2, ..., n$.

2. *Случай отсутствия задержек:* $d_i = 0, i = 1, 2, ..., n$.

Для этих случаев были получены аналитические формулы вероятностей $p_i(t)$.

МЕТРИКИ БЕЗОПАСНОСТИ

В работе формируется понятие метрики безопасности. *Метрика* — это некоторая оценка или система оценок, основанная на имеющихся данных или полученная в результате измерений, которая используется для облегчения принятия решений.

В работе сконструированы две метрики:

1. *Время до отказа безопасности* - мы будем называть число T переходов между состояниями в марковской цепи до ее первого попадания в одно из поглощающих состояний (которое система не сможет покинуть). Данная метрика может служить для оценки временных аспектов безопасного функционирования автоматизированных систем.

Нами была получена явная формула для вычисления среднего времени до отказа безопасности (4).

$$\tau = \frac{\prod_{j=1}^{n}\left(1-d_i\right) + \sum_{i=1}^{n} q_i \prod_{j=1}^{n}\left(1-\left(1-\delta_{ij}\right)d_i\right)}{\sum_{i=1}^{n} q_i \prod_{j=1}^{n}\left(1-\delta_{ij} r_i - d_i\right)} \tag{4}$$

2. *Средний риск при отказе безопасности (R)* - используется для оценки потенциальных потерь, возникающих в результате той или иной кибератаки, направленной на систему.

Нами была получена аналитическая формула (5) для R.

$$R = \frac{\sum_{i=1}^{n} q_i U_i \prod_{j=1}^{n}\left(1-\delta_{ij} r_i - d_i\right)}{\sum_{k=1}^{n} q_k \prod_{j=1}^{n}\left(1-\delta_{kj} r_i - d_i\right)} \tag{5}$$

ЗАДАЧА ВЫБОРА ОПТИМАЛЬНОГО НАБОРА СРЕДСТВ ЗАЩИТЫ

В работе решается задача выбора оптимального набора средств защиты. Первоначально формируется вектор средств защиты для исследуемой системы (6).

$$z = \left\{z_1, z_2, \ldots, z_m\right\} \in \{0,1\}^m \tag{6}$$

Введем обозначение $r_{i,a}$ – вероятность отражения i-ой угрозы a-ым средством защиты. Поскольку несколько средств защиты могут отразить одну угрозу одновременно, вероятность отражения угрозы всеми средства защиты будет выражено формулой (7).

$$r_i(z) = \sum_{k=1}^{m} (-1)^b \sum_{a_1<a_2<\ldots<a_k} \left(r_{i,a_1} z_{a_1}\right)\left(r_{i,a_2} z_{a_2}\right)\cdots\left(r_{i,a_k} z_{a_k}\right) \tag{7}$$

Исходя из практики, чаще всего ставится задача определения оптимального поднабора из некоторого заранее заданного набора средств защиты информации. В зависимости от конкретных целей, задача оптимизации может быть сформулированная по-разному. Использование представленной модели позволяет сформулировать задачу оптимизации, сводящуюся к нахождению баланса между стоимостью защитных мер и их функциональной эффективностью.

Введём функцию стоимости конфигурации системы защиты. Для этого обозначим c_a стоимость a-го средства защиты. Тогда стоимость данной конфигурации **z** может быть записана в виде следующей линейной по **z** (8)

$$C(z) = \sum_{a=1}^{m}\left(c_a z_a\right) \tag{8}$$

Первая из возможных оптимизационных задач – максимизация среднего время жизни системы при ограниченных средствах на использование механизмов защиты. Формальная запись этой задачи будет выглядеть следующим образом (9).

$$\tau(z) \to max, C(z) \le C_0 \tag{9}$$

Здесь C_0 – максимальная величина затрат на приобретение и использование средства защиты от кибератак.

Вторая возможная оптимизационная задача – выбор конфигурации системы защиты, при которой затраты будут минимальные при ограничении на продолжительность функционирования автоматизированной системы (10).

$$\tau(z) \geq \tau_0, C(z) \rightarrow min \tag{10}$$

Здесь τ_0 – нижняя граница среднего времени до отказа безопасности, приемлемая для данной системы.

Аналогичные оптимизационные задачи могут быть поставлены и в случае использования второй метрики – среднего риска до отказа безопасности. Отметим также, что может быть сформулирована и более сложная оптимизационная задача, в которой имеется две целевые функции или в которой используется ограничение в виде двух неравенств; рассмотрение таких возможностей, однако, не является предметом настоящей работы.

Для решения оптимизационных задач существует целый ряд решений, к примеру прямой перебор, метод генетического алгоритма и т.д.. Для решения представленной задачи был выбран метод последовательное анализа вариантов. Главная идея метода заключается в пошаговом движение по дереву частичных решений и отсев тех решений, которые не могут быть достроены ни до оптимальных, ни до допустимых.

Отсев таких решений происходит с помощью набора элиминирующих тестов (11)

$$\sigma = \left\{ \xi_0, \xi_1, \ldots, \xi_k \right\} \tag{11}$$

В работе, помимо двух тестов, которые присутствуют в методе всегда, были также определены еще два дополнительных теста:

1. ξ_0 - проверяет допустимость решения (удовлетворяет ли условию $\tau(z) \geq \tau_0$);
2. ξ_1 - сравнивает допустимые решения по значимой целевой функции *C(z);*
3. ξ_2 - использует свойство не убывания целевой функции *C(z)* при вычислении оценки частичных решений;
4. ξ_3 - использует свойство монотонности функции $\tau(z)$.

РАЗРАБОТКА АЛГОРИТМА СБОРА И ОБРАБОТКИ ЗНАЧИМЫХ ИСХОДНЫХ ДАННЫХ ОБ АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ

Определим одну из проблем, которая решается в данном исследовании– при нахождении в рамках нормативно-правовых актов набор средств защиты должен соответствовать определенному классу автоматизированной системы. Данный набор средств защиты определяется как необходимый; однако для того, чтобы оптимизировать расходы на средства защиты, такой набор должен обладать свойством достаточности, который позволит получить высокую оценку уровня защищенности с помощью строгих математических моделей. В исследовании приводится разработка алгоритма сбора и обработки значимых исходных данных о текущем состоянии автоматизированной системы и ее средств защиты, если тако-вые имеются.

Общий метод оценки уровня защищенности информации в информационной системе с использование марковской модели в соответствии с методологией SADT представлена на рис. 2.

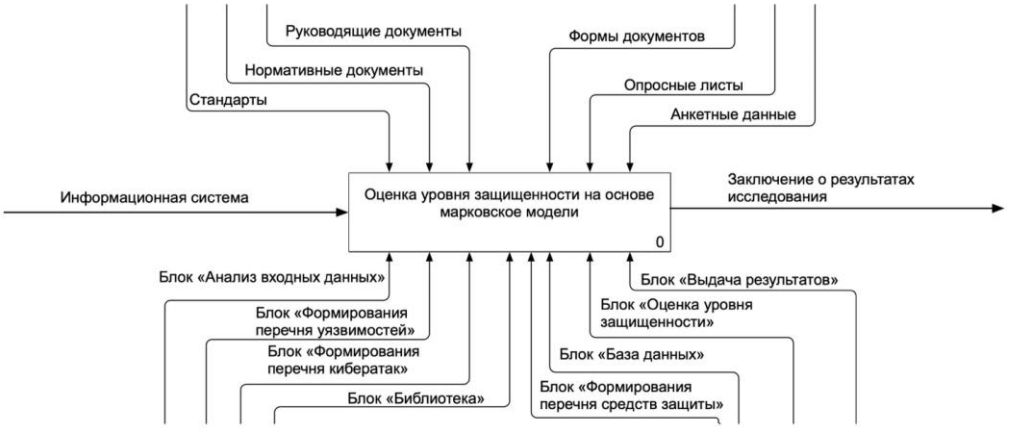


Рис. 2. Верхний уровень IDFE0-модели

Определим составляющие:

1) Вход
    a. Исследуемая информационная система
2) Управление
    a. Стандарты (ГОСТ)
    b. Нормативные документы
    c. Руководящие документы
    d. Формы документов
    e. Опросные листы
    f. Анкетные данные
3) Механизмы
    a. Блок «Анализа входных данных
    b. Блок «База данных»
    c. Блок «Библиотека»
    d. Блок «Формирования перечня уязвимостей»
    e. Блок «Формирования перечня кибератак»
    f. Блок «Формирования перечня средств защиты»
    g. Блок «Оценка уровня защищенности»
    h. Блок «Выдача результатов»
4) Выход
    a. Заключение о результатах исследований

Все механизмы имеют взаимосвязи между собой. Общая схема связей блоков представлена на рис. 3.

Определим основные стадии алгоритма:

1) анализ входных данных – определяется текущий состав информационной системы путем анкетирования, определяется состав системы защиты если таковая имеется, определяется защищаемая информация;

2) формирование перечня угроз – определяются текущие актуальные уязвимости и угрозы на основе анкетирования и состава системы;

3) формирование перечня кибератак – определяются возможные кибератаки на основе оставленного перечня уязвимостей;

4) формирование перечня средств защиты – для формирование используются данные из анализа входных данных, а также определяется перечень средств на основе возможных кибератак;

5) оценка защищенности – определение среднего времени до отказа безопасности и возможного ущерба;

6) формирование результатов.

Первые этапы алгоритма позволяют собрать необходимую информацию об автоматизированной системе, для проведения оценки защищенности.

На основе полученных данных происходит формирование перечня возможных угроз. При формировании перечня угроз используется комплекс методов:

1) на основе банка данных ФСТЭК и обще доступного справочника уязвимостей CVE формируется список уязвимостей в зависимости от установленного программного обеспечения, операционной системы, средств защиты и оборудования;

2) на основе полученных уязвимостей формируется перечень возможных кибератак. Перечень формируется на основе общедоступных баз CAPEC и MITRE ATT&CK. Данные базы позволяют наиболее максимально сформировать возможные векторы атак;

3) с использование стандарта CVSSv3 оценивается опасность каждой уязвимости с использованием понятий базовая метрика, временные метрики и контекстные метрики. Стандарт CVSS позволяет сформировать вектор вероятностей кибератак q .

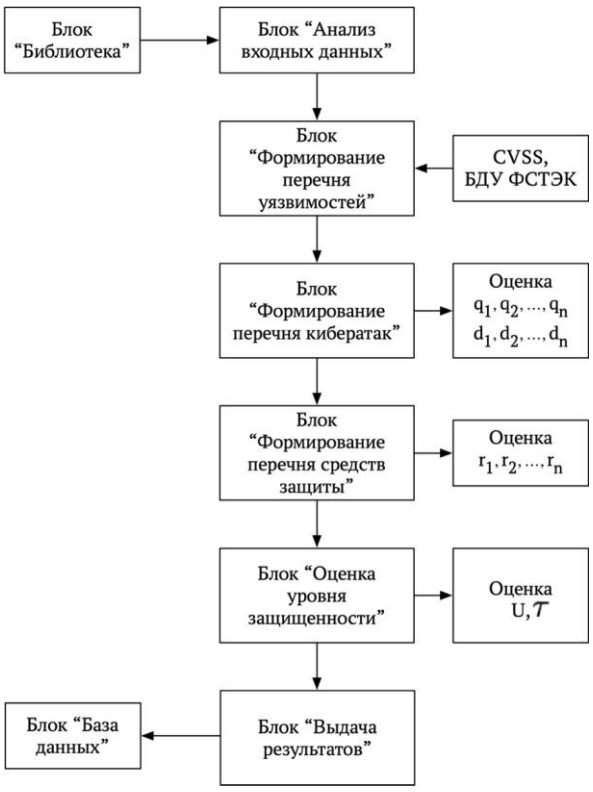


Рис. 3. Схема взаимосвязей механизмов

На основе проведеного анализа необходимо определить набор средств защиты, который позволит отражать, либо сдерживать возможные векторы атак. Перечень формируется на основе существующих средств, так и на основе возможных векторов атак.

В итоге формируется вектор вероятностей отражений кибератак $r = (r_1, r_2, ..., r_n)$ и вектор вероятностей задержки кибератак $d = (d_1, d_2, ..., d_n)$. Полученные данные необходимы для итоговых расчетов по оценки защищенности.

Для вычисления предложенных метрик безопасности требуется знать величины исходных параметров модели, которые определяются с помощью представленного алгоритма. Этими параметрами являются:

- вектор вероятностей возникновения кибератак $q = (q_1, q_2, ..., q_n)$;
- вектор вероятностей отражений кибератак $r = (r_1, r_2, ..., r_n)$;
- вектор вероятностей задержки кибератак $d = (d_1, d_2, ..., d_n)$;
- вектор ущербов от кибератак: $U = (U_1, U_2, ..., U_n)$.

Кроме того, требуется явно указать временной интервал Δt, который задает минимальное время, по истечении которого компьютерная система может изменить свое состояние (такт времени). В соответствии с этим, все требуемые вероятности должны быть отнесены к данному временному интервалу; например, величина q_i задает вероятность возникновения i-ой кибератаки в течении промежутка времени Δt. Таким образом, нам фактически требуется задать $4n+1$ исходных параметров нашей модели, где n — количество рассматриваемых видов кибератак. Можно, однако, немного снизить число свободных параметров, если учесть, что всякая кибератака осуществляется с помощью эксплуатации некоторой уязвимости, присутствующей в системе, и использовать для оценки вероятностей появления кибератак общую систему оценки уязвимостей CVSS.

В работе был проведен эксперимент для гипотетической локальной сети организации с набором определенного оборудования. Для нее был определен перечень возможных угроз и уязвимостей, произведен расчет. В результате были получены графики зависимости среднего времени до отказа безопасности и среднего риска от вероятности отражения кибератак.

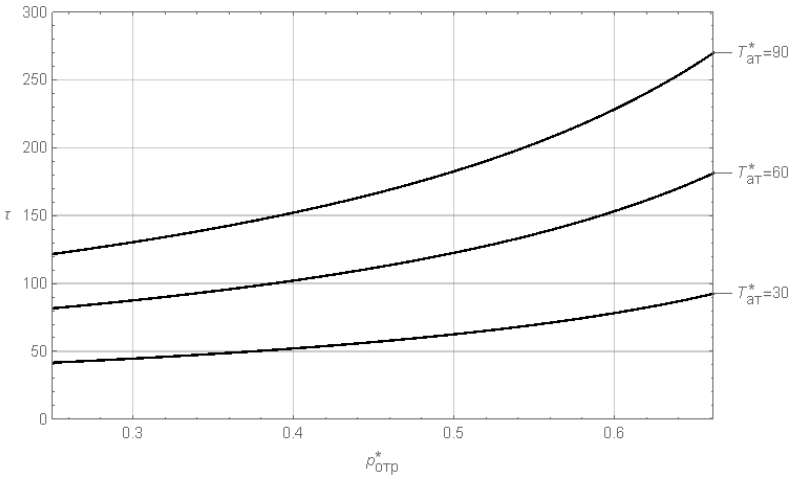


Рис. 4. График функции $\tau(p_{отр^*})$

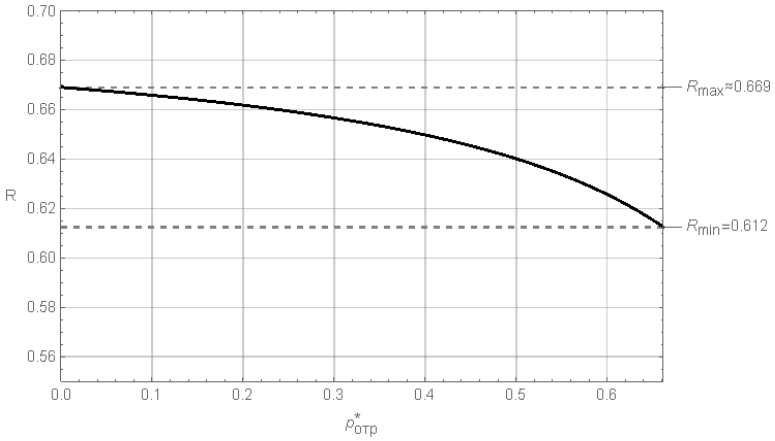


Рис. 5. График функции $R(p_{отр^*})$

На рис. 3 приведено несколько графиков функции $\tau(p_{отр^*})$ при различных значениях параметра $T_{AT}{}^*$. Видно, что при увеличении $T_{AT}{}^*$ среднее время до отказа безопасности увеличивается, так как увеличивается средний интервал между кибератаками. Время τ также быстро растет с увеличением $p_{отр}{}^*$: эффективность системы защиты приводит к удлинению среднего промежутка времени до отказа безопасности. Зависимость $\tau = \tau(p_{отр}{}^*)$ может быть использована на практике для установления минимального порогового значения $p_{отр}{}^*$, при которой метрика τ не будет меньшей заранее фиксированной начальной величины.

РЕАЛИЗАЦИЯ ПРОГРАММНОЙ ЧАСТИ

В исследовании реализованы и модифицированы несколько программных решений.

Для апробации модели и алгоритма сбора значимых данных реализовано программное обеспечение на языке программирования C# (рис. 6).

Программное обеспечение позволяет автоматизировать процесс оценки защищенности автоматизированной системы. В результате работы формируется отчет, в котором представлены результаты, позволяющие сделать выводы о наличии или отсутствии необходимости модификации системы защиты.

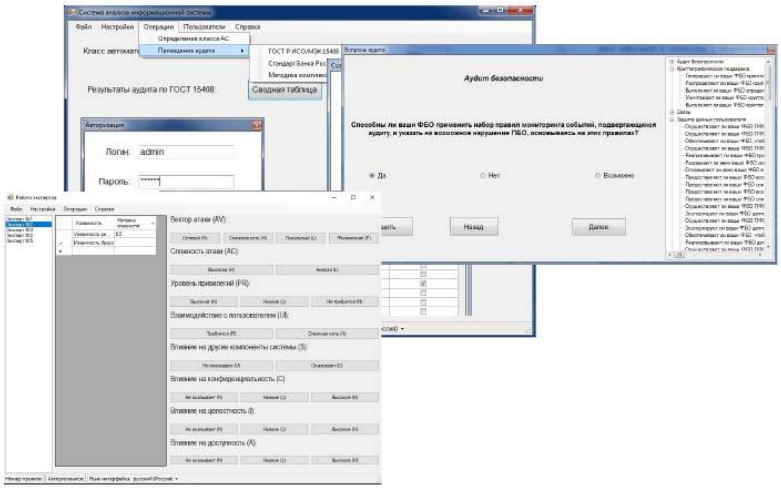


Рис. 6.Интерфейсы работы программного обеспечения

ЗАКЛЮЧЕНИЕ

Основные результаты работы заключаются в следующем:

1. Рассмотреная модель защиты информаци, сформулирована в терминах марковских процессов. Модель описывает функционирование информационной системы как последовательность отказов и восстановлений, которые возникают в следствии воздействии угроз безопансности.
2. В работе рассмотрены метрики безопасности, которые характерны для представленной модели.
3. Сформулированы оптимизационные задачи и представлен вариант их решения.
4. Сформулирован процесс формирования перечня угроз и уязвимостей с использованием стандарта CVSSv3.
5. Разработаны необходимые программные средства для апробации представленной модели и алгоритма сбора данных.
6. Результаты выполнения оценки уровня защищенности информационной системы доказывают его практическую значимость.

СПИСОК ЛИТЕРАТУРЫ

1. Альшанская, Т. В. Особенности экономических аспектов защиты информации на основе концепции инвестирования / Т. В. Альшанская, Н. В. Хри-пунов // Информационные системы и технологии: управление и безопасность. – 2016. – № 4. – С. 21–25.
2. Альшанская, Т. В. Экономические аспекты защиты информации / Т. В. Альшанская // Вестник Поволжского государственного университета сервиса. Сер. Экономика. – 2013. – № 6 (32). – С. 182–186.
3. Taylor, R. G. Potential Problems with Information Security Risk Assessments / R. G. Taylor. – https://doi.org/10.1080/19393555.2015.1092620 // Information Security Journal: A Global Perspective. – 2015. – Vol. 24, no. 4–6. – P. 177–184.
4. Kamenskih, A. N. The Development of Method for Evaluation of Information Security Threats in Critical Systems / A. N. Kamenskih, M. A. Filippov, A. A. Yuzhakov // 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic En-gineering (Saint Petersburg; Moscow, 27–30 January 2020) : proceedings. – Saint Pe-tersburg : IEEE, 2020. – P. 333–336.
5. Математическая модель оптимального выбора средств защиты от угроз безопас-ности вычислительной сети предприятия / А. И. Овчинников, А. М. Журавлев, Н. В. Медведев, А. Ю. Быков // Вестник Московского государственного техни-ческого университета им. Н. Э. Баумана. Сер. Приборостроение. – 2007. – № 3. – С. 115–121.
6. Shirtz, D. Optimizing investment decisions in selecting information security remedies / D. Shirtz, Y. Elovici. – https://doi.org/10.1108/09685221111143042 // In-formation Management & Computer Security. – 2011. – Vol. 19, no. 2. – P. 95–112.
7. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности : нац. стандарт Российской Федерации : утв. и введ. в действие Приказом Федер. агентства по техн.

регулированию и метрологии от 30 нояб. 2010 г. № 632-ст : дата введ. 2011-12-01 // КонсультантПлюс : справ.-правовая система. – Режим доступа: по подписке.
8. Дорофеев, А. В. Менеджмент информационной безопасности: основные концепции / А. В. Дорофеев, А. С. Марков // Вопросы кибербезопасности. – 2014. – № 1 (2). – С. 67–73.
9. Анализ информационной безопасности автоматизированных систем управления техническими процессами газодобывающего предприятия / А. А. Захаров, А. С. Римша, А. М. Харченко, И. Р. Зулькарнеев // Вестник УрФО. Безопасность в информационной сфере. – 2017. – № 3 (25). – С. 24–33.
10. Golnari, G. Markov fundamental tensor and its applications to network analysis / G. Golnari, Z.-L. Zhang, D. Boley. – https://doi.org/10.1016/j.laa.2018.11.024 // Linear Algebra and its Applications. – 2019. – Vol. 564. – P. 126–158.
11. Lalropuia, K. C. Modeling cyber-physical attacks based on stochastic game and Markov processes / K. C. Lalropuia, V. Gupta. – https://doi.org/10.1016/j.ress.2018.08.014 // Reliability Engineering & System Safety. – 2019. – Vol. 181. – P. 28–37.
12. Кашаев, Т. Р. Алгоритмы активного аудита информационной системы на основе технологий искусственных иммунных систем: специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность» : дис. ... канд. техн. наук / Т. Р. Кашаев. – Уфа, 2008. – 131 с.
13. Пащенко, А. Е. Применение байесовских сетей доверия для расчета относительных оценок показателей процессов, ассоциированных с риском, в условиях ин-формационного дефицита / А. Е. Пащенко // Труды СПИИРАН. – 2013. – № 8 (31). – С. 95–122.
14. Ahmad, I. Application of artificial neural network in detection of probing attacks / I. Ahmad, A. B. Abdullah, A. S. Alghamdi // IEEE Symposium on Industrial Electronics & Applications : proceedings (Kuala Lumpur, Malaysia, 4–6 Oct. 2009). – Kuala Lumpur : IEEE, 2009. – Vol. 2. – P. 557–562.
15. Применение методов теории нечетких множеств к оценке рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем управления / А. И. Братченко, И. В Бутусов, А. М. Кобелян, А. А. Романов // Вопросы кибербезопасности. – 2019. – № 1 (29). – С. 18–24.

Трепачева А.В.
ИКТИБ ЮФУ, м.н.с.,
alina1989malina@yandex.ru

РАЗРАБОТКА И ИССЛЕДОВАНИЕ АЛГОРИТМОВ ОЦЕНКИ КРИПТОСТОЙКОСТИ ГОМОМОРФНЫХ НАД КОЛЬЦОМ ШИФРОВ, ОСНОВАННЫХ НА ЗАДАЧЕ ФАКТОРИЗАЦИИ ЧИСЕЛ

Аннотация. Изучение гомоморфных криптосистем актуально в связи с их приложениями в облачных вычислениях. В работах последних лет были представлены гомоморфные криптосистемы с низкими вычислительными издержками, в которых пространство открытых текстов – кольцо вычетов по трудно факторизуемому модулю. Однако не были предоставлены обоснования их стойкости. Позднее был проведен анализ их стойкости к атаке с известными открытыми текстами и они оказались нестойкими к ней. Данная работа завершает серию работ по криптоанализу этих криптосистем анализом стойкости к атаке только по шифртекстам. Итог таков, что стойкость к атаке только по шифртекстам можно показать лищь для равномерного распределения на множестве открытых текстов, при этом есть сводимость к NP-трудной задаче факторизации.

Ключевые слова: гомоморфное шифрование, атака только по шифртекстам, задача факторизации.

Введение и актуальность темы исследования. Будем рассматривать алгебраически гомоморфное шифрование (АГШ), для которого пространство шифртекстов C и пространство открытых текстов P – алгебраические структуры с операциями сложения и умножения. Для $\forall c_1, c_2 \in C$ выполняется $Dec(c_1 * c_2) = Dec(c_1) \circledast Dec(c_2)$, где $*$ – одна из двух операций на множестве C, соответствующая операции $\circledast$ на P, Dec – отображение расшифрования. P – обычно кольцо вычетов $\mathbb{Z}_t$, а C не обязательно кольцо. Особенно интересно полностью гомоморфное шифрование (ПГШ), позволяющего эффективно вычислять над шифртекстами любой полином. Идея ГШ впервые была сформулирована в [1]. С помощью ГШ клиент может делегировать вычисления над данными облачному серверу, не раскрывая данные.

Основное направление в области ПГШ – разработка ассиметричных схем с доказуемой стойкостью против атаки по выбранным открытым текстам (АВОТ). Основателем является Джентри [2]. Для получения ПГШ Джентри предлагает проводить самокоррекцию (bootstrapping). Она индуцирует сложную операцию умножения на C, так что оно перестает быть кольцом. Низкая эффективность ПГШ типа Джентри препятствует внедрению на практике [3].

Продолжаются попытки построить альтернативные эффективные схемы ПГШ [4-10]. Чаще всего они симметричны, в них C – коммутативное кольцо. Но для большинства из них отсутствует обоснование стойкости. Уже показано, что все они нестойки к атаке с известными открытыми текстами (АИОТ). Пока открыт вопрос о стойкости к атаке только по шифртекстам (АТШ).

Отметим, что уже есть общие результаты, показывающие, что при определенном наборе свойств кольца C и $P = \mathbb{Z}_2$ невозможно построить стойкую против АВОТ ассиметричную схему ПГШ [11]. В связи с этим возникает вопрос: существует ли P для которого можно построить стойкую ПГШ, у которой C – кольцо.

Цели и задачи работы. Мы анализируем стойкость подмножества вероятностных симметричных схем АГШ, построенных без применения метода Джентри. В них $P = \mathbb{Z}_n$, где n – трудно факторизуемое число, C – кольцо. Этот класс криптосистем обозначим как $HomSymRing_n$.

Основные задачи:

1) Создание общей методологии оценки стойкости шифров из класса $HomSymRing_n$ против АИОТ и АТШ.

2) Исследование связей между АТШ ик АИОТ. Установление возможности построения полиномиального от $\log(n)$ алгоритма, который сводит АТШ к АИОТ.

3) Установление возможности построения эффективно вычислимых полиномиальных функций с компактным образом для $\mathbb{Z}_n$ по труднофакторизуемому модулю n, что означает эквивалентность АТШ и АИОТ для ГШ из $HomSymRing_n$.

4) Разработка программного комплекса, который при подаче на вход формализованного описания схемы ПГШ, автоматически провел бы анализ и выдал бы вердикт об уровне стойкости конструкции.

5) Выработка практических рекомендаций для построения и эксплуатации криптосистем из $HomSymRing_n$.

Теоретическая и практическая значимость работы. Схемы ПГШ из $HomSymRing_n$, интересны, т.к. они на практике могут быть эффективнее, чем ПГШ Джентри. Важно понимать уровень стойкости, чтобы определить для каких приложений их применение допустимо. Полезно получить универсальные программные средства для оценка стойкости новых криптосистем из этого класса.

Криптосистемы из $HomSymRing_n$ интересны тем, что при попытке исследования их стойкости возникает вопрос о связи с задачей факторизации. Вопрос о возможности построения вероятностной схемы ПГШ, чья криптостойкость сводилась бы к ней, поставлена в [1]. Данное исследование может помочь пролить свет на этот вопрос.

Степень разработанности темы. Идею об обработке данных в зашифрованном виде впервые высказали в [1]. Были предложены примеры шифров, обладающие мультипликативными и/или аддитивными алгебраическими свойствами. Но все они оказались нестойкими к АИОТ, а некоторые и к АТШ. Алгоритм их взлома описаны в [12].

Говоря о ГШ из $HomSymRing_n$ стоит упомянуть [13], в которой задались вопросом, существуют ли детерминированные схемы АГШ над $\mathbb{Z}_n$, взлом которых эквивалентен факторизации n. Было введено понятие инкапсулированного представления кольца (ИПР).

Определение ([13]). Пусть (R, +, ·) – конечное кольцо, S – конечное множество битовых строк, где $|S|=|R|$. Набор (σ, O), состоящий из случайно выбранной кодирующей биективной функции σ: $R \to S$ и оракула O закрытого кольца, вычисляющего по паре кодировок $\sigma(r_i)$ и $\sigma(r_j)$ их сумму $\sigma(r_i + r_j)$ или произведение $\sigma(r_i \cdot r_j)$, называется ИПР для R и обозначается R^σ.

ИПР моделирует ПГШ над $\mathbb{Z}_n$. Из результатов, полученных в [13], следует, что теоретически может существовать ПГШ над $\mathbb{Z}_n$, стойкость которого к АИОТ эквивалентна факторизации n. Однако моделирование ПГШ с помощью ИПР абстрактно. Не учитывается сложность σ и O. На практике подходят лишь схемы, у которых σ и O имеют разумную вычислительную сложность. Это не учтено в [13].

Рассмотрим схемы из $HomSymRing_n$ и основные результаты анализа их стойкости. Здесь и далее $P = \mathbb{Z}_n$, где $n = p \cdot q$ – трудно факторизуемое число, p и q – простые числа, $p < q$, C – кольцо. Начнем с АГШ DF96 из [4]. Здесь $C \subset \mathbb{Z}_p[x] \times \mathbb{Z}_q[x]$, пространство ключей $K = \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Чтобы зашифровать $m \in \mathbb{Z}_n$, генерируются случайно $d-1$ чисел $a_2, \dots, a_d \in \mathbb{Z}_n$, $a_d \neq 0$, вычисляется $a_1 = m - a_2 - \dots - a_d$, и $a(x) = a_d \cdot x^d + \dots + a_1 \cdot x \in \mathbb{Z}_n[x]$. Шифртекст – пара $(c_p(x), c_q(x))$, $c_p = a(r_p \cdot x) mod\ p$, $c_q = a(r_q \cdot x) mod\ q$, $(r_p, r_q) \in K$ – секретный ключ. Разложение числа n также часть секрета. Для расшифрования вычисляют $m_p = c_p(r_p^{-1}) mod\ p$ и $m_q = c_q(r_q^{-1}) mod\ q$. Из них по Китайской теореме об остатках восстановим m. В [14] показано, что DF96 не стойка к АИОТ. Для взлома необходимо $d+1$ пар (открытый текст, шифртекст). В [15] было показано, что достаточно 2-х пар.

В [6] предложена схема ZZK13. Здесь $P = \mathbb{Z}_n$, где n может быть простым или составным. Шифровкой m является $c(x) \in \mathbb{Z}_n[x]$, где $c(k) = m$, $k \in \mathbb{Z}_n$ – секретный ключ. В [7] предложен похожий вариант ПГШ RM11, где $P = \mathbb{Z}_n$, $C = \mathbb{Z}_n[x]/(f(x))$, $n = p \cdot q$ – трудно факторизуемое число, $f(x) \in \mathbb{Z}_n[x]$ – полином, имеющий корень секретный ключ $k \in \mathbb{Z}_n$. В [16] показано, что при наличии нескольких пар (открытый текст, шифртекст) вычисление НОД позволит вычислить секретный ключ. В [17] был проведен анализ их стойкости к АТШ. Методы криптоанализа, описанные в [17], опираются на алгоритмы декомпозиции и факторизации полиномов. Показано, что если вероятностное распределение Ψ на P сильно отлично от равномерного, то вероятность взлома близка к 1.

В [9] описали схему ПГШ SBKAS14. В ней $n = p \cdot q$ – труднофакторизуемое число, $P = \mathbb{Z}_p$, $C = \mathbb{Z}_n[x]$, ключ – $\{p, u(x)\}$, где $u(x) \in \mathbb{Z}_p[x]$ – неприводимый степени d. Для шифрования генерируется случайный неприводимый $s(x)$ степени d и случайный $r(x)$ степени $2d-1$. Шифртекст выглядит так: $c(x) = [s(x) \cdot u(x) + p \cdot r(x) + m]\ mod\ n$.В [18] показано, что SBKAS14 нестойка к АИОТ. Нужно иметь 2 пары $(m_i, c_i(x)), i = 1,2$ для раскрытия ключа. Также был проведен анализ стойкости к АТШ для неравномерного Ψ.

В [8, 10] описаны матричные схемы ПГШ MORE и XBY12, в которых C – кольцо матриц. Открытый текст $m \in \mathbb{Z}_n$ отображается в $D \in \mathbb{Z}_n^{k \times k}$ так, что m – собственное число D. Ключ – обратимая матрица $K \in \mathbb{Z}_n^{k \times k}$. Шифртекст – $c = K^{-1} \cdot D \cdot K$. В [19 - 21] показано, что это шифрование нестойко АИОТ. В [22] приведен анализ стойкости данного типа схем к АТШ. Показано, что при неравномерном Ψ, конструкция уязвима к АТШ.

В литературе уделялось внимание анализу стойкости схем ПГШ из $HomSymRing_n$ относительно АИОТ. Все конструкции нестойки к ней в отличие от схем ПГШ типа Джентри. Остается вопрос о стойкости $HomSymRing_n$ к АТШ, который здесь необходимо рассматривать. В литературе был освещен вопрос о стойкости к АТШ для неравномерного Ψ, но в общем случае стойкость не исследована.

Интересен вопрос о сводимости АТШ к АИОТ для $HomSymRing_n$, т.к. для ГШ часто по произвольному шифртексту можно создать шифртекст заданного открытого текста. Сводимость АТШ → АИОТ для $HomSymRing_n$ не изучалась ранее.

Научная новизна. Ранее не исследовалась стойкость к АТШ криптосистем из $HomSymRing_n$. Новой является постановка вопроса о возможности сводимости между атаками на криптосистемы данного класса.

Основные положения, выносимые на защиту.

1. Для криптосистем из $HomSymRing_n$ есть сводимость стойкости к АТШ к задаче факторизации n для равномерного Ψ.
2. В общем случае нет сводимости АТШ к АИОТ для $HomSymRing_n$. Несмотря на ее отсутствие, гомоморфную над кольцом криптосистему можно дерандомизировать, т.е. свести к шифру простой замены, если шифртексты этой криптосистемы образуют кольцо и Ψ отлично от равномерного.
3. Проведенный анализ известных результатов об АГШ не является обнадеживающим. Построить стойкую гомоморфную криптосистему на основе колец невозможно в случае, если P является подкольцом C. Но можно себе представить стойкую криптосистему, в которой $P = \mathbb{Z}_2$, $C = \mathbb{Z}_n$, где n — труднофакторизуемое число.

Краткое содержание диссертации.

1. Анализ стойкости к АИОТ. Приведем обзор основных результатов по анализу стойкости криптосистем из $HomSymRing_n$ к АИОТ. В [15] показано, что DF96 уязвима к АИОТ. Предположим, что есть пары $(m_i, \left(c_{p,i}(x), c_{q,i}(x)\right), i = 1{,}2$, изготовленные на одном ключе. Тогда $f_i(x) = c_{p,i}(x) - m_i \in \mathbb{Z}_n[x], i = 1{,}2$ имеют общий корень r_p^{-1} по модулю p. Вероятность того, что они имеют общий корень по модулю q пренебрежимо мала. Значит с вероятностью ~1 результант $\theta = Res(f_1(x), f_2(x))$ таков, что $\theta = p \cdot w$. Противник найдет p, вычислив НОД(θ, n). Далее он вычислит $f_i^p(x) = f_i(x) mod\ p \in \mathbb{Z}_p[x], i = 1{,}2$. Посчитав НОД$(f_1^p(x), f_2^p(x))$, можно определить r_p^{-1} вероятностью ~1. Алгоритм определения r_q^{-1} аналогичен.

Рассмотрим ZZK13. Здесь $P = \mathbb{Z}_n$, где n может быть простым или составным числом. Для шифрования m генерируется случайный $\sigma(x) \in P[x], \sigma(0) = m$. Секретным ключом является $k(x) \in P[x]$. Шифртекст – $c(x) = \sigma(k(x))$. Для расшифрования вычисляют $m = c(a)$, где a – корень $k(x)$. Также в [7] предложил очень похожий вариант ПГШ RM11, но здесь $P = \mathbb{Z}_n$, $C = \mathbb{Z}_n[x]/(f(x))$, $n = p \cdot q$– трудно факторизуемое число, $f(x) \in \mathbb{Z}_n[x]$ – полином, имеющий корень $k \in \mathbb{Z}_n$ – секретный ключ

В [16] ZZK13 и RM11 были проанализированы на стойкость к АИОТ. Ясно, что здесь для пары $(m, c(x))$ выполнится $c(x) - m = k(x) \cdot \delta(x)$, где $\delta(x)$ – случайный, $k(x)$ – секретный ключ. Необходимо иметь 2 пары $(m_i, c_i(x)), i = 1{,}2$. Тогда $g_i(x) = c_i(x) - m_i, i = 1{,}2$ имеют общий множитель кратный $k(x)$. При $n < 100$ достаточно 5 пар, чтоб найти ключ. А для большого n НОД$(g_1(x), g_2(x)) = k(x)$ с вероятностью ~ 1.

Рассмотрим SBKAS14. В [18] показано, что SBKAS14 нестойка к АИОТ. Необходимо иметь 2 пары $(m_i, c_i(x)), i = 1{,}2$. Тогда $g_i(x) = c_i(x) - m_i, i = 1{,}2$ имеют общий множитель по модулю p. Тогда НОД$(\mathrm{Res}(g_1(x), g_2(x)), n) = p$ с вероятностью ~ 1. С вероятностью ~ 1 можно найти $u(x)$, вычислив НОД$(g_1(x), g_2(x))$ по модулю p.

2. Анализ сводимости АТШ к АИОТ. Для любой криптосистемы есть сводимости: АИОТ → АТШ, АВОТ → АИОТ. Но для ГШ могут быть обратные сводимости. Исследование сводимости АТШ → АИОТ для $HomSymRing_n$ может дать ответ на вопрос остойкости к АТШ. Рассмотрим сводимость для ZZK13 в случае $P = \mathbb{Z}_p$, p – простое. Пусть противник имеет $c_1(x), \dots, c_s(x)$, изготовленные на $k(x)$, и знает p. Он вычислит $c_i'(x) = (c_i(x))^p - c_i(x)$, $i = 1, \dots, s$, это даст ему пары для АИОТ $(0, c_1'(x)), \dots, (0, c_s'(x))$, где $c_i'(x) = k(x) \cdot r_i(x) \cdot ((k(x) \cdot r_i(x))^{p-1} - 1)$, $c_i'(x)$ кратно $x^p - x$ для $\forall k(x), r_i(x)$. АТШ на ZZK13 формализована в виде *Алгоритма 1*. ZZK13 некомпактна, т.к. при умножении размеры шифровок растут с экспоненциальной скоростью. Поэтому для больших p атака не эффективна.

Алгоритм 1 COA1($c_1, \dots, c_t$)

Вход: «свежие» шифртексты $c_1(x), \dots, c_s(x)$ ZZK13, простое число p
Выход: $k(x)$ или его множитель
1: **for** *i=1* to *s* **do**
2: $c_i^*(x) := (c_i(x))^p - c_i(x)$
3: **end**
4: **return** НОД$(c_1^*(x), \dots, c_s^*(x))/(x^p - x)$
5: **end**

Для $P = \mathbb{Z}_n$, где n – составное число, можно использовать $f(x) = x^{\varphi(n)} - x$. Если n трудно факторизуемо, то вычислить $\varphi(n)$ трудно. Но если противник без знания разложения найдет над $\mathbb{Z}_n$ эффективно вычислимую полиномиальную функцию, имеющую областью значений подмножество $\mathbb{Z}_n$, мощность которого $\log(n)$, то он сведет АТШ к АИОТ. Основная гипотеза заключается в том, что если можно построить такую функцию, то можно доказать, что нет отличий в требованиях, предъявляемых к гомоморфным криптосистемам: все должны выдерживать АИОТ.

Алгоритм 2 COA2($c_1, \dots, c_s$)

Вход: шифртексты $c_1, \dots, c_s$ криптосистемы; функция f.
Выход: секретный ключ sk в случае успешной атаки
1: **for** *i=1* to *s* **do**
2: $c_i^* := f(c_i)$
3: **end**
4: **for** $(p_1, \dots, p_s) \in Im(f) \times \dots \times Im(f)$ **do**
5: sk′ = АИОТ $((p_1, c_1^*), \dots, (p_s, c_s^*))$
5: **if** АИОТ $((p_1, c_1^*), \dots, (p_s, c_s^*))$ прошла успешно **then**
6: sk = Normalize(sk′)
7: **return** sk
8: **end**
9: **end**

Определение. Назовем функцию $f: P \to P$ σ *- логарифмически сжимающей*, если $|\mathrm{Im}(f(P))| < \sigma \cdot \log_2 |P|$, т.е. количество элементов в её образе $\leq \sigma \cdot \log_2 |P|$, $\sigma \in \mathbb{R}$, $\sigma \ll |P|$.

Теорема ([23]). Если существует алгоритм, работающий на всех входах за $O(\log n)$ шагов, который при $P = \mathbb{Z}_n$ для некоторой схемы АГШ, и некоторого σ выдает эффективно вычислимую σ - логарифмически сжимающую функцию $f: \mathbb{Z}_n \to \mathbb{Z}_n$, то АТШ и АИОТ на эту ГШ эквивалентны.

Вопрос об эквивалентности АТШ и АИОТ можно свести к поиску семейства сжимающих функций над $\mathbb{Z}_n$. И, забегая вперед, скажем, что сводимости в общем случае нет и функций с желаемыми свойствами без знания факторизации построить нельзя. Если распределение Ψ близко к равномерному, то сводимости нет.

Если Ψ отлично от равномерного, то, воспользовавшись гомоморфными свойствами, можно свести АТШ к АИОТ. Рассмотрим сводимость на примере SBKAS14. Предположим, атакующий перехватил $\{c_i(x) = [s_i(x) \cdot u(x) + p \cdot r_i(x) + m_i] mod\ n\}, i = 1..t$. Он вычисляет $c_{i,j}(x) = \left[c_i(x) - c_j(x)\right] mod\ n$ для $\forall i, j, i \neq j$, где $c_{i,j}(x)$ шифрует $[m_i - m_j] mod\ p$. Если в последовательности $\{m_i\}, i = 1..t$ существуют $m_i, m_j | m_i = m_j, i \neq j, c_i(x) \neq c_j(x)$, то $c_{i,j}(x)$ будет шифровать ноль. При наличии ключа вычисления $w(x)$, где $w(x) = [s(x) \cdot u(x) + p \cdot r(x)] mod\ n$, можно атаковать SBKAS14 описанным ранее способом. Атакующий вычисляет $\delta_{i,j} = Res(c_{i,j}(x), w(x)) = \left[c_i(x) - c_j(x)\right] mod\ n$ и НОД$(\delta_{i,j}, n)$ до тех пор, пока не получит НОД $\neq 1, n$. Если получен нетривиальный НОД, то найден p и можно найти $u(x)$. Вероятность успеха можно оценить по формуле:,

$$\eta_t = \Pr\left[\exists m_i, m_j \middle| m_i = m_j, i \neq j\right] = 1 - \prod_{m=0}^{p-1}\left(\left(1 - \Pr_{\psi}[m]\right)^t + t \cdot \left(1 - \Pr_{\psi}[m]\right)^t \cdot \Pr_{\psi}[m]\right).$$

Вероятность η_t может быть ≈ 1 при небольших t (около 100) и Ψ, являющимся дискретным Гауссовым распределения $D_{n,\mu.\sigma^2}$ с небольшой дисперсией. В случае неравномерного Ψ эта стратегия работает для всех криптосистем из $HomSymRing_n$.

3. Анализ стойкости против АТШ.

Задача (Взлома DF96*).* Пусть противник A владеет шифровками $c_1 = \left(c_{p,1}(x), c_{q,1}(x)\right), \dots, c_l = \left(c_{p,l}(x), c_{q,l}(x)\right) \in \mathbb{Z}_n[x] \times \mathbb{Z}_n[x]$, созданными на ключе $k = (r_p, r_q) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ при параметре d. Задача $COA_{DF,d}(c_1, \dots, c_l)$ состоит в том, чтобы раскрыть k.

Лемма. $\forall f(x) \in \mathbb{Z}_n$[x] степени d можно мыслить как первую (вторую) координату шифртекста DF96.

Доказательство. Выберем случайный $k_p \in \mathbb{Z}_n$, $k_p < n/2$. Проверяем, что k_p взаимнопрост с n. Если нет, раскрыли факторизацию. Если да, считаем, что k_p – первая координата ключа DF96, шифрующая $m \in \mathbb{Z}_n$, который по модулю p равен $f(k_p^{-1})$. □

Теорема. Если A проводит μ ($\mu \le n$) операций с шифртекстами DF96 и решает $COA_{DF,d}(c_1, \dots, c_l)$ с вероятностью ε, то существует алгоритм B, который, имея открытый доступ к A, находит сомножитель n за m операций с шифртекстами с вероятностью ε.

Доказательство. Криптоаналитик – алгоритм A, который на каждом шаге совершает одну из операций: алгебраическая операция $\circ \in \{+, -, \cdot\}$ в $\mathbb{Z}_n[x]$, вычисление НОДа в $\mathbb{Z}_n[x]$. Будем работать по 1-й координате. A инициализирует список полиномов L = $\{c_{p,1}, \dots, c_{p,l}\}$. Далее над L проводит операции. На каждом шаге A достраивает L: A выбирает два индекса $1 \le i, j \le |$ L $|$ и вычисляет $\circ \in \{+, -, \cdot\}$, получая $c_{p,i+j}(x) = c_{p,i}(x) \circ c_{p,j}(x)$. $c_{p,i+j}(x)$ добавляется в конец L. Запускается алгоритм на обновленном L:

- Перебираем в цикле всевозможные отличные друг от друга пары $(c_{p,i}(x), c_{p,j}(x)), 1 \le i, j \le |L| - 1$ и $(c_{p,z}(x), c_{p,|L|}(x)), 1 \le z \le |L| - 1$. Вычисляем $\theta = Res(c_{p,i}(x) - c_{p,j}(x), c_{p,|L|}(x) - c_{p,z}(x))$. Если $c_{p,i}$ и $c_{p,j}$ шифруют один открытый текст, и $c_{p,z}$ и $c_{p,|L|}$ так же шифруют один открытый текст, то $c_{p,i}(x) - c_{p,j}(x)$ и $c_{p,|L|}(x) - c_{p,z}(x)$ имеют общий корень по модулю p. Тогда НОД(θ, n)=p.
- Вычисляется b=НОД(θ, n). И проверяется условие: *1 < b < n?* Если условие выполнено, значит $b = p$, тривиально вычисляем r_p и выходим из цикла.

Предположим, что A делает τ шагов, так что $|\mathrm{L}| = l + \tau$. Тогда общее число операций μ с шифртекстами $\le \tau \cdot (l + \tau) \cdot (l + \tau - 1)^2/2$. Если A с преимуществом ε за операций μ находит секретный ключ DF96, то он раскрывает факторизацию n за операций μ с преимуществом ε.

Алгоритм B *факторизации n.*

Дано: n, d.

- Генерируем случайные $c_1(x), \dots, c_l(x) \in \mathbb{Z}_n[x]$ степени d. Их можно мыслить как первые координаты шифртекстов DF96.
- Запускаем на $c_1(x), \dots, c_l(x)$ алгоритм A. □

A опирается на то, что в DF96 есть встроенный оракул $\mathcal{O}^=$, позволяющий проводить тест на равенство. $\mathcal{O}^=$ получает на вход 2 пары $(c_i(x), c_j(x))$ и $(c_l(x), c_k(x))$ и отвечает на вопрос: $c_i(x), c_j(x)$ шифруют одно и тоже и $c_l(x), c_k(x)$ шифруют одно и тоже?

Когда строится алгоритм факторизации, он должен иметь возможность генерировать шифртексты для данного n. Исходя из леммы, сгенерировав по равномерному распределению $c_1(x), \dots c_l(x)$, мы можем мыслить их как первые координаты шифртекстов DF96. При этом распределение Ψ будет равномерным. Сводимость от $COA_{DF,d}(c_1, \dots, c_l)$ к задаче факторизации будет справедлива только для равномерного Ψ.

Пусть A перехватил последовательность шифровок DF96 для некоторых n, d и известно, что Ψ сильно отличается от равномерного. Тогда на основе алгоритма, представленного в доказательстве, мы получаем алгоритм взлома DF96.

Теорема. Пусть у A есть шифртексты $c_1, \dots, c_l$. Знание факторизации n не дает преимущества в раскрытии $k = (r_p, r_q) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

Доказательство. Имеем $c_i = \left(c_{p,i}(x), c_{q,i}(x)\right) \in \mathbb{Z}_n[x], i = 1..l$. Будем работать с 1-й координатой шифртекстов. Поскольку p известно, то можем вычислить $g_i(x) = c_{p,i}(x) mod\, p \in \mathbb{Z}_p[x], i = 1..l$. Для любого $0 < \kappa < p$ $g_i(x)$ можно мыслить как половину шифровки открытого текста, который по модулю p равен $a_{i,\kappa} = g_i(\kappa^{-1}) mod\, p$ на ключе κ. Знание факторизации не влияет на возможность разрешить данную неопределенность. Единственный шанс решить ее будет в случае, если Ψ сильно отличается от равномерного. Ниже представлен алгоритм, похожий на описанный ранее. Если $g_i(x)$ и $g_j(x)$ шифруют один и тот же открытый текст по модулю p на r_p, то $g_i(x) - g_j(x)$ имеет корень r_p^{-1}, т.е. нетривиальный НОД равный $x - r_p^{-1}$. Далее можно запустить следующий алгоритм:

- Перебираем в цикле разные пары $(g_i(x), g_j(x)), 1 \le i,j \le l$ и $(g_z(x), g_t(x)), 1 \le z,t \le l$. Если $g_i(x)$ и $g_j(x)$ шифруют один открытый текст, и $g_z(x)$ и $g_t(x)$ так же шифруют один открытый текст, то $\delta_{i,j,z,t}(x) = \text{НОД}(g_i(x) - g_j(x), g_z(x) - g_t(x)) \in \mathbb{Z}_p[x]$ нетривиален и делится на $x - r_p^{-1}$. Если $\delta_{i,j,z,t}(x)$ нетривиален, то сохраняем его в список Г.
- Считаем НОД δ всех полученных полиномов из Г. Если НОД равен 1, то надо исключить случайный полином из Г и снова посчитать НОД для редуцированного Г. Если удается найти нетривиальный δ, то его можно объявить ключом.

Алгоритм хорошо работает только, если Ψ отлично от равномерного. На успех никак не влияет знание факторизации n. □

Перейдем к SBKAS14. Здесь справедливы аналогичные результаты. Сейчас нет доказательства, что для $\forall d\ f(x) \in \mathbb{Z}_n[x]$ степени $2d$ представим в виде $[\tilde{s}(x) \cdot u(x) + p \cdot \tilde{r}(x) + \tilde{m}] \mod n$, где $\tilde{s}, u$ – неприводимые степени d из $\mathbb{Z}_p[x]$. Но в [9] не наложены ограничения на d. При $d = 2$ это свойство выполнится.

Лемма. Произвольный $f(x) \in \mathbb{Z}_n[x]$ степени 2 с младшим коэффициентом равным 1 можно представить в виде $[s(x) \cdot u(x) + p \cdot r(x) + m]$.

Задача (Взлома криптосистемы SBKAS14*).* Пусть А владеет шифртекстами $c_1(x), \dots, c_l(x) \in \mathbb{Z}_n[x]$ SBKAS14, созданными на ключе $k = (p, u(x))$ при фиксированном d. Задача $COA_{SBKAS,d}(c_1, \dots, c_l)$ состоит в том, чтобы раскрыть k.

Теорема. Если А проводит μ (μ ≤ n) операций с шифртекстами SBKAS14 и решает $COA_{SBKAS,d}(c_1, \dots, c_l)$ с вероятностью ε, то существует алгоритм В, имеющий открытый доступ к А, который находит сомножитель n за μ операций с вероятностью ε.

Доказательство этой теоремы похоже на доказательство, приведенное выше для DF96. Оно также опирается на то, что для SBKAS14 есть встроенный оракул $\mathcal{O}^{=}$. Алгоритм факторизации строится аналогичным образом. Сводимость от $COA_{SBKAS,d}(c_1, \dots, c_l)$ к задаче факторизации n здесь также справедлива только для равномерного Ψ.

Теорема. Предположим А имеет шифртексты $c_1(x), \dots, c_l(x)$. Знание факторизации числа n не дает преимущества в раскрытии часть секретного ключа $u(x)$.

Доказательство аналогично доказательству приведенному выше для DF96.

Рассмотрим ZZK13 при $P = \mathbb{Z}_n$, где $n = p \cdot q$ – трудное для факторизации. Представим обоснование стойкости к АТШ для равномерного Ψ. Покажем, что есть сводимость от задачи раскрытия секретного ключа ZZK13 к задаче факторизации n. Будем работать в кольцевой модели (КМ). КМ рассматривает алгоритмы, построенные из последовательности операций кольца и не использующие свойства представления элементов кольца. Известен результат, что взлом RSA эквивалентен разложению на множители числа n именно в КМ [24].

Доказательство сводимости в КМ не есть сильный индикатор сложности вычислительной задачи в стандартной модели. В [25] показано, что в КМ вычисление символа Якоби эквивалентно факторизации. Но в стандартной модели это не выполняется. Несмотря на это общие результаты сложности в КМ по-прежнему интересны, т.к. обеспечивают оценку сложности для большого класса алгоритмов. Рассмотрим расширение КМ. Разрешено выполнять стандартные операции $(+, \cdot, -)$ в $\mathbb{Z}_n[x]$ и деление с остатком. Полагаем также, что у А есть неограниченный доступ к оракулу $\mathcal{O}_{\text{k}}^{=}$, который проверяет шифруют ли 2 шифртекста один и тот же открытый текст.

Задача (Взлома криптосистемы ZZK13). Пусть А владеет шифртекстами $c_1(x), \dots, c_l(x) \in \mathbb{Z}_n[x]$ криптосистемы ZZK13, созданными на ключе $k \in \mathbb{Z}_n$, и может делать запросы к $\mathcal{O}_{\text{k}}^{=}$. Задача $COA_{ZZK}(\mathcal{O}_{\text{k}}^{=})$ состоит в том, чтобы раскрыть $k \in \mathbb{Z}_n$.

Теорема. Если А проводит μ (μ ≤ n) алгебраических операций с шифртекстами криптосистемы ZZK13 и решает $COA_{ZZK}(c_1(x), \dots, c_l(x), \mathcal{O}_{\text{k}}^{=})$ с вероятностью ε, то существует алгоритм В, который, имея открытый доступ к $\mathcal{A}$, находит сомножитель n с вероятностью $\frac{\varepsilon - \frac{1}{\text{n}}}{(\mu+2)\cdot(\mu+1)}$.

Доказательство. А инициализирует L = $c_{-1}(x), c_0(x), c_1(x), \dots, c_l(x)$, где $c_{-1}(x) = 1$, $c_0(x) = x$, который далее пополняет по мере проведения операций так, что в конце работы алгоритма с μ шагами список будет состоять из $2 + l +$ μ полиномов. На s-м шаге А выбирает два индекса $-1 \le i, j \le l + s - 1$ и операцию $\circ \in \{+, -, \cdot\}$, получая $c_{l+s}(x) = c_i(x) \circ c_j(x)$. $c_{l+s}(x)$ добавляется в конец L. А делает запросы к оракулу $\mathcal{O}_{\text{k}}^{=}(c_j(x), c_{l+s}(x))$, $-1 \le j \le l + s - 1$ до тех пор, пока не встретит $c_j(x)$ такой, что

ответ будет true, или пока не закончится L. Если $c_j(x)$ найден, то пара $(c_j(x), c_{l+s}(x))$ сохраняется отдельно. Далее нужно найти хотя бы еще одну пару. Тогда можно найти ключ, посчитав НОД.

Рассмотрим оракул $\mathcal{O}^{=}_{\mathrm{sym}}$, который «не знает» k и действует так: при получении запроса $\mathcal{O}^{=}_{\mathrm{sym}}(c_s(x), c_t(x))$ выбирает случайный элемент $\rho \in \mathbb{Z}_n$ и возвращает результат проверки $(c_1 - c_2)(\rho) = 0\ (mod n)$?. Оракулы $\mathcal{O}^{=}_{\mathrm{k}}$ и $\mathcal{O}^{=}_{\mathrm{sym}}$ в большинстве случаев выдают false, пока не случится ошибка имитации F, т.е. для некоторых i, j случится:

$$((c_i - c_j)(\mathrm{k}) \neq 0\ (mod n) \wedge (c_i - c_j)(\rho) = 0\ (mod n))\ \vee$$
$$\vee\ ((c_i - c_j)(\mathrm{k}) = 0\ (mod n) \wedge (c_i - c_j)(\rho) \neq 0\ (mod n)) = true. \quad (1)$$

A может заметить разницу между $\mathcal{O}^{=}_{\mathrm{k}}$ и $\mathcal{O}^{=}_{\mathrm{sym}}$ только в случае F. Пусть S событие успешного нахождения k алгоритмом A при работе с $\mathcal{O}^{=}_{\mathrm{k}}$, а S_{sym} – с $\mathcal{O}^{=}_{\mathrm{sym}}$. Если F не случится, то A не заметит разницу, имеем $\mathrm{S} \wedge \mathrm{F} \Leftrightarrow \mathrm{S}_{sym} \wedge \mathrm{F}$ и получим верхнюю оценку на Pr[S], оценив $\Pr[\mathrm{S}_{sym}]$ и Pr[F].

Лемма («Разностная лемма») из [26]). Пусть E1, E2 и E3 – события из объемлющего пространства событий. Если $\mathrm{E1} \wedge \mathrm{E3} \Leftrightarrow \mathrm{E2} \wedge \mathrm{E3}$, то: $|\Pr[\mathrm{E1}] - \Pr[\mathrm{E2}]| \leq \Pr[\mathrm{E3}]$.

Имеем $\Pr[\mathrm{S}] - \Pr[\mathrm{S}_{sym}] \leq \Pr[\mathrm{F}]$. Т.к. $\mathcal{O}^{=}_{\mathrm{sym}}$ независим от k, то $\Pr[\mathrm{S}_{sym}] \leq 1/|\mathbb{Z}_n| = 1/n$. Оценим Pr[F]. Рассмотрим $\mathcal{D} = \{c_i(x) - c_j(x) \mid 1 \leq i < j \leq l + m\}$. Для $\delta(x) \in \mathcal{D}$ обозначим F_δ событие, что для $\delta(x)$ выполняется (1). Пусть D_δ обозначает событие, что НОД$(n, \delta(a)) \neq 1$, где $a \in \mathbb{Z}_n$ случаен.

Лемма. Для $\forall \delta \in \mathcal{D}$ справедливо $2\Pr[\mathrm{D}_\delta] > \Pr[\mathrm{F}_\delta]$.

Доказательство. Пусть $n = p \cdot q$, где $p \neq q,\ p, q$ – простые числа. По Китайской теореме об остатках для $a \in_U \mathbb{Z}_n$ выполняется:

$$\Pr[\delta(\mathrm{a}) \equiv 0\ mod\ n] = \Pr[\delta(\mathrm{a}) \equiv 0\ mod\ p \wedge \delta(\mathrm{a}) \equiv 0\ mod\ q] =$$
$$= \Pr[\delta(\mathrm{a}) \equiv 0\ mod\ p] \cdot \Pr\ [\delta(\mathrm{a}) \equiv 0\ mod\ q] = \nu_p \cdot \nu_q,$$

где $\nu_h = \frac{|\{a \in \mathbb{Z}_n | \delta(a) \equiv 0 mod h\}|}{n}, h = p, q.$

Оценим $\Pr[\mathrm{F}_\delta]$ для $a \in_U \mathbb{Z}_n$:

$$\Pr[F_\delta] = \Pr[\delta(\mathrm{a}) \equiv 0\ mod\ n] \cdot (1 - \Pr[\delta(\mathrm{a}) \equiv 0\ mod\ n]) + (1 - \Pr[\delta(\mathrm{a}) \equiv 0\ mod\ n])$$
$$\cdot \Pr[\delta(\mathrm{a}) \equiv 0\ mod\ n] = 2 \cdot \nu_p \cdot \nu_q \cdot (1 - \nu_p \cdot \nu_q)$$

Оценим теперь $\Pr[D_\delta]$:

$$\Pr[D_\delta] = 1 - \Pr[\delta(\mathrm{a}) \equiv 0\ mod\ n] - \Pr[(\delta(\mathrm{a}) \neq 0\ mod\ p) \wedge (\delta(\mathrm{a}) \neq 0\ mod\ q)] = 1 -$$
$$\Pr[\delta(\mathrm{a}) \equiv 0\ mod\ n] - \Pr[(\delta(\mathrm{a}) \neq 0\ mod\ p)] \cdot \Pr[(\delta(\mathrm{a}) \neq 0\ mod\ q)] = 1 - \nu_p \cdot \nu_q - \left(1 - \nu_\mathrm{p}\right) \cdot$$
$$\left(1 - \nu_\mathrm{q}\right).$$

$$2 \cdot \Pr[D_\delta] - \Pr[F_\delta] = 2 \cdot \left(1 - 2 \cdot \nu_p \cdot \nu_q - \left(1 - \nu_\mathrm{p}\right) \cdot \left(1 - \nu_\mathrm{q}\right) + \nu_p^2 \cdot \nu_q^2\right) \geq 0 \Leftrightarrow (1 - \nu_p \cdot \nu_q)^{\,2} \geq$$
$$\left(1 - \nu_\mathrm{p}\right) \cdot \left(1 - \nu_\mathrm{q}\right).$$ Последнее неравенство выполняется для $0 \leq \nu_p, \nu_q \leq 1$. □

Рассмотрим алгоритм B, который запускает A. B для $\forall \delta \in \mathcal{D}$ выбирает случайный $a \in \mathbb{Z}_n$ и считает НОД$(n, \delta(a))$. Таких полиномов не более $(\mu + l + 2)(\mu + l + 1)/2$, и каждый из них может быть вычислен за $\mu + l + 1$ операций кольца. Обозначим за D событие, что одно из вычислений НОД$(n, \delta(a))$ даст нетривиальный сомножитель n. Тогда $\Pr[D] \geq \max_{\delta \in \mathcal{D}}(\Pr\ [D_\delta])$ и получаем:

$$\Pr[F] \leq \textstyle\sum_{\delta \in \mathcal{D}} \Pr\ [F_\delta] \leq 2 \cdot \sum_{\delta \in \mathcal{D}} \Pr[D_\delta] \leq (\mu + 2 + l) \cdot (\mu + 1 + l) \cdot \Pr[D]\,. \quad (2)$$

Т.к. $\varepsilon = \Pr[\mathrm{S}]$ имеем:$\Pr[F] \geq \Pr[S] - \Pr\left[S_{sym}\right] \geq \varepsilon - \frac{1}{\mathrm{n}}$. Подставляя эту оценку в (2) получаем: $\Pr[D] \geq \frac{\Pr[F]}{(\mu+2) \cdot (\mu+1)} \geq \frac{\varepsilon - \frac{1}{\mathrm{n}}}{(\mu+2) \cdot (\mu+1)}$. □

Теорема. Если A проводит μ ($\mu \leq n$) алгебраических операций с шифртекстами криптосистем RM11 и решает $COA(c_1(x), \ldots, c_l(x), \mathcal{O}^{=}_{\mathrm{k}})$ с вероятностью ε, то существует алгоритм B, который, имея открытый доступ к A, находит сомножитель n с вероятностью $\frac{\varepsilon - \frac{1}{\mathrm{n}}}{(\mu+2) \cdot (\mu+1)}$.

Заключение. Проведен обзор схем АГШ с $P = \mathbb{Z}_n[x]$, где n – трудно факторизуемый модуль. Все существующие конструкции нестойки к АИОТ. Проведен анализ стойкости к АТШ. В случае равномерного распределения на P доказана сводимость от задачи взлома к задаче факторизации. При неравномерном распределении на P все эти криптосистемы становятся нестойкими, АТШ можно свести к АИОТ.

СПИСОК ЛИТЕРАТУРЫ

1. Rivest, R.L. On data banks and privacy homomorphisms / R.L. Rivest, L. Adleman, M.L. Dertouzos // Foundations of secure computations. — 1978. — № 11. — С. 169-180.
2. Gentry, C. Fully homomorphic encryption using ideal lattices / C. Gentry // Proceedings of forty-first annual ACM Symposium on Theory of computing. — 2009. — С. 169-178.

3. Sathya S. S. et al. A review of homomorphic encryption libraries for secure computation //arXiv preprint arXiv:1812.02428. – 2018.
4. J. D. i. Ferrer, A new privacy homomorphism and applications. Information Processing Letters, vol. 60, no. 5, pp. 277–282, 1996.
5. Josep Domingo-Ferrer and Jordi Herrera-Joancomart. A privacy homomorphism allowing field operations on encrypted data.
A. O. Zhirov, O. V. Zhirova, and S. F. Krendelev. Bezopasnye oblachnye vychisleniya s pomoshhyu homomorfnoj cryptographii.BIT (bezopasnost' informacionnyx technology) journal, 1:6–12, 2013.
A. B. Alexander Rostovtsev and M. Mikhaylov. Secure evaluation of polynomial using privacy ring homomorphisms. Cryptology ePrint Archive, Report 2011/024, 2011.http://eprint.iacr.org/
6. Kipnis, Aviad, and Eliphaz Hibshoosh. "Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification." *Cryptology ePrint Archive* (2012).
7. Shatilov K., Boiko V., Krendelev S., Anisutina D. and Sumaneev A. Solution for secure private data storage in a cloud // In Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on. P. 885-889. IEEE, 2014.
8. Xiao L., Bastani O., Yen I. L. An Efficient Homomorphic Encryption Protocol for Multi-User Systems // IACR Cryptology ePrint Archive.–2012.– No193.
9. *Barcau M., Paşol V.* On the IND-CPA security of ring homomorphic encryption schemes over F2 // Proceedings of the Romanian Academy Series A - Mathematics Physics Technical Sciences Information Science. – 2020. – № 1(21). – С. 3-10
10. Brickell, E.F. On privacy homomorphisms / E.F. Brickell, Y. Yacobi // Advances in Cryptology— EUROCRYPT'87. — 1988. — С. 117-125.
11. Altmann, K. On black-box ring extraction and integer factorization / K. Altmann, T. Jager, A. Rupp // Proceedings of the 35th international colloquium on Automata, Languages and Programming, Part II. — 2008. — С. 437-448.
12. J. H. Cheon, W.-H. Kim, and H. S. Nam. Known-plaintext cryptanalysis of the domingo-ferrer algebraic privacy homomorphism scheme. Information Processing Letters, 2006, vol. 97, no. 3, pp. 118–123.
13. Трепачева А. В. Улучшенная атака по известным открытым текстам на гомоморфную криптосистему Доминго-Феррера //Труды Института системного программирования РАН. – 2014. – Т. 26. – №. 5. – С. 83-98.
14. Trepacheva A., Babenko L. Known plaintexts attack on polynomial based homomorphic encryption //Proceedings of the 7th International Conference on Security of Information and Networks. – 2014. – С. 157-165.
15. Trepacheva A. Cryptanalysis of Polynomial based Homomorphic Encryption //Proceedings of the 7th International Conference on Security of Information and Networks. – 2014. – С. 205-210.
16. Трепачева А. В. О криптоанализе одной полностью гомоморфной криптосистемы на основе задачи факторизации //Безопасность информационных технологий. – 2015. – Т. 22. – №. 4. – С. 19-25
17. Vizár D., Vaudenay S.Analysis of Chosen Symmetric Homomorphic Schemes // Central Eu- ropean Crypto Conference.–2014.– No.EPFL-CONF-198992.
18. Tsaban B., Lifshitz N. Cryptanalysis of the MORE symmetric key fully homomorphic encryption scheme //Journal of Mathematical Cryptology. – 2015. – Т. 9. – №. 2. – С. 75-78.
19. Трепачева А. В. Криптоанализ симметричных полностью гомоморфных линейных криптосистем на основе задачи факторизации чисел //Известия Южного федерального университета. Технические науки. – 2015. – №. 5 (166). – С. 89-102.
20. Трепачева А. В. Атака по шифртекстам на одну линейную полностью гомоморфную криптосистему //Прикладная дискретная математика. Приложение. – 2015. – №. 8. – С. 75-78.
21. Трепачева А. В. О соотношениях между атаками на симметричные шифры, гомоморфные над кольцом вычетов //Безопасность информационных технологий. – 2017. – Т. 24. – №. 2. – С. 82-91.
22. Aggarwal D., Maurer U. Breaking RSA generically is equivalent to factoring //Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Berlin, Heidelberg, 2009. – С. 36-53.
23. Jager T., Schwenk J. On the analysis of cryptographic assumptions in the generic ring model //Journal of cryptology. – 2013. – Т. 26. – №. 2. – С. 225-245.
24. Victor Shoup. Sequences of games: a tool for taming complexity in security proofs. CryptologyePrintArchive, Report 2004/332, 2004. http://eprint.iacr.org/

Фадеев И.И.
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича, ассистент кафедры
fadeev.collapse@yandex.ru

АНАЛИЗ ПОДХОДОВ К МОДЕЛИРОВАНИЮ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: В ходе анализа подходов к моделированию актуальных угроз необходимо определить научные подходы к разработке базовой модели угроз, методик оценки рисков и анализа масштабов возможных последствий, а также методики принятия решений при задании и разработке требований к подсистеме безопасности объектов критической информационной инфраструктуры, функционирующих в области оборонной промышленности. Итоговым результатом работы будет являться методика оценки эффективности принятых организационных и технических мер объекта КИИ, функционирующего в области оборонной промышленности.

Ключевые слова: критическая информационная инфраструктура, оборонная промышленность, угрозы информационной безопасности, деструктивные воздействия, целевые компьютерные атаки, модель нарушителя информационной безопасности, модель угроз, компьютерные инциденты, подсистема безопасности.

Введение. В XXI веке окружающая среда с каждым днем все стремительней развивается и меняется благодаря новым информационным технологиям и интернету [1].

В период с 2005 по 2008 год ФСТЭК России, были разработаны и утверждены методические документы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации.

В связи с применением вновь утвержденной Методики оценки угроз безопасности информации [2] Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных и Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры более не применяются. При этом Базовые модели угроз безопасности информации могут применяться для моделирования угроз безопасности информации на значимых объектах критической информационной инфраструктуры Российской Федерации до утверждения ФСТЭК России соответствующих методических документов [3].

При этом действующие методики предполагают анализ всех угроз безопасности информации, а уточняющие методические документы, такие как Типовые модели угроз безопасности информации для конкретных видов объектов КИИ или Базовые модели угроз безопасности объекта КИИ в конкретных сферах деятельности субъектов КИИ частично находятся в стадии разработки.

Актуальность темы исследования. Развитие подходов в области обеспечения безопасности критической информационной инфраструктуры, развитие требований, предъявляемых к их защите, выделение отдельных понятий в информационной безопасности таких систем и практика применения изданных ранее нормативных и методических документов обусловлены различными направлениями информатизации и развитием информационных технологий. Цифровая трансформация затрагивает всё больше повседневных процессов, затрагивающих экономику, потенциал и безопасность государства, а также здоровье и безопасность граждан, в том числе за счет экологической и социальной безопасности. При этом, защита от угроз, обусловленных техногенными источниками, регулируется различными отраслями ещё с конца XX века.

В настоящее время особое внимание уделяется антропогенным источникам угроз: с развитием информационных (автоматизированных) систем и сетей компьютерные инциденты и возможные последствия их возникновения должны быть рассмотрены как результаты целевых компьютерных атак, с учетом подготовки потенциальных нарушителей к реализации сценариев, использующих все последовательности возможных тактик и соответствующих им техник.

Одним из проблемных вопросов, возникающим при моделировании угроз является определение актуальности применяемых нормативных и методических документов в области защиты информации. Многогранность подходов к обеспечению безопасности существующих и создаваемых объектов критической информационной инфраструктуры обусловлена широкой сферой использования информационных (автоматизированных) систем и сетей и разнообразием их типов.

Так, в соответствии с законодательством Российской Федерации [4] определено 12 сфер и областей функционирования объектов критической информационной инфраструктуры. В зависимости от критических процессов субъекта, реализуемых в информационных (автоматизированных) системах и сетях, а также типов таких систем могут быть определены базовые подходы к их категорированию и моделированию актуальных угроз, путём экспертной оценки и статистических данных.

Степень разработанности темы. Изученные научные подходы и практические решения в области информационной безопасности объектов критической информационной инфраструктуры зачастую связаны с автоматизированными решениями. Созданию интеллектуальных сервисов защиты информации в критических инфраструктурах посвящены работы таких ученых, как Д.П. Зегжда, И.В. Котенко, И.Б. Саенко, С.А. Петренко, А.Е. Кучерявый, А.И. Толстой. Также в научных исследованиях отражены подходы к анализу и оценке рисков в области информационной безопасности, в том числе с использованием нейро-нечёткой модели, данные исследования включены в работы С.А. Агеева [5], И.М. Ажмухамедова [6,7], И.В. Аникина [8,9], Е.К. Барановой [10,11], Т.И. Булдаковой [12], Н.Г. Милославской [13] и других.

Проведенный анализ работ по научной деятельности в области информационной безопасности показал, что научно-техническая задача оценки рисков и прогнозирования угроз информационной безопасности не охватывает область оборонно-промышленного комплекса (ОПК). В частности не рассмотрена специфика предприятий и организаций, работающих в сфере ОПК и объектов критической информационной инфраструктуры, принадлежащих им. Существующие методики не охватывают информационных систем реальных производств в указанной сфере, новые информационные угрозы и сопутствующие им риски и возможные негативные сценарии.

Цели и задачи работы. Цели исследования заключаются в повышении защищенности объектов критической информационной инфраструктуры (КИИ) и состоят из следующих задач: анализ текущего состояния защищенности объектов КИИ, разработка варианта базовой модели угроз и типовой модели нарушителя объекта КИИ, функционирующего в области оборонной промышленности; разработка методики оценки рисков и анализа масштабов возможных последствий; разработка методики принятия решений при задании и разработке требований к системе защиты информации. Все задачи взаимосвязаны и результаты их выполнения позволят выработать рекомендации по принятию решений о целесообразности внесения изменений в существующие объекты КИИ, на предпроектной стадии или на стадии определения перечня объектов КИИ, подлежащих категорированию.

Научная новизна. Впервые проведен анализ подсистем безопасности объектов КИИ, функционирующих в области оборонной промышленности, обобщены достоверные сведения в масштабе федерального округа.

Теоретическая и практическая значимость работы. В ходе анализа современного состояния исследований в данной области было выявлено, что существующие методические подходы зачастую находятся в стадии разработки и требуют апробации. Отсутствие широкой правоприменительной практики, в том числе полноценных (в рамках охвата большого количества объектов) результатов государственного надзора (контроля) за обеспечением безопасности значимых объектов критической информационной инфраструктуры позволяет формировать новые подходы и оценивать применимость различных методов в ходе проведения научных исследований.

Разрабатываемые базовые модели угроз, которые будут содержать описание типовых объектов критической информационной инфраструктуры, номенклатуру и общее описание угроз безопасности и рекомендации по их нейтрализации (парированию), регулятором также планируется разработать Методики оценки показателей критериев значимости и Типовые модели угроз.

В Методиках оценки показателей критериев значимости помимо непосредственного описания (алгоритма) оценки показателей будут доступны основные логические и (или) расчетные соотношения, необходимые для оценки возможных ущербов, возникающих вследствие реализации компьютерных атак и нарушения функционирования объектов критической информационной инфраструктуры, а также соотношения, необходимые для определения показателей критериев значимости. Таким образом, среди подходов по категорированию необходимо выделить особенности сферы (области) функционирования объектов критической информационной инфраструктуры, принадлежащим субъектам и сфер деятельности субъектов в целом с привязкой к возможным негативным последствиям в данных сферах и непосредственно применимым показателям критериев значимости. Основой для осуществления моделирования будут являться в первую очередь анализ критических процессов, реализуемых в конкретной сфере (области) деятельности субъекта критической информационной инфраструктуры. На основании экспертной оценки и статистических данных для каждой сферы

возможна разработка примерных базовых моделей угроз с учетом определения обобщенных групп возможных нарушителей и основных негативных последствий актуальных для определенной сферы деятельности.

Методы исследования базируются на положениях теории системного анализа, математического моделирования, теории вероятности и методологии теории рисков.

В рамках проводимого исследования проанализированы результаты мониторинга сведений о публикуемых критических уязвимостях программного обеспечения государственных информационных систем и объектов критической информационной инфраструктуры, а также связанных с ними компьютерных атаках. На основании сведений, полученных из общедоступных источников информации в период с 28 февраля 2022 г. по настоящее время оценено влияние целевых компьютерных атак на состояние защищенности критической информационной инфраструктуры Российской Федерации.

По результатам анализа проведенного в рамках взаимодействия

с организациями, функционирующими в области разработки и внедрения средств защиты информации, и информации Национального координационного центра по компьютерным инцидентам, установлено, что в указанный период:

повысилась интенсивность рутинного опроса внешних интерфейсов информационных систем и сетей;

основные компьютерные инциденты были вызваны использованием «открытых» инструментов, распространяемых в общедоступных источниках информации;

инциденты, повлекшие масштабные негативные последствия зачастую были реализованы за счет возможностей внутренних нарушителей или связаны со слабой парольной защитой.

Учитывая, что потенциал и мотивация нарушителей теперь не являются определяющими факторами в условиях открытого распространения и простоты использования инструментов для реализации атак, для разработки базовой модели угроз предлагается рассмотреть угрозы безопасности информации, реализуемые нарушителями, обладающими высокими возможностями по реализации угроз безопасности информации (Н4).

Таким образом, в случае отсутствия информации о времени и цели атаки на критическую информационную инфраструктуру, а также в условиях отсутствия масштабных негативных последствий возможно рассмотреть состояния объектов КИИ в рамках марковских процессов для решения задачи по разработке базовой модели угроз. Использование Методики [2], автором смоделировано функционирование объектов КИИ со следующими работоспособными состояниями (Табл. 1).

Табл. 1. Состояние объектов КИИ

Вариант состояния	Описание состояния
S0	нормальное состояние, в работе, без инцидентов
S1	нормальное состояние, отключен, без инцидентов
S2	нарушение конфиденциальности, в работе
S3	несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным; в работе
S4	отказ в обслуживании компонентов (нарушение доступности), в работе
S5	нарушение целостности информации, в работе
S6	несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач, в работе
S7	нарушение функционирования (работоспособности) отдельных программно-аппаратных средств обработки, передачи и хранения информации, в работе

Разработка варианта базовой модели угроз и типовой модели нарушителя ОКИИ для организаций ОПК необходима по причине отсутствия методических документов, предлагаемых (рекомендуемых) к применению при моделировании актуальных угроз безопасности информации. Также разработанная модель систематизирует виды и категории актуальных нарушителей и последовательности тактик и техник, применение которых может привести к реализации угрозы безопасности информации.

Типовые модели угроз предполагают описание архитектуры систем (совокупность основных структурно-функциональных характеристик, свойств, компонентов систем и сетей, воплощенных в

информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации), являющихся объектами критической информационной инфраструктуры, и их описание как объектов защиты от компьютерных атак. На основании типовой архитектуры описываются потенциальные уязвимости систем (с учетом основного программного и программно-аппаратного обеспечения, используемого в данных системах), типовая модель нарушителя в системе, типовые способы (сценарии) реализации угроз и типовые компьютерные инциденты, происходящие в результате реализации угроз безопасности. Таким образом в развитие Базовых моделей угроз, определив типовые объекты критической информационной инфраструктуры для каждой сферы, могут быть разработаны примерные Типовые модели угроз для актуальных типов информационных (автоматизированных) систем, где особенно важным будет являться определение интерфейсов объектов воздействия для конкретных видов систем.

Указанные подходы при формировании модели угроз и определения актуальных угроз безопасности информации также могут быть использованы до утверждения ФСТЭК России соответствующих методических документов.

Также в ходе оценки угроз безопасности информации для типовых объектов критической информационной инфраструктуры, актуальных для сферы деятельности субъекта должны быть определены возможные негативные последствия (социальные, политические, экономические, экологические, и последствия для обеспечения обороны страны, безопасности государства и правопорядка), которые могут наступить от реализации (возникновения) угроз безопасности информации [14]. При этом, решая задачу моделирования угроз необходимо помнить о взаимосвязи возможных негативных последствий с показателями критериев значимости.

Дополнительно возможно провести анализ источников угроз, определив общую характеристику нарушителей и (или) источники угроз для конкретных угроз безопасности информации. В рамках данного анализа рекомендуется определить взаимосвязь последствий реализации угрозы с видами воздействий (нарушение конфиденциальности, целостности, доступности), а также с целями и объектами защиты.

Таким образом исходя из актуальных возможных негативных последствий, актуальности источников угроз разрабатывается номенклатура угроз безопасности информации для конкретной сферы деятельности субъекта. На данном этапе при формировании Базовых моделей угроз из общего перечня угроз безопасности информации при наличии обоснования могут быть исключены угрозы невозможность реализации которых связана с отсутствием объектов воздействия (применяемых информационных технологий), отсутствием актуальных источников угроз и отсутствием актуальных негативных последствий (во взаимосвязи с показателями критериев значимости). Отдельные угрозы безопасности, реализация которых обусловлена эксплуатацией уязвимостей также могут быть исключены из общего перечня уязвимостей.

В соответствии с полученной номенклатурой угроз безопасности информации для объектов критической инфраструктуры, функционирующих в конкретных сферах деятельности должны быть выработаны рекомендации по их нейтрализации (парированию). В зависимости от сферы деятельности субъекта в целом или объекта критической информационной инфраструктуры меры по защите могут определяться в соответствии с существующими требованиями в области защиты информации (например, при рассмотрении возможных категорий обрабатываемой информации), также могут применяться отдельные организационные и технические мероприятия, направленные на предотвращение определенных ранее актуальных негативных последствий. Должны быть разработаны отдельные рекомендации для парирования угроз, реализация которых обусловлена эксплуатацией уязвимостей.

Разработка Типовых моделей угроз сопряжена с анализом и классификацией существующих информационных (автоматизированных) систем и сетей. В соответствии с Методикой оценки угроз безопасности информации допускается разработка одной модели угроз безопасности информации для нескольких однотипных создаваемых систем и сетей обладателя информации или оператора. Типовые модели угроз предлагают конкретную классификацию объектов критической информационной инфраструктуры и направлены на их детальное описание как объектов защиты.

Первой задачей в разработке Типовой модели угроз является обобщенное описание архитектуры, свойственной описываемым системам. На основании типовой архитектуры должно быть выполнено логическое сегментирование компонентов систем и сетей с целью определения отдельных сегментов как объектов (интерфейсов) воздействия угроз безопасности информации.

Дополнительно для объектов (интерфейсов) воздействия могут быть определены типы программного (программно-аппаратного) обеспечения, применяемого для реализации критических процессов, могут быть рассмотрены конкретные продукты (продуктовые линейки).

На основании анализа типовой архитектуры оценивается наличие потенциальных угроз безопасности информации (и, при необходимости уязвимостей) в соответствии с используемыми информационными технологиями, возможными объектами воздействия. Дополнительно может быть определена критичность объектов воздействия с использованием описания векторов компьютерных атак, содержащиеся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.) [2].

В развитие описываемой в Базовых моделях угроз общей характеристики модели нарушителя при разработке Типовой модели угроз определяются типовые нарушители, на основании возможностей которых должны быть определены способы реализации угроз безопасности информации. Обладая уточненной информацией о типовых архитектурах и объектах воздействия, полученных в ходе разработки модели угроз, данные способы должны учитывать сценарии реализации угроз с применением соответствующих основных тактик и типовых техник, основывающихся на применении свойственных типовому объекту информационных технологий и программных (программно-аппаратных) средств.

При этом, угроза безопасности информации является актуальной, только в том случае, если имеется сценарий реализации угрозы: имеется источник угрозы (нарушитель), имеются объекты и интерфейсы воздействия, а способы реализации угрозы безопасности информации и непосредственно реализация угрозы может привести к негативным последствиям [2]. Таким образом, описав типовые объекты воздействия, типовых нарушителей и способы реализации угроз следующим шагом в разработке Типовой модели угроз будет являться определение актуальных видов воздействий и возможных негативных последствий. В рамках данного шага необходимо провести анализ в соответствии с новой Методикой, где помимо используемых в Банке данных угроз безопасности информации ФСТЭК России нарушений конфиденциальности, целостности и доступности актуальными также будут являться: несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным; несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач; нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации [2].

Положения, выносимые на защиту.

1. Разработка базовой модели угроз.

Проведен анализ подсистем безопасности ОКИИ, функционирующих в области оборонной промышленности, обобщены достоверные сведения в масштабе федерального округа, автором проведен анализ информационных систем более 40 значимых организаций оборонно-промышленного комплекса.

Научно-исследовательская работа позволила разработать базовую модель угроз объектов КИИ, функционирующих в области оборонной промышленности. В целях выполнения задач, решаемых в ходе оценки угроз, исходя из сферы деятельности субъекта были определены объекты критической информационной инфраструктуры, реализующие критические процессы. Разработанная базовая модель угроз объекта КИИ функционирующего в области оборонной промышленности (**пункт 3 паспорта специальности 2.3.6.**) **систематизирует** виды и категории актуальных нарушителей и последовательности тактик и техник, применение которых может привести к реализации угроз безопасности информации и **позволяет совершенствовать** процесс моделирования актуальных угроз безопасности информации в организациях ОПК, **выработать рекомендации по парированию** угроз безопасности и содержит информацию о мерах защиты информации, направленных на нейтрализацию угроз.

Достоверность результатов обеспечивается корректным применением общенаучных методов исследования, подтверждается апробацией полученных результатов на практике и хорошей корреляцией с известными исследованиями.

2. Разработка типовой модели угроз.

Автором также оценены и проанализированы статистические данные более 200 субъектов КИИ.

Анализ рисков нарушения информационной безопасности в информационных системах управления производством (**пункт 8 паспорта специальности 2.3.6.**) позволяет смоделировать актуальные угрозы безопасности для таких систем. Проведен обширный анализ подсистем

безопасности объектов КИИ, являющихся информационными системами управления производством, обобщены достоверные сведения в масштабе федерального округа. **Определены и конкретизированы** применительно к особенностям деятельности организаций ОПК типовые компьютерные инциденты, их **взаимосвязь** с объектами и интерфейсами воздействия. Разработанная типовая модель ОКИИ, **позволит определить** границу оценки угроз безопасности информации и необходимые исходные данные, используемые в ходе выявления критических процессов организаций ОПК и объектов, подлежащих категорированию.

Достоверность результатов обеспечивается надежными исходными данными и подтверждается внедрением полученных результатов в практику организаций оборонно-промышленного комплекса.

3. Разработка метода принятия решений.

Дополнительно автором разработан метод принятия решений при задании и установлении требований к подсистемам защиты информации ОКИИ (**пункт 16 паспорта специальности 2.3.6.**).

В отличие от известных, метод учитывает требования к обеспечению безопасности различных систем и сетей, **дополняет** существующие базовые модели угроз и основан на совершенствовании проведения экспертных оценок за счёт определения весовых коэффициентов. Метод **устанавливает зависимость** объектов и видов воздействия от негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации, а также **обеспечивает поддержку принятия решений и позволяет** задать требования к обеспечению безопасности объекта КИИ (в том числе не являющегося значимым) и определить базовый набор мер по обеспечению безопасности объекта КИИ и (или) повысить уровень их защищенности за счет совершенствования подсистем безопасности.

Разработка метода принятия решений при задании и установлении требований к системе защиты информации в зависимости от типов систем и сетей **в отличие от известных**, учитывает требования к обеспечению безопасности различных систем и сетей, дополняет существующие базовые модели угроз Метод **основан на совершенствовании проведения экспертных оценок** за счёт определения весовых коэффициентов. устанавливает зависимость объектов и видов воздействия от негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации.

4. Разработка методики оценки эффективности.

Итоговым результатом работы будет являться методика оценки эффективности принятых организационных и технических мер объекта КИИ, функционирующего в области оборонной промышленности (**пункт 11 паспорта специальности 2.3.6.**) в которой**, в отличие от известных методик** конкретизированы критерии оценки эффективности защиты применительно к области оборонной промышленности.

Апробация результатов будет осуществлена не позднее ноября текущего года в рамках работы Координационного совета по проблемам противодействия иностранным техническим разведкам в организациях ОПК Северо-Западного федерального округа (более 20 предприятий ОПК).

Заключение.

В работе использованы результаты, в которых автору принадлежит определяющая роль. Часть опубликованных (публикуемых) работ и написана в соавторстве с сотрудниками СПбГУТ и Управления ФСТЭК России по Северо-Западному федеральному округу. В настоящее время полученные научные результаты проходят экспертизу в целях возможности открытого опубликования в рецензируемых изданиях из перечня ВАК при Минобрнауки России (3 публикации). В соответствии с планом выполнения проекта подготовлены материалы регистрации программы для ЭВМ (2 программы). Представление диссертации на НТС СПбГУТ спланировано на октябрь-ноябрь 2022 г.

СПИСОК ЛИТЕРАТУРЫ

1. Организация концептуальной модели критической информационной инфраструктуры / А. М. Гельфанд, Н. Н. Лансере, А. А. Ложкина, И. И. Фадеев // Методы и технические средства обеспечения безопасности информации. – 2020. – № 29. – С. 39-40. – EDN PYPOHZ.
2. Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.);
3. Информационное сообщение ФСТЭК России «Об утверждении методики оценки угроз безопасности информации» от 15 февраля 2021 г. № 240/22/690.
4. Федеральный закон Российской Федерации от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

5. Агеев, С.А. Оценка рисков сетевой компьютерной безопасности на основе нечеткого логического вывода / С.А. Агеев, И.Б. Саенко // ИБРР-2017: X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России». – Санкт-Петербург: СПб.: СПОИСУ, 1-3 ноября, 2017. – Том 3. – С. 28–30.
6. Ажмухамедов, И.М. Управление рисками информационной безопасности в условиях неопределенности / И.М. Ажмухамедов, О.Н. Выборнова, Ю.М. Брумштейн // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 1. – С. 7–14.
7. Ажмухамедов, И.М. Анализ рисков информационной безопасности / И.М. Ажмухамедов, О.Н. Выборнова, О.М. Князева: Учебное пособие. – Астрахань: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Астраханский государственный технический университет», 2015. – 104 с.
8. Аникин, И.В. Обеспечение информационной безопасности корпоративных информационных сетей через оценку и управление рисками / И.В. Аникин, Л.Ю. Емалетдинова, А.П. Кирпичников // Вестник технологического университета. – 2015. – Том 18, № 7. – С. 247–250.
9. Аникин, И.В. Метод управления рисками информационной безопасности в корпоративных информационных сетях / И.В. Аникин // Инфокоммуникационные технологии. – 2015. – Том 13, № 2. – С. 215–221.
10. Баранова, Е.К. Методики анализа и оценки рисков информационной безопасности / Е.К. Баранова // Образовательные ресурсы и технологии. – 2015. – № 1(9). – С. 73–79.
11. Баранова, Е.К. Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартами серии ИСО/МЭК 27000-27005 / Е.К. Баранова, А.С. Забродоцкий // Образовательные ресурсы и технологии. – 2015. – № 3(11). – С. 73–80.
12. Булдакова, Т.И. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечёткой модели / Т.И. Булдакова, Д.А. Миков // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. – 2013. – № 11. – С. 295–310.
13. Милославская, Н.Г. Управление рисками информационной безопасности / Н.Г. Милославская, М.Ю Сенаторов, А.И. Толстой: Учебное пособие для вузов. 2-е изд., испр. – М.: Горячая линия-Телеком, 2014. – 130 с.
14. Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

Шевяков И.А.
ЮУрГУ, инженер-исследователь,
regnlager@mail.ru

СИСТЕМА ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ СОЗДАНИЯ КОНЦЕПТУАЛЬНЫХ ПРОЕКТОВ ПРОГРАММНО-АППАРАТНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ СЕТИ ПОДКЛЮЧЕННОГО ТРАНСПОРТНОГО СРЕДСТВА

Аннотация: Целью работы является разработка метода определения критических узлов в подсистемах информационных сетей транспортных средств. С увеличением количества электронных устройств в современных транспортных средствах и появлению возможностей связи транспортного средства с окружающим миром с помощью беспроводных интерфейсов возросла опасность взлома подсистем транспортного средства, что может привести к авариям с тяжелыми последствиями. Для предотвращения взломов необходимо обеспечивать достаточный уровень защищённости информационной сети транспортного средства, для чего необходимо выявлять наиболее уязвимые с точки зрения информационной безопасности узлы сети. В статье используется метод моделирования логического описания операционных зависимостей в подсистеме распределения тормозных усилий с использованием И\ИЛИ графов. Меры защиты, которые применяются к элементам подсистемы, представляются как дополнительных слой над графом и совместно с узлами подсистемы моделируются как ребра гиперграфа. Операционные зависимости в подсистеме представляются в виде логических зависимостей со связями типа И/ИЛИ и представляются в конъюнктивной нормальной форме, после чего решается задача выполнимости SAT. Предлагаемый подход позволит получить новый метод математического моделирования защищённости узлов информационных сетей транспортного средства для построения оптимальной конфигурации защитных средств при известных критических узлах информационной сети транспортного средства и некоторых максимальных затратах на разработку.

Ключевые слова: информационная безопасность, защита информации, информационная сеть транспортного средства, подключенное транспортное средство, электронный блок управления (ЭБУ), И/ИЛИ граф, гиперграф, средство защиты информации (СЗИ), кибератака, кибербезопасность.

Современные автомобили в значительной степени компьютеризированы и подключены к сети. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1] и другие сопутствующие нормативные правовые акты обязали владельцев информационных систем (ИС), входящих в состав критической информационной инфраструктуры (КИИ), частью которой являются внутренние и внешние информационные сети всех транспортных средств, а также дорожная информационная инфраструктура, принимать меры по защите информации. Большая часть этих мер безопасности должна закладывается в информационные системы ещё на этапе проектирования.

На информационных ресурсах имеется много публикаций об атаках на автомобильные системы. Некоторые из них находились под пристальным вниманием средств массовой информации, что привело к ущербу репутации производителей автомобилей.

Помимо ущерба репутации, стоимость кибербезопасности становится проблемой для производителей автомобилей. Были обнаружены уязвимости, что привело к постоянному увеличению количества отзывов:

• Чарли Миллер и Крис Валасек [2] продемонстрировали концепцию удаленных атак, взяв под контроль джип и отправив его в бездорожье, заставив отозвать 1,4 миллиона автомобилей;

• Исследователи безопасности взломали BMW ConnectedDrive и смогли удаленно разблокировать автомобили, что оказало даже большее влияние на промышленность, чем взлом Миллера и Валасека – было отозванно 2,2 миллиона автомобилей;

Еще один пример - взлом электромобилей Tesla, потребовавший обновления программного обеспечения для операционной системы автомобиля. Эти угрозы влияют на безопасность, безопасность и конфиденциальность пассажиров и других граждан.

Из описанных выше примеров следует, что при проектировании ТС должно уделяться внимание безопасности информации на уровне как всей информационной сети в целом, так и на уровне отдельных узлов и подсистем. Для этого необходимо ещё на этапе проектирования обладать информацией о необходимых мерах защиты, которые необходимо применить в информационной сети

каждого конкретного разрабатываемого транспортного средства, чтобы обеспечить требуемый уровень безопасности информации, передающейся по внутренней сети ТС.

Степень разработанности темы исследования. Исследования по рассматриваемой тематике, как правило, проходят следующие этапы:

1) определение перечня угроз ИБ, которые могут возникать в сети ТС;

2) разработка алгоритмов и методик распределения мер защиты в информационной сети ТС;

3) программная реализация разработанных алгоритмов создания проекта размещения средств защиты;

4) разработка методик оценки эффективности создания проекта размещения средств защиты;

5) внедрение методики создания проекта средств защиты в процесс проектирования информационной сети ТС;

Проблеме обеспечения информационной безопасности транспортных средств и сложных киберфических систем посвящено множество исследований российских и иностранных ученых.

Вопросы, связанные с исследованием и классификацией угроз безопасности информации в сети ТС, рассматривались в работах авторов Juan Deng [3], Florian Sommer, Jürgen Dürrwang [4]. Авторами представлена классификация для описания атак на автомобильную безопасность, предложены различные методы обеспечения ИБ, как в рамках отдельного узла, так и системы в составе информационной сети ТС, описаны технические и организационные меры, направленные на нейтрализацию угроз ИБ.

Применению математических методов и алгоритмов анализа защищённости информации в сетях технических объектов и идентификации критических узлов в сложных сетях посвящено множество научных работ, среди которых необходимо отметить труды учёных Martín Barrère, Chris Hankin [5]. Авторы представили методику оценки уровня информационной безопасности, направленную на определение критических киберфизических компонентов и измерение общей безопасности сетей АСУ ТП. В основе подхода к созданию методики лежит использование моделей на основе графов И/ИЛИ, которые позволяют представлять сложные зависимости, которые обычно присутствуют в реальных промышленных сетях.

Разработке методов информационной поддержки для принятия решений при создании концептуальных проектов систем обеспечения защиты информации посвящены работы Тарасова А. Д. [6, 7]. В работах рассматривается метод определения требований к системе физической защиты объектов информатизации. Автором передоложен подход к определению требований к системе защиты объекта информатизации и метод создания концептуального проекта системы физической защиты с определением размещения средств защиты на территории объекта.

Часть указанных работ содержат количественные оценки результатов работы алгоритмов, что позволяет выбрать наилучший для решения задач анализа данных. Используя подходы, предложенные авторами, можно разработать метод определения требований и к системе защиты сети ТС и метод размещения средств защиты в сети ТС.

Таким образом, в настоящее время, не существует единой методики комплексного проектирования системы информационной безопасности ТС, позволяющей определить количество и состав мер защиты информации в информационной сети ТС при проектировании или модернизации электронных систем ТС. Возникает потребность в разработке комплексного метода распределения мер защиты в сети ТС, учитывающего все известные уязвимости узлов ТС.

Для разработки этого метода необходимо определить перечень актуальных угроз безопасности информации в сети ТС, типовой состав узлов и подсистем сети ТС, протоколов передачи данных по шинам информационной сети ТС. Необходимо создать алгоритмический и методологический аппарат автоматизированного проектирования размещения средств защиты в сети ТС, и на его основе разработать специальный комплекс программных средств, позволяющий ускорить процесс.

Целью диссертационной работы является разработка метода и алгоритмов для создания концептуальных проектов программно-аппаратной защиты информации информационной сети подключенного транспортного средства.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Разработать метод создания проекта размещения средств защиты в информационной сети транспортного средства.

2. Разработать математическую модель защищённости типовой сети ТС на основе теории графов.

3. Разработать программный комплекс для поддержки принятия решений при создании концептуальных проектов создания концептуальных проектов программно-аппаратной защиты информации информационной сети ТС.

Объект исследования - информационная сеть транспортного средства.

Предмет исследования - методы и алгоритмы проектирования комплекса защитных мер информационной сети транспортного средства

Методы исследования включают методы теории графов, гиперграфов, методы дискретной математики и математической логики.

Научная новизна результатов:

1. Разработан метод создания концептуального проекта размещения средств защиты в информационной сети транспортного средства с использованием моделей и метрик безопасности на основе И\ИЛИ графов и базы данных об инцидентах ИБ, и кибератаках на системы транспортных средств. Соответствует п.7 паспорта специальности «Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования».

2. Разработана математическая модель защищённости типовой сети ТС, основанная на представлении операционных зависимостей в сети ТС в виде И/ИЛИ графа. Соответствует п.10 паспорта специальности «Модели и методы оценки защищенности информации и информационной безопасности объекта».

3. Разработан алгоритм размещения средств защиты информации в информационной сети ТС для определения количества и видов средств программно-аппаратной защиты информации информационной сети ТС. Соответствует п.2 паспорта специальности «Методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида».

Практическая ценность работы и внедрение результатов:

Результаты исследования, в частности, полученный на основе математической модели безопасности информационной сети ТС алгоритм оптимального распределения средств защиты, и разработанный на его основе программный комплекс, могут быть использованы для информационной поддержки и проектирования систем защиты информации в аппаратуре узлов сети ТС.

Полученные в результате исследования материалы и научные данные могут быть использованы для создания методических указаний к учебному курсу по кибербезопасности транспортных средств. Разработанный программный комплекс может быть использован для проведения практических и лабораторных занятий по этому курсу.

Положения, выносимые на защиту:

1. Разработанный метод моделирования уязвимости узлов и защитных мер информационной сети транспортного средства, заключающийся в представлении узлов сети и защитных мер в виде гиперграфов, позволяет построить оптимальную конфигурацию защитных мер для сети ТС.

2. Разработанная математическая модель защищённости типовой сети ТС на основе теории графов, реализующая алгоритм оптимального распределения средств защиты информации в сети ТС, позволяет определить параметры защищённости узлов при различных конфигурациях сети ТС и актуальных для конфигурации угрозах.

3. Разработанные алгоритмы для поддержки принятия решений при создании концептуальных проектов программно-аппаратной защиты информации информационной сети ТС позволяют предоставлять информацию о количестве и типе защитных мер, и узлов, где они должны применяться для достижения оптимальной защищённости сети ТС.

- степень достоверности и апробацию результатов;

Апробация работы и публикации:

Результаты работы докладывались и обсуждались на следующих конференциях с публикацией в сборнике трудов:

1. Безопасность информационного пространства 2017: XVI Всероссийская научно-практическая конференция студентов, аспирантов, молодых ученых. - Екатеринбург, 2017.

2. Безопасность информационного пространства: XVIII Всероссийская научно-практическая конференция студентов, аспирантов, молодых ученых. - Магнитогорск, 2019.

3. Научный поиск: XIII научная конференция аспирантов и докторантов ЮУрГУ. – Челябинск, 2021.

4. Безопасность информационного пространства: XX Всероссийская научно-практическая конференция студентов, аспирантов, молодых ученых. – Тюмень, 2021.

5. 2022 Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology, USBEREIT. – Екатеринбург, 2022.

Результаты диссертационной работы опубликованы в 7 печатных изданиях, в том числе в 1 статье в изданиях из перечня ВАК.

Типовая архитектура информационной сети транспортного средства

Большинство архитектур ИСТС включают нескольких систем, связанных между собой центральным шлюзом (рис. 1). Системы отвечают за различные функциональные характеристики компонентов ТС. При компрометации этих компонентов могут появиться риски нарушения ИБ. Влияние этих рисков на безопасное, для дорожного движения, функционирование ТС может варьироваться. По этой причине, критичные для безопасности дорожного движения, компоненты ТС требуют соответствующей защиты.

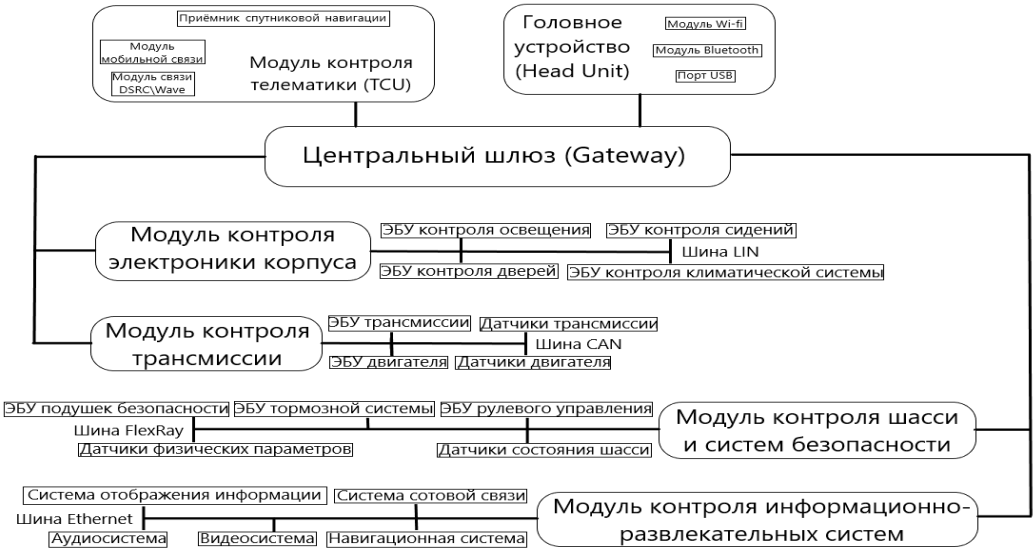


Рис. 1. Структура информационной сети транспортного средства

Компоненты разделяются по следующим категориям:
- управление трансмиссией;
- управление шасси;
- контроль корпуса;
- управление информационно-развлекательной системой;
- контроль коммуникаций;
- системы диагностики и обслуживания.

Угрозы, актуальные для информационной сети транспортного средства

Для представления основных задач информационной безопасности, актуальных для информационной сети транспортного средства, рассмотрены угрозы, которые могут возникнуть при эксплуатации и обслуживании транспортных средств. Большая часть угроз безопасности информации в ИСТС описана в базе данных Automotive Attack Database (AAD) [7], разработанной в университете Карлсруэ. База данных предлагает схему классификации для описания автомобильных атак безопасности в виде единой таксономии. Чтобы иметь возможность использовать описания атак на нескольких этапах разработки в качестве источника информации, атаки представлены с различным уровнем детализации.

Все угрозы, актуальные для ИСТС, можно объединить в несколько групп.

*Угрозы потери информации***:**
- угроза потери информации в облаке;
- угроза потери целостности конфиденциальной информации;
- угрозы потери информации от конфликтов DRM.

*Угрозы возникновения сбоев и неисправностей***:**
- угроза сбоя или перебоев в электроснабжении;
- угроза наличия критических программных ошибок;
- угроза сбоя или нарушения работы каналов связи.

*Угрозы перехвата и подделки сообщений сети***:**

- угроза перехвата информации через побочные электромагнитные излучения;
- угроза подделки сообщений сети;
- угроза «человек посередине» (MitM).

*Угрозы вредоносного воздействия на информационную сеть***:**

- угроза отказа в обслуживании;
- угроза манипуляции с аппаратным и программным обеспечением, манипулирования информацией;
- угроза несанкционированного доступа к информационной системе/сети;
- угроза компрометации конфиденциальной информации;
- угроза действия вредоносного программного обеспечения;
- угроза удаленного исполнения кода.

Для противодействия угрозам информационной безопасности в сети транспортного средства используются меры обеспечения ИБ, которые применяются и к компьютерным информационным сетям, но модифицируются с учётом специфики используемых протоколов и алгоритмов работы устройств, а также требований надёжности и быстродействия. Все меры защиты условно можно поделить на две категории – программные и аппаратные.

Программные меры защиты информации в сети ТС:

- обфускацию кода;
- использование криптографических методов;
- ловушки руткитов.

Аппаратные меры защиты информации в сети ТС:

- системы обнаружения вторжений;
- межсетевой экран центрального шлюза.

При определении угроз мы учитываем все типы источников, однако в первую очередь уделяем внимание оценке угроз, напрямую связанных с преднамеренными или случайными действиями нарушителей, так как реализация угроз, определяемых другими источниками, чаще всего подразумевает участие нарушителя.

В зависимости от наличия у нарушителя права доступа к сети объекта будем рассматривать внешних и внутренних нарушителей.

При детализации угроз существенное значение имеет потенциал нарушителя, определяемый его возможностями и характером воздействия (преднамеренное или случайное воздействие).

Классификация нарушителей в зависимости от имеющихся возможностей с краткой характеристикой методов воздействия на объект защиты представлена в Таблице 1.1. Для внутренних нарушителей возможности каждого последующего типа нарушителя по умолчанию включает возможности предыдущего.

Таблица 1.1. Типы и возможности нарушителей

Вид нарушителя	Характеристика имеющихся прав доступа	Способы реализации угроз воздействия	Характер воздействия
1	2	3	4
Внешний нарушитель			
Произвольный внешний субъект (хакер, преступная группа, конкуренты и др.)	Без каких-либо прав доступа к ИСТС или связанным с ней сетям и системам	- сбор информации об объекте защиты из внешних источников; - поиск путей проникновения через внешние системы; - эксплуатация уязвимостей; - применение методов социальной инженерии	Преднамеренный

Разработчик	Доступ к исходным кодам ПО и прошивок отдельных аппаратных и (или) программных компонентов ИСТС	- внесение ошибок, уязвимостей, недекларированных возможностей в ПО, программных или аппаратных закладок на стадии разработки;	Преднамеренный Случайный

Продолжение таблицы 1.1

1	2	3	4
Внутренний нарушитель без права доступа к ИСТС			
Пользователь внешних сервисов	доступ к внешним сервисам и системам, связанным с ИСТС посредством программных интерфейсов	- эксплуатация уязвимостей; - создание вредоносных закладок на ресурсах, доступных из ИСТС - злоупотребление полномочиями	Преднамеренный
Администратор внешних сервисов и внешней информационной инфраструктуры	доступ к сети и сетевому оборудованию	изменение конфигурации сетевого оборудования	Преднамеренный Случайный
Внутренний нарушитель, авторизованный в ИСТС			
Пользователь (водитель, пассажир)	доступ к отдельным компонентам и функциям ИСТС	- подлог данных - прослушивание/перехват данных; - некорректное изменение параметров ТП;	Преднамеренный Случайный
Обслуживающий персонал сервисных центров	- полный доступ к компонентам ИСТС и функциям конфигурирования, перепрограммирования и администрирования	изменение конфигурации компонентов ИСТС	Преднамеренный Случайный
Внешние субъекты, занимающиеся обслуживанием компонентов ИСТС (например, ремонтный центр, производитель)	- полный удаленный доступ к компонентам ИСТС и функциям конфигурирования, перепрограммирования и администрирования	изменение конфигурации компонентов ИСТС	Преднамеренный Случайный

Представление информационной сети ТС в виде графа

Автомобильную информационную сеть *W* можно представить как ориентированный И/ИЛИ граф *G* = (*V, E*), который представляет взаимодействия между узлами в *W* (рис. 2). Граф включает три типа базовых вершин, называемых атомарными узлами (V_{AT}), которые моделируют различные компоненты сети: *S* представляет набор узлов датчиков, *C* представляет набор узлов исполнительных механизмов, а *A* представляет набор программных агентов (работающих, например, в ЭБУ и TCU). V_{AT}

определяется как: $V_{AT} = S \cup C \cup A$. Кроме того, граф также включает два типа искусственных узлов, которые моделируют логические зависимости между компонентами сети: Δ представляет собой набор логических узлов И, а Θ представляет собой набор узлов логического ИЛИ. Набор всех узлов графа определяется как $V(G) = V_{AT} \cup \Delta \cup \Theta$. $E(G)$ является набором ребер между узлами, и их семантика зависит от типа узлов, которые они соединяют.

Меры защиты, применяемые в информационных сетях транспортного средства, могут применяться сразу к нескольким узлам сети, поэтому могут быть представлены как дополнительный уровень над графом логических зависимостей информационной сети транспортного средства. Множество задействованных мер безопасности Mi определяется как $S = \{s_1, s_2, ...\}$.

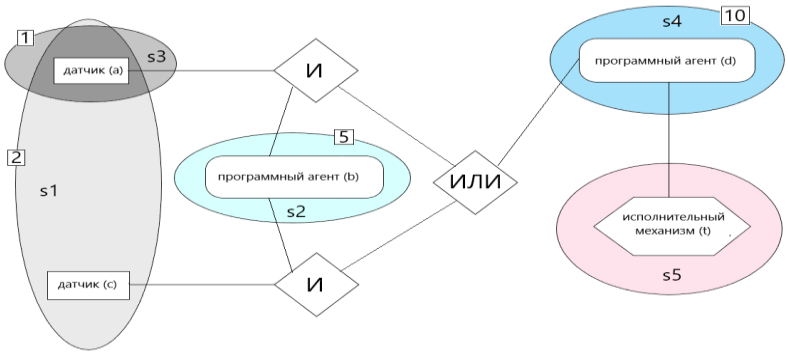


Рис. 2. Участок информационной сети в виде И/ИЛИ графа с перекрывающимися мерами безопасности

Гиперребра объединяют каждый сетевой узел с мерами безопасности, которые используются для их защиты. Таким образом, можно следовать той же логической структуре, что и в исходном графе, и объединять эти суперузлы с помощью связок И/ИЛИ, как показано на рис. 3.

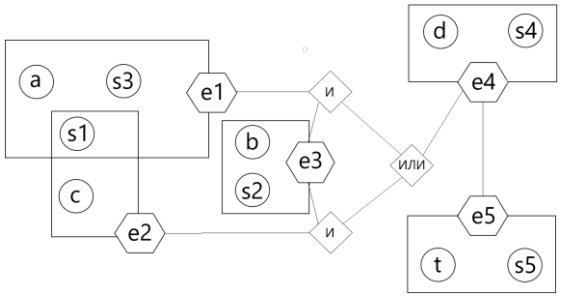


Рис. 3. Представление узлов сети (a, b, c, d, c1) и мер безопасности (s1, s2, s3, s4, s5) в виде рёбер гиперграфа И/ИЛИ (e1, e2, e4, e5)

Проблема рассматривается с логической точки зрения, следовательно, с точки зрения выполнимости.

Решение задачи максимальной выполнимости для описанного логического представления информационной сети транспортного средства, где веса задаются функциями $\phi(n)$ для каждого узла $n \in V_r$ и $q(s)$ для каждой меры безопасности $s \in S$. состоит из нескольких этапов:

1. Представление операционных зависимостей в подсистеме в виде логических зависимостей типа И/ИЛИ графа G.

2. Преобразование зависимостей графа G в эквивалентное логическое представление $g(x)$,

3. $g(t)$ преобразуется в новую формулу $k(t)$, где каждый не виртуальный узел сети $n \in V_r$ в $g(x)$ заменяется на $(n \vee s_i \vee ... \vee s_j)$, где $s_i \vee ... \vee s_j$ — это дизъюнкция мер безопасности, которые защищают узел n.

4. Затем цель атакующего $\neg k(t)$ преобразуется в конъюнктивную нормальную форму (КНФ) с помощью преобразования Цейтина, т. е. $G(x) = КНФ (\neg g(x))$, где $g(x) = (v_{1i} \vee ... \vee v_{1j}) \wedge ... \wedge (v_{hi} \vee ... \vee v_{hj})$.

5. Определяется мягкое предложение для каждого невиртуального узла $n \in V_r$ и каждой меры безопасности $s \in S$ и присваиваем им веса $(n, w(n))$ и $(s, q(s))$ соответственно.

Пусть W - информационная сеть ТС, G = (V, E) - ориентированный граф И / ИЛИ, представляющий рабочие зависимости в W, и t - целевой сетевой узел. Учитывая входной граф И/ИЛИ G = (V, E) и целевой узел t, метрика безопасности μ(G, t) моделируется как взвешенная частичная задача MAXSAT, где веса задаются функциями стоимости ϕ (v) для каждого узла v ∈ V_{AT} и ψ (s) для каждой меры безопасности s ∈ S.

Цель метрики безопасности μ (G, t) - идентифицировать набор узлов X = {x_1, .., x_h}, защищенный мерами S (X) = {s_1,. . . s_k} ⊆S, которые должны быть скомпрометированы, чтобы нарушить нормальную работу целевого узла t с минимальными затратами для злоумышленника. Более формально, S(X) = $\bigcup_{xi\in X} m(x_i)$ и μ: Γ × V → 2^V определяются как:

$$\mu(G,t) = \underset{X\subseteq V_{AT}}{\operatorname{argmin}} \left(\sum_{x_i\in X} \varphi(x_i) + \sum_{s_j\in S(X)} \omega(s_j)\right), \tag{2.1}$$

$$wcc\big(\sigma(G,X)\big) \geq 2 \vee X = \{t\}, \tag{2.2}$$

где решение с минимальной стоимостью должно быть либо узлом t, либо набором узлов X таким образом, что при удалении (с функцией σ) t отсоединяется от графа.

Функция σ(G, X) удаляет из G каждый узел x∈X и узлы, которые зависят от них, после распространения в логическом стиле. Затем результат анализируется с помощью функции wcc(G), которая вычисляет количество слабо связанных компонентов в G. Если G содержит два или более компонентов, это означает, что целевой узел t отключается от непустого набора узлов, на котором t зависит (прямо или косвенно) от правильного функционирования. S (X) возвращает набор экземпляров меры безопасности, используемых для защиты узлов в X. Следовательно, экземпляры меры, которые защищают более одного узла в X, появляются только один раз, и, таким образом, их стоимость учитывается только один раз при втором суммировании в уравнении (1). Также ϕ (n) может быть нейтральным (например, ϕ(n) = 0, ∀n∈V_{AT}), чтобы учитывать только затраты на меры безопасности, или он может быть соотнесён, например, с показателями CVSS.

Так как проблема рассматривается с логической точки зрения, то, следовательно, с точки зрения выполнимости. Процесс разрешения метрики включает три основных шага, которые подробно описаны в следующем разделе. В частности, первый шаг включает преобразование входного графа И/ИЛИ в логическую формулировку, которая представляет логические зависимости, от которых зависит цель t. Второй шаг расширяет эту формулировку, чтобы захватить экземпляры мер безопасности, которые защищают каждый узел в системе информационной сети. Для этого используется модель на основе гиперграфа И / ИЛИ, которая позволяет понять, как взаимосвязаны меры безопасности и компоненты сети. Наконец, третий шаг включает присвоение компромиссных затрат (весов) переменным в расширенной логической формулировке. Полученная взвешенная формула затем используется для решения задачи Weighted Partial MAX-SAT, решение которой укажет набор критических узлов и мер безопасности, которые должны быть скомпрометированы, с минимальными затратами для злоумышленника, чтобы нарушить работу системы.

Расчёт параметров системы защиты сети ТС

Для реализации метода было разработано программное обеспечение (ПО), в основу которого лёг обобщённый алгоритм решения задачи максимальной выполнимости. Функционально ПО состоит из трёх вычислительных модулей, модуля отображения результата, модуля чтения исходных данных и модуля формирования результата. Модуль расчёта показателей основан на решателе META4ICS [9], используемом для анализа защищённости сетей АСУ ТП.

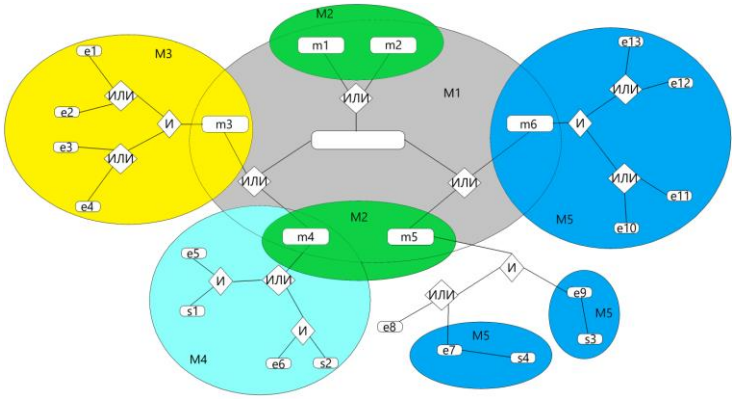


Рис. 4. Модель распределения средств защиты в типовой информационной сети ТС (e1…e13 – ЭБУ, s1… s4 – датчики, m1 … m6 – модули)

Результаты, представленные в таблице 1, представляют собой список узлов и экземпляров мер защиты (М1 – М6) для информационной сети ТС, представленной на рис. 1, каждая система которой представлена в виде И/ИЛИ графа (рис. 4), которые необходимо применить к этим узлам, чтобы затраты злоумышленника на преодоления данного узла были максимальны. Затраты злоумышленника, необходимые для преодоления системы защиты в расчитанной конфигурации, приведены в третьем столбце таблицы 1.

Табл. 2. Список мер защиты для каждого из компонент подсистемы

Мера защиты	Тип меры защиты	Затраты на преодоление	Защищаемые узлы
M1	M1	1	m1, m2, m3, m4, m5, m6
M2-1	M2	1	m1, m2
M2-2	M2	2	m4, m5
M3	M3	4	e1, e2, e3, e4, m3
M4	M4	4	e5, e6, s1, s2, m4
M5-1	M5	3	e7, s4
M5-2	M5	3	e9, s3
M5-3	M5	2	e10, e11 e12, e13, m6

Полученные данные о количестве и типе мер защиты информации можно использовать в системах автоматизированного проектирования, а также вносить в спецификации выпускаемых изделий.

Заключение

В работе решена актуальная научно-техническая задача поддержки принятия решений при создании концептуального проекта системы защиты информации информационной сети транспортного средства. Предложен новый метод моделирования уязвимости узлов информационных сетей транспортного средства, для построения оптимальной конфигурации защитных средств, заключающийся в применении математического моделирования с помощью И/ИЛИ графов и представлении совокупности защитных мер и узлов сети ТС в виде гиперграфов. Метод основан на применении моделей безопасности компьютерных и индустриальных систем к информационным сетям транспортного средства.

Применение методики создания концептуальных проектов систем защиты к информационным сетям транспортного средства с использованием моделей и метрик безопасности на основе И\ИЛИ графов с использованием базы данных об инцидентах ИБ и кибератаках на системы транспортных средств позволит получить систему, позволяющую при построении проекта защиты информации в сети ТС использовать опыт из других областей.

Результаты исследования, в частности, полученный на основе математической модели безопасности информационной сети ТС алгоритм оптимального распределения средств защиты, и

разработанный на его основе программный комплекс, могут быть использованы для информационной поддержки и ускорения проектирования систем защиты информации в аппаратуре ТС (10).

Полученные в результате исследования материалы и научные данные могут быть использованы для создания методических указаний к учебному курсу по кибербезопасности транспортных средств. Разработанный программный комплекс может быть использован для проведения практических и лабораторных занятий по этому курсу (11).

СПИСОК ЛИТЕРАТУРЫ

1. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26 июля 2017 г. №187-ФЗ // Собр. законодательства РФ. — 2017.
2. Charlie Miller, Chris Valasek. Adventures in Automotive Networks and Control Units. [Электронный ресурс]: https://illmatics.com/car_hacking.pdf
3. Juan Deng, Lu Yu, Yu Fu, Oluwakemi Hambolu, Richard R. Brooks. Chapter 6 - Security and Data Privacy of Modern Automobiles // Data Analytics for Intelligent Transportation Systems, Elsevier, 2017, Pages 131-163.
4. Sommer F, Dürrwang J, Kriesten R. Survey and Classification of Automotive Security Attacks. Information. 2019; 10 (4) :148. https://doi.org/10.3390/info10040148.
5. Martín Barrère, Chris Hankin, Nicolas Nicolaou, Demetrios G. Eliades, Thomas Parisini. Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies // Journal of Information Security and Applications, Volume 52, 2020, 102471, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2020.102471.
6. Боровский А.С., Тарасов А. Д. Автоматизированное проектирование систем физической защиты на основе функциональной и структурно – логической потоковых моделях / Информационные технологии, теоретический и прикладной научно-технический журнал. №6(202). 2013 г. С. 43–48.
7. Боровский А.С., Тарасов А. Д. Программный комплекс информационной поддержки решения задачи проектирования системы физической защиты / Системы управления и информационные технологии. №4.1(66). 2016 г. С. 122–128.
8. Martín Barrère, Chris Hankin, Nicolas Nicolaou, Demetrios G. Eliades, Thomas Parisini, Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies // Journal of Information Security and Applications, Volume 52, 2020, 102471, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2020.102471.
9. M. Barrère. META4ICS – metric analyser for industrial control systems. https://github.com/mbarrere/meta4ics; 2019.
A. Barinov, N. Davydkin, D. Sharova and S. Skurlaev, "Prioritization methodology of computing assets for connected vehicles in security assessment purpose," 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), 2019, pp. 1-6.
10. Шевяков И. А., Соколов А. Н. Концепция стенда для исследования кибербезопасности устройств на шине FlexRay «подключенного» транспортного средства, основанная на использовании интерфейсных плат // Вестник УрФО: Безопасность в информационной сфере. – Челябинск: Изд-во Южно-Уральский юридический вестник. - 2019. - №3(33) - С.73-81.

Шурховецкий Г.Н.
ФГБОУ ВО ИрГУПС, ассистент каф. «ИСиЗИ»,
gshn5@yandex.ru

ПЕРСОНАЛЬНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА БЕЗОПАСНОЙ ПЕРЕДАЧИ, ХРАНЕНИЯ И ОБРАБОТКИ ДАННЫХ

Аннотация: облачные технологии на сегодняшний день позволяют, как юридическим, так и физическим лицам уходить от трудностей, связанных с железом, инфраструктурой, кабелями, охлаждением и т.д. на физическом уровне, позволяя перейти в виртуальную инфраструктуру, где есть необходимая панель управления, с которой можно сделать нужные манипуляции и ни о чём лишнем не думать, с этой точки зрения облачные технологии идеальны для пользователей. Причём за безопасность облаков при нынешних технологиях уже можно не беспокоиться, но за безопасность наших данных в облаках беспокоиться стоит, т.к. её в принципе нет. Поэтому следует разработать технологию защищённой передачи, хранения и обработки информации в облачных и корпоративных хранилищах данных, а также в любой другой базе данных, которая будет осуществляться без использования алгоритмов шифрования. Это позволит устранить риски, связанные с «противоправными» действиями всех заинтересованных сторон в отношении пользователя.

Ключевые слова: новая парадигма в сфере защищённой передачи и хранения информации, некриптографические методы защиты, персональная информационная система, побитовое разложение.

Актуальность

Реальность нашего времени делает облачные технологии привлекательными и актуальными для нас – пользователей, т.к. хранение большого массива данных требует решения определённого спектра проблем, связанных с организацией и управлением необходимой инфраструктурой на физическом уровне, гораздо легче воспользоваться «облаками», где уже всё готово для работы пользователя в виртуальном виде, где мы можем решать все свои задачи, связанные с данными. Но, сегодня остро стоит вопрос, как в стране, так и в мире об эффективном обеспечении информационной безопасности. Это же касается и облачных технологий. За последнее время число кибератак и киберпреступлений постоянно растёт год от года и так будет продолжаться дальше. Так, например, в нашей стране рост составляет в 3-4 раза каждый год, по сравнению с предыдущими и тенденция на дальнейший рост продолжает сохраняться, причём наблюдается интересная особенность у данного процесса: регулярное снижение роста количества преступлений, совершённых на улице в реальном мире и постепенный интенсивный переход криминала в сферу информационных технологий [1]. В этих условиях, чтобы обеспечивать более совершенную защиту зачастую приходиться усложнять комплекс мер, направленных на обеспечение более лучшей защищённости данных, что достаточно часто повышает затраты ресурсов, времени и приводит к снижению производительности информационных систем, где происходят эти усложнения. Шифрование становится всё более сложным, с применением невероятно огромных массивов данных. Но не всегда усложнение решения проблемы, способствует её разрешению и предотвращает её дальнейшее развитие. Гораздо эффективнее не усложнять постоянно информационную безопасность, не конкурировать с другими участниками в данной сфере, а постоянно применять творческий подход к решению проблемы, стремиться его упрощать и создавать новые методы и новые технологии. Также здесь стоит отметить то, какую безопасность нашим данным предлагают крупные компании и корпорации, на примере Microsoft. Если обратиться к заявлению о конфиденциальности корпорации Майкрософт, то можно прочитать такие интересные вещи, как:

«Наконец, мы будем получать, сохранять, передавать, раскрывать или хранить ваши персональные данные, включая ваше личное содержимое (например, содержимое электронной почты на странице Outlook.com или файлы, которые находятся в личных папках в службе OneDrive)…» [2]

Или, например:

«…мы вручную изучаем некоторые прогнозы и выводы, создаваемые автоматизированными методами на основе базовых данных. Например, мы вручную проверяем короткие фрагменты голосовых данных (после выполнения действий по деидентификации), чтобы улучшить наши технологии распознавания речи. Эта проверка вручную может выполняться сотрудниками Майкрософт или поставщиками, которые работают от имени корпорации Майкрософт.» [2]

Если взять аналогичные документы Google и др. корпораций, то по аналогии можно найти примерно ту же самую информацию. Поэтому говорить о том, что все данные пользователя шифруются и находятся под надёжной защитой, нельзя [3].

Степень разработанности темы

Анализ современного состояния исследований в данной области показал, что вопрос некриптографической защиты информации с учётом множественности хранилищ, исследован слабо. Данный подход радикально меняет общепринятую практику и парадигму, которая состоит в хранении информации в одном физическом и географическом местоположении или с одним конкретным поставщиком услуг. Существующие исследования и патенты в этой области не используют всей полноты возможностей данного подхода.

В ходе исследования российского рынка патентов, было выявлено 5 патентов, из них 3 взяты за аналог, за прототип был взят американский патент US 10216822B2 от 26.02.2019 «Data distribution methods and systems», информация о котором будет представлена далее по тексту [4-8]. Причём стоит отметить, что как таковых аналогов и прототипов найдено не было (за исключением выше указанного патента), они были найдены в смысле общей решаемой задачи. При изучении зарубежного рынка патентов использовалась база Patentoscope. PatentScope © предоставляет доступ к порядку 1.7 миллиона международных заявок [9]. Это бесплатная база, предоставленная Европейским патентным ведомством. Было выявлено порядка 11 патентов [10-20]. Также интересующий продукт был найден в американской компании IBM через их облачную платформу IBM Cloud Storage Object (высоко масштабируемый сервис облачных систем хранения данных, предназначенный для высокой прочности, устойчивости и безопасности). Патента данного продукта найти не удалось, хотя возможно он подкреплён рядом патентов. На русском информации об этом продукте найдено не было, поэтому в качестве источника информации был использован официальный американский сайт компании [21]. Так как объём данного научного доклада не позволяет просмотреть все эти патенты более детально, ниже будет представлен наиболее важные из них.

Также отчасти к тематике данного проекта можно отнести метод рассечения-разнесения, автора которого, к сожалению, найти не удалось, как и более детальной информации о методе, обычно не более 1 абзаца в различных литературных источниках, в том числе сети интернет [22-24]. У этого метода известны различные реализации, лучшая из которых рассечение-разнесение посимвольно, вплоть до битов. Также было рассмотрено дополнительно пространственно-временное распыление информации для более углубленного понимания тематики данного вопроса, для понимания ценности нашего исследования [25-32]. Если использовать все предлагаемые меры защиты данного метода, то существенно увеличивается время передачи данных, соответственно, если данные большие (100-и Мб, Гб и т.д.), то будет ли эффективен данный метод или же он безнадёжен в таких условиях использования. Также при использовании всех мер возрастает число ошибок при передаче сообщения. И в целом можно говорить об общем усложнении процедуры передачи, снижения возможности комфортного хранения информации, т.е. можно предположить, что данный метод защиты информации может не отвечать реалиям практического использования, хотя и имеет высокую степень надёжности, по крайней мере заявленную.

За главный прототип взят «Data distribution methods and systems» («Методы и системы распределения данных») патент US 10216822B2 от 26.02.2019 «Data distribution methods and systems» [33-34]. Важно отметить, что в американском патенте (US 10,216,822 B2) рассматривается лишь частный случай (причём данный случай не самый сложный) в новом направлении защиты информации. В рамках же данного проекта исследуется всё заданное направление по мере возможности и в ходе реализации исключается ряд существенных недостатков, которые присутствуют в американском патенте (US 10,216,822 B2), явно в нём прописанных.

Цели и задачи

Целью исследования данного проекта является практическая реализация возможностей технологий защищённой передачи и хранения информации во внешних хранилищах данных с использованием некриптографических способов защиты, а также основанных на множественности хранилищ данных, размещаемых в различных физических и географических разноудалённых местах, с использованием высокого уровня защиты информации (например, конфиденциальность, целостность и доступность) и с минимальными затратами. Изучение возможностей внедрение результатов данного проекта в персональную информационную систему.

Задачи исследования в рамках данного проекта:

- изучить и проанализировать существующие подходы к защите данных во внешних и облачных хранилищах, запатентовать наш метод защиты;

- рассмотреть возможность использования некриптографического метода защиты информации, основанного на побитовом разложении исходной информации на несколько потоков с последующим их расположением по нескольким, в т.ч. географически удалённым хранилищам данных;

- подать заявку, а в последствии запатентовать предложенный метод;

- реализовать данный метод в соответствующем программном обеспечении с учётом проведённых теоретических исследований;

- доработать диссертационную работу до финальной стадии защиты (т.е. выход на защиту в диссертационном совете по финалу проектных исследований (через 1 год)).

Научная новизна

Научная новизна данного проекта заключается в том, что разработка технологии защищённой передачи, хранения и обработки информации в облачных и корпоративных хранилищах данных, а также в любой другой базе данных, будет осуществляться без использования алгоритмов шифрования. Настоящий способ может быть воплощён в персональной информационной системе в различных формах, включая программное обеспечение, встроенное программное обеспечение, аппаратное обеспечение или их комбинацию. Данная технология радикально изменит общепринятую практику и парадигму, которая на сегодня состоит в хранении информации в одном физическом и географическом местоположении или с одним конкретным поставщиком услуг. В ходе реализации данного проекта будет обеспечена высоконадёжная защита от «противоправных» действий всех заинтересованных сторон, кроме самого владельца информации, как при передаче, так и при хранении информации. При дальнейшей работе и исследовании в данном направлении можно будет устранить все риски в основе своей и на стороне самого пользователя.

Теоретическая и практическая значимость

Теоретическая значимость заключается в исследовании заданного направления в рамках защищённой передачи и хранения данных в «облаках» и любых других внешних хранилищах данных, по мере возможности, и в ходе реализации данного метода создать программное обеспечение с учётом проведённых теоретических исследований и исключением ряда существенных недостатков «коллег», что представляет собой практическую значимость.

Методология и методы исследования

Предлагаемые методы и подходы к решению поставленных задач:

- метод побитового рассечения-разнесения на потоки (части) исходного сообщения разной длины;

- а также метод, который будет отражён непосредственно в самой заявке на патент, а по результатам патентопроизводства и в самом патенте.

План проводимых исследований:

- благодаря подачи заявки на патент в рамках данного проекта и дальнейшего патентопроизводства, а также, написания 4 статей, выступления на 3 конференциях и др. исследовательской деятельности, планируется завершить работу по доведению диссертации до защиты в диссертационном совете федерального государственного бюджетного образовательного учреждения высшего образования «Томского государственного университета систем управления и радиоэлектроники» по специальности ВАК 05.13.19. Методы и системы защиты информации, информационная безопасность.

- так как современный рынок технологий меняется очень быстро, то планируется периодический анализ современного состояния исследований в данной области, чтобы своевременно корректировать все необходимые исследования по данному проекту.

- в рамках изучения теоретических возможностей метода будет создана математическая модель, исследована стойкость метода по сравнению с использованием шифрования, дана исчерпывающая оценка по затратам ресурсов при реализации метода.

- реализовать данный метод в соответствующем программном обеспечении на языке Python с учётом проведённых теоретических исследований, обеспечить оптимальную работу на любом устройстве и на любой платформе. Разработать гражданский вариант и возможно для различных силовых структур и ведомств.

Положения, выносимые на защиту

На защиту выносятся:

- представленная реализация метода рассечения-разнесения, который по своим характеристикам может быть отнесён к некриптографическим методам защиты информации;

- результаты криптографического анализа метода рассечения-разнесения, применяемого для обеспечения безопасной передачи, хранения и обработки информации во внешних хранилищах данных;

- программно-алгоритмическая реализация метода;

- специальное программное обеспечение для работы с внешними хранилищами данных;

- применение программного продукта «Программа Vic.» в глобальной информационной системе безопасной передачи, хранения и обработки данных.

Степень достоверности и апробацию результатов

Результаты исследований, отражающие основные положения диссертационного исследования, обсуждены на 17 конференциях, среди которых: 5 Международных конференций; 1 Международный симпозиум; 6 Всероссийских конференциях; 2 Межведомственная конференция; 1 Межвузовская научно-практическая конференция с международным участием; 2 Всероссийская конференция с международным участием.

Публикации. По теме диссертационного исследования опубликовано 14 статей, 2 из которых включена в издания, входящие в перечень изданий, рекомендованных высшей аттестационной комиссией (ВАК), также 1 статья опубликована в рецензируемом научном журнале, индексируемом базой Scopus. В рецензируемых журналах и сборниках научных трудов – 11 статей, получено 1 свидетельство о государственной регистрации программы. Без соавторов опубликовано 10 работ.

Краткое содержание диссертации с упором на результаты, полученные за период реализации научного проекта в рамках гранта

В целях решения проблемы защиты информации защищённой передачи, хранения и обработки информации в облаке или внешнем хранилище данных, возникает необходимость создания ПО для организации защиты информации в рамках данной задачи, сюда же можно отнести и удалённую работу сотрудников компании. Это могут быть отдельные утилиты, либо же плагины для браузеров или ПО организации, через которые работает удалённый сотрудник. Тем самым будет организована защита информации в информационной системе (ИС) (в данном случае подразумевается система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию (ISO/IEC 2382:2015)) [35, 36]. В рамках ИС предполагается использование программы, обеспечивающей простую и надёжную защиту данных пользователя без использования криптографии, как основного средства защиты. Данное ПО работает с файлами на уровне битов, формируя из них несколько битовых последовательностей, условно назовём их потоками, т.е. речь идёт о побитовом рассечении-разнесении данных. Предлагаемая программа должна иметь простой интерфейс, позволять открывать файл и побитово преобразовывать его автоматически сгенерированным способом на несколько потоков данных, которые направляются в различные места хранения, более подробно можно прочитать в следующих работах [37-39]. При необходимости этот же пользователь, либо другой сотрудник организации, или доверенное лицо могут получить эти потоки из мест хранения и преобразовать их обратным способом в исходный файл. Причём эти потоки могут формироваться без использования криптографических методов, что позволит существенно сократить затраты. При этом стоит также подчеркнуть, что каждый отдельный поток не несёт в себе никакой полезной информации и потому не интересен для злоумышленника. В случае если злоумышленник сможет получить доступ к потокам вероятность восстановления исходного информационного сообщения остаётся низкой [37-39]. В данном ПО предполагается содержание следующих баз данных: места хранения данных; информация о передаваемых потоках. Предполагается создание кросс-платформенного ПО.

Алгоритм реализации защиты данных пользователя на удалённом месте работы предполагается обеспечить следующим образом (рис. 1):

1) Пользователю нужно отправить свои рабочие или личные данные в места хранения данных.
2) Далее пользователь открывает предлагаемое ПО, где ему открывается простой интерфейс (рис. 2) и предлагается сделать следующие шаги:
    1. Выбрать нужный файл на своём устройстве.
    2. Сгенерировать способ преобразования своих данных.
    3. Выбрать количество получаемых поток.
    4. Выбрать места хранения данных для отправки.
    5. Выполнить данную процедуру со всеми выбранными полями.
3) Необходимо отправить потоки через интернет в заранее выбранные места хранения данных (МХД1, МХД2, … , МХД(n))
4) При необходимости этот же пользователь, либо другой сотрудник организации, или доверенное лицо могут получить эти потоки из их мест хранения и преобразовать их обратным способом в исходный файл.

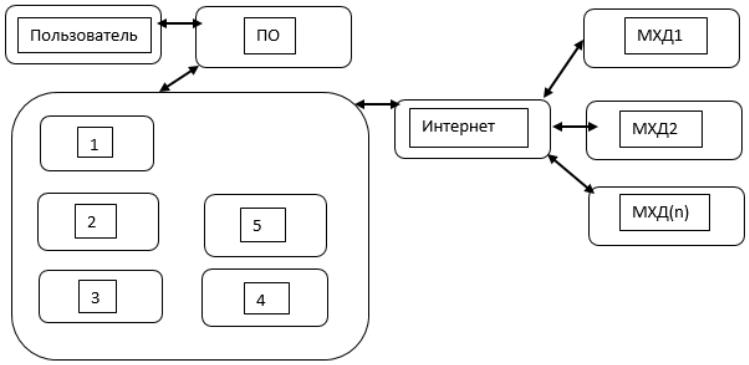


Рис. 1 – Алгоритм реализации защиты данных пользователя на удалённом месте работы

Технологию можно реализовать в виде плагина для любого из современных браузеров [40, 41]. Диалоговое окно с пользователем может иметь следующий вид (рис. 2). Пользователь – руководитель процесса может инициировать в программе создание информационных потоков на основании нового сообщения для безопасной передачи и хранения данных в географически удалённых местах хранения без использования шифрования, но в информационной системе можно предусмотреть применение различных криптографических методов в качестве дополнительных средств защиты. Для реализации этого действия, разработано простое диалоговое окно с пользователем (см. рис. 2, данное диалоговое окно позволяет: генерировать способ преобразования; выбирать количество потоков и места хранения данных), которое позволяет выбрать нужный объект, преобразования на потоки, а также в случае необходимости собрать обратно, сохраняя целостность данных (см. рис. 3).

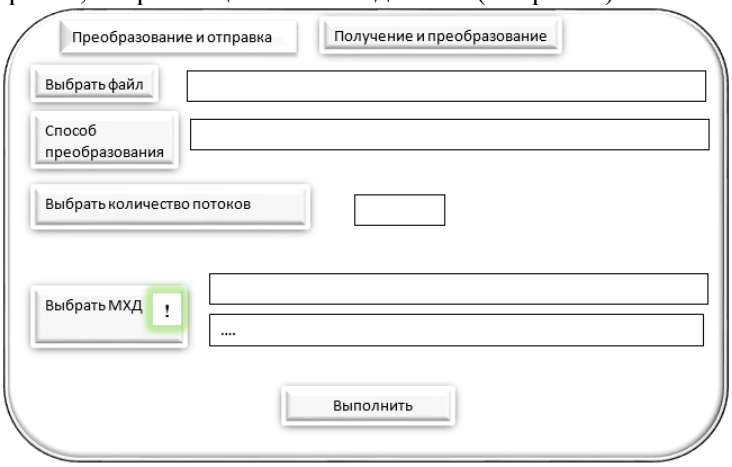


Рис. 2 – Возможное диалоговое окно с пользователем в ПО. Преобразование и отправка

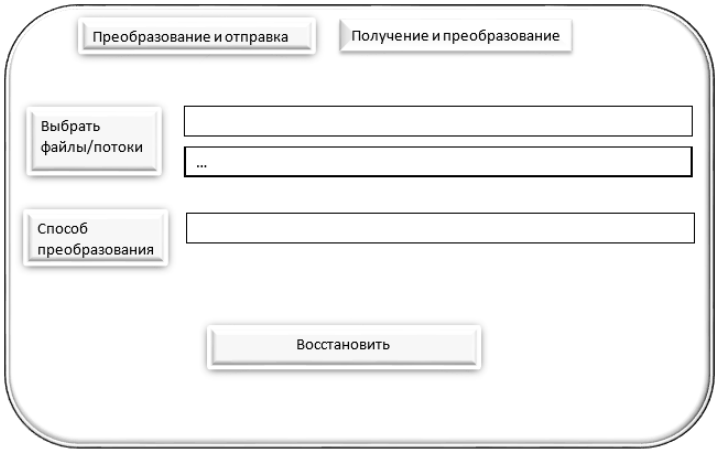


Рис. 3 – Получение и обратное преобразование

В Plug-in предполагается наличие двух баз данных: одна со списком мест хранения (например, облачные хранилища данных (ОХД)), куда могут быть отправлены данные; вторая с информацией о потоках передаваемого сообщения. В базе данных с местами хранения потоков предполагается, что пользователь сам может вносить изменения в список предполагаемых мест хранения, изначально возможно будет сформирован базовый список из популярных и рекомендованных (например, организацией или законодательством РФ) мест хранения. Во второй базе данных информация о

потоках может быть реализована через контрольную сумму или хэширование (например, SHA-256), т.е. в независимости от информации о потоках они всегда будут фиксированной длины заданной алгоритмом функции хэширования [42]. В качестве информации о потоках можно рассматривать адреса МХД (ОХД и т.д.) каждого потока [43].

Общий принцип побитового рассечения-разнесения можно сформулировать как способ защищённой передачи и хранения информации, размещаемой в облачных и внешних хранилищах данных, который включает в себя формирование и преобразование первичной цифровой информации, отличающийся тем, что биты первичной цифровой информации образуют несколько битовых последовательностей так, что существует не менее одного байта первичной цифровой информации, биты которого были помещены в разные последовательности, с последующей передачей и размещением последовательностей в разных хранилищах данных, причем обеспечивается обратимый и контролируемый процесс.

Программная реализация такого подхода даже в простейшем случае двух потоков с нормальным порядком даёт защищённость (1.1):

$$D = \frac{2^E}{\varepsilon^S}(2^L - 2) - 1 \,, \qquad (1.1)$$

где D – защищённость, E – неизвестное количество битов в сообщений, ε – вероятность получения доступа к потоку, S – количество потоков, L – длина потока.

Подытоживая, можно заключить следующее:

- в условиях повсеместного внедрения технологий облачного хранения данных остро встал вопрос защищённости размещаемой в них информации;

- облачные провайдеры недостаточно внимания уделяют вопросам защиты клиентских данных, что существенно снижает интерес к этой технологии;

- в случае криптографической защиты на стороне провайдера по-прежнему остаётся вопрос доверия к нему в случае размещения критически важной информации;

- одним из перспективных способов защиты информации в облаках является метод рассечения-разнесения, заключающийся в том, что информация делится на фрагменты, из которых по определённому алгоритму формируются потоки данных, направляемых в различные хранилища так, что владение одним потоком даже в незашифрованном виде не позволяет атакующему воспользоваться полученными сведениями;

- защищённость тем выше, чем выше коэффициент дробления информации и больше длина ключа. Количество потоков при этом существенной роли не играют;

- наибольшую защищённость обеспечивает побитовое рассечение, притом так, что потоки формируются из битов исходной информации случайным образом. Какой-либо регулярности следует избегать. Это обеспечивает высокий уровень защиты даже при получении атакующим всех потоков. При завладении лишь частью потоков перед ним стоит вообще труднореализуемая задача заполнения неизвестных битов, особенно если файлы имеют нетекстовый характер.

Рекомендации и перспективы дальнейшей разработки темы

Реализация предлагаемого ПО, его тестирование, осуществление его проверки на надежность, внедрение в информационную систему и разработка гражданского варианта, а также возможно для различных силовых структур и ведомств.

СПИСОК ЛИТЕРАТУРЫ

1. Айфон вместо отмычки. В России снизилось количество разбоев и грабежей, но стало больше киберпреступлений [Электронный ресурс]. – Режим доступа : https://rg.ru/2020/08/19/mvd-v-2020-godu-chislo-kiberprestuplenij-v-rossii-vyroslo-na-946.html
2. Заявление о конфиденциальности корпорации Майкрософт [Электронный ресурс]. – Режим доступа : https://privacy.microsoft.com/ru-ru/privacystatement
3. 5 причин не переживать за безопасность облаков | Безопасность облаков [Электронный ресурс]. – Режим доступа : https://www.youtube.com/watch?v=tUPhyVJF7B4
4. Способ преобразования данных с равновероятностной инициализацией [Текст]: пат. Российский патент 2017 года по МПК H04L9/16; RU 2 623 894 C1 / Мартынов А. П., Мартынова И. А., Марунин М. В., Николаев Д. Б., Фомченко В. Н. [Электронный ресурс]. – Режим доступа: https://patenton.ru/patent/RU2623894C1
5. Способ защиты текстовой информации от несанкционированного доступа [Текст]: пат. Российский патент 2012 года по МПК G06F 21/24 (2006.01); RU 2 439 693 C1 / Минаков В. А.,

Мирошников В. В., Толстихин Г. Н.; патентообладатель(и): ФГУ "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ГНИИИ ПТЗИ ФСТЭК). – заявл. 04.06.2010; опубл.10.01.2012, Бюл. №1. [Электронный ресурс]. – Режим доступа : www1.fips.ru/Archive/PAT/2012FULL/2012.01.10/DOC/RUNWC1/000/000/002/439/693/DOCUMENT.PDF

6. Способ защищённого хранения информации [Текст]: пат. Российский патент 2010 года по МПК H04M 1/68 (2006.01); RU 2 384 965 C2 / Щербаков А. Ю., Сотский С. В., Корольков А. Ю.; патентообладатель(и): Некоммерческая организация "Фонд сопровождения инвестиционных проектов "ГЕНКЕЙ". – заявл. 10.1.2008; опубл.20.03.2010, Бюл. №8. [Электронный ресурс]. – Режим доступа : www1.fips.ru/Archive/PAT/2010FULL/2010.03.20/DOC/RUNWC2/000/000/002/384/965/DOCUMENT.PDF
7. Способ защиты информации от несанкционированного доступа [Текст]: пат. Российский патент 2010 года по МПК G06F 12/14 (2006.01); RU 2 434 266 C2 / Минаков В. А.; патентообладатель(и): Федеральное государственное учреждение "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ГНИИИ ПТЗИ ФСТЭК). – заявл. 19.05.2009; опубл.27.11.2010, Бюл. №32. [Электронный ресурс]. – Режим доступа : http://www1.fips.ru/Archive/PAT/2011FULL/2011.11.20/DOC/RUNWC2/000/000/002/434/266/DOCUMENT.PDF
8. Система связи и способ связи [Электронный ресурс]. – Режим доступа : http://www1.fips.ru/Archive/PAT/2009FULL/2009.02.20/DOC/RUNWA/000/002/007/129/927/DOCUMENT.PDF
9. База Patentoscope [Электронный ресурс]. – Режим доступа : https://patentscope.wipo.int/search/ru/search.jsf
10. (WO2017146669) СИСТЕМА ПЕРЕДАЧИ КОДИРОВАННОЙ ИНФОРМАЦИИ [Электронный ресурс]. – Режим доступа : https://patentscope.wipo.int/search/ru/detail.jsf?docId=WO2017146669&recNum=5&office=&queryString=FP%3A%28защита+информации%29&prevFilter=&sortOption=Даты+публикации+по+убыванию&maxRec=118
11. (RU0002630751) СИСТЕМЫ И СПОСОБЫ ДЛЯ КРИПТОГРАФИЧЕСКОЙ БЕЗОПАСНОСТИ КАК СЕРВИС [Электронный ресурс]. – Режим доступа : https://patentscope.wipo.int/search/ru/detail.jsf?docId=RU204131873&recNum=4&office=&queryString=FP%3A%28защита+информации%29&prevFilter=&sortOption=Даты+публикации+по+убыванию&maxRec=118
12. (EA201291464) УСОВЕРШЕНСТВОВАННАЯ ЗАЩИТА ПРИ ПЕРЕДАЧЕ ДАННЫХ [Электронный ресурс]. – Режим доступа : https://patentscope.wipo.int/search/ru/detail.jsf?docId=EA95438829&recNum=39&office=&queryString=FP%3A%28защита+информации%29&prevFilter=&sortOption=Даты+публикации+по+убыванию&maxRec=118
13. (RU2012137719) ЗАЩИТА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ЗОН [Электронный ресурс]. – Режим доступа : https://patentscope.wipo.int/search/ru/detail.jsf?docId=RU96355530&recNum=38&office=&queryString=FP%3A%28защита+информации%29&prevFilter=&sortOption=Даты+публикации+по+убыванию&maxRec=118
14. (RU2014132162) ЗАЩИТА ДАННЫХ С ПЕРЕВОДОМ [Электронный ресурс]. – Режим доступа : https://patentscope.wipo.int/search/ru/detail.jsf?docId=RU159994690&recNum=24&office=&queryString=FP%3A%28защита+информации%29&prevFilter=&sortOption=Даты+публикации+по+убыванию&maxRec=118
15. (RU02155451) СПОСОБ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В МНОГОАБОНЕНТНОЙ СИСТЕМЕ И СИСТЕМА ДЛЯ ЕГО ОСУЩЕСТВЛЕНИЯ [Электронный ресурс]. – Режим доступа: https://patentscope.wipo.int/search/ru/detail.jsf?docId=RU29367237&recNum=90&office=&queryString=FP%3A%28защита+информации%29&prevFilter=&sortOption=Даты+публикации+по+убыванию&maxRec=118
16. (RU02300851) СИСТЕМА И СПОСОБ ОБРАБОТКИ ПОТОКА АУДИО/ВИДЕОДАННЫХ ДЛЯ ЗАЩИТЫ ДАННЫХ ОТ КОПИРОВАНИЯ [Электронный ресурс]. – Режим доступа :

https://patentscope.wipo.int/search/ru/detail.jsf?docId=RU29493805&rec Num=72&office=&queryString=FP%3A%28защита+информации%29&prevFilter=&sortOption=Даты+публикации+по+убыванию&maxRec=118
17. (RU02405199) ЗАЩИТА ЦЕЛОСТНОСТИ ПОТОКОВОГО КОНТЕНТА [Электронный ресурс]. – Режим доступа : https://patentscope.wipo.int/search/ru/detail.jsf?docId=RU29563861&rec Num=62&office=&queryString=FP%3A%28защита+информации%29&prevFilter=&sortOption=Даты+публикации+по+убыванию&maxRec=118
18. (RU2009145958) ЗАЩИТА КОНТЕНТА РЕАЛЬНОГО ВРЕМЕНИ В СЕТИ [Электронный ресурс]. – Режим доступа : https://patentscope.wipo.int/search/ru/detail.jsf?docId=RU75794634&rec Num=57&office=&queryString=FP%3A%28защита+информации%29&prevFilter=&sortOption=Даты+публикации+по+убыванию&maxRec=118
19. (RU2011147225) НАДЕЖНАЯ ЗАЩИТА ОТ КОПИРОВАНИЯ И/ИЛИ ВОСПРОИЗВЕДЕНИЯ [Электронный ресурс]. – Режим доступа : https://patentscope.wipo.int/search/ru/detail.jsf?docId=RU92347814&rec Num=42&office=&queryString=FP%3A%28защита+информации%29&prevFilter=&sortOption=Даты+публикации+по+убыванию&maxRec=118
20. (RU2012108120) СИСТЕМА СВЯЗИ, УСТРОЙСТВО СВЯЗИ, СПОСОБ СВЯЗИ И КОМПЬЮТЕРНАЯ ПРОГРАММА [Электронный ресурс]. – Режим доступа : https://patentscope.wipo.int/search/ru/detail.jsf?docId=RU95902754&rec Num=40&office=&queryString=FP%3A%28защита+информации%29&prevFilter=&sortOption=Даты+публикации+по+убыванию&maxRec=118
21. IBM Cloud Storage Object [Электронный ресурс]. – Режим доступа : https://www.ibm.com/cloud/object-storage
22. Безбогов А.А., Яковлев А.В., Шамкин В.Н. Методы и средства защиты компьютерной информации: Учебное пособие / Безбогов А.А., Яковлев А.В., Шамкин В.Н. // - Тамбов: Издательство ТГТУ, 2006. – с. 196.
23. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования / Партыка Т.Л., Попов И.И. // — М.: ФОРУМ: ИНФРА-М, 2002. - с. 368.
24. Лыгин Е.А. Тайнопись. Практическое пособие по ручному шифрованию. – 4-е изд., доп. / Лыгин Е.А. // – Саратов: издательство «Новый ветер», 2010. – 206 с.
25. Алексеев А.П. Информатика 2015: учебное пособие / Алексеев А.П. // М.: © СОЛОН-Пресс, — 2015. — с. 400.
26. Алексеев А.П. Пространственно-временное распыление информации / Алексеев А.П. // II Научный форум телекоммуникации: теория и технологии ТТТ-2017. Проблемы техники и технология телекоммуникаций ПТИТТ-2017, - материалы XVIII Международной научно-технической конференции. 2017. Издательство: Казанский государственный технический университет им. А.Н. Туполева (Казань) – с. 401
27. Способ пространственно-временной защиты информации [Текст]: Российский патент 2019 года по МПК H04L9/00. RU 2 703 972 C1 [Электронный ресурс]. – Режим доступа : https://patenton.ru/patent/RU2703972C1 (Дата обращения 20.03.2021)
28. Алексеев А.П. Многоуровневая защита информации / Алексеев А.П. // — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа : http://www.iprbookshop.ru/75387.html — Режим доступа: для авторизир. Пользователей — Самара : Поволжский государственный университет телекоммуникаций и информатики, 2017. — с. 128.
29. Алексеев А. П., Сокрытие сообщений путём их распыления в пространстве/ Алексеев А. П., Орлов В.В. // Инфокоммуникационные технологии. Том 6, № 3, 2008. с. 52-56.
30. Алексеев А.П., Блатов И.А., Макаров М.И. Оценка вероятности обнаружения мультимедиаконтейнеров при пространственно-временном распылении информации / Алексеев А.П., Блатов И.А., Макаров М.И. // - Учреждения: Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ). Выпуск: Том 11, № 3 (2013). - С. 91-95. Раздел: Статьи. Режим доступа : https://journals.eco-vector.com/2073-3909/article/view/56003
31. Алексеев А.П. Метод пространственно-временного распределения информации / Алексеев А.П. // Тезисы XVI РНТК ПГУТИ. Самара: ПГУТИ, 2009. с. 167-168.

32. Патент «СПОСОБ ПРОСТРАНСТВЕННО-ВРЕМЕННОЙ ЗАЩИТЫ ИНФОРМАЦИИ», заявителя Алексеев Александр Петрович (RU). RU 2 703 972 C1 [Электронный ресурс]. – Режим доступа : https://viewer.rusneb.ru/ru/000224_000128_0002703972_20191022_C1_RU?page=1&rotate=0&theme=white
33. (PCT/CA2013/000927) DATA DISTRIBUTION METHODS AND SYSTEMS [Электронный ресурс]. – Режим доступа : https://vod2.com/doc/vod2-patent-us.pdf
34. Патент US 10216822B2 от 26.02.2019 «Data distribution methods and systems» [Текст] Пат. 10,216,822 США: МПК G06F 16/1724 (20190101); G06F 16/278 (20190101); G06F 21/62 (20130101); G06F 16/182 (20190101); H04L 9/085 (20130101) / Rene Verge (Montreal, CA). – № 61722025; заявл. 01.05.2015; опубл. 15.10.2015, Бюл. № WO2014/066986.
35. Информационная система – Режим доступа : https://ru.wikipedia.org/wiki/Информационная_система
36. Международный стандарт ISO/IEC 2382:2015 Information technology — Vocabulary:
Information system: An information processing system, together with associated organizational resources such as human, technical, and financial resources, that provides and distributes information.
Information processing system: One or more data processing systems and devices, such as office and communication equipment, that perform information processing.
Data processing system: One or more computers, peripheral equipment, and software that perform data processing.
Режим доступа : https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en
Режим доступа : https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:fr
37. Шурховецкий Г.Н. Защита информации во внешних хранилищах данных методом рассечения-разнесения [Электронный ресурс] / Г.Н. Шурховецкий // Молодая наука Сибири: электрон. науч. журн. – 2020. – №3(9). – Режим доступа: http://mnv.irgups.ru/toma/39-2020, свободный. – Загл. с экрана. – Яз. рус., англ.
38. Шурховецкий Г. Н. Защита информации в облачных технологиях методом рассечения-разнесения // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. - 2021. - №03. - С. 231-236 DOI 10.37882/2223-2966.2021.03.38.
39. Шурховецкий Г. Н., Аршинский Л. В. Особенности применения метода рассечения—разнесения для безопасного хранения данных во внешних хранилищах // Информационные технологии. - 2021. - №05. - т. 27. - С. 259–266 УДК 004.056.53 DOI: 10.17587/it.27.259-266.
40. КриптоПро ЭЦП Browser plug-in – Режим доступа : https://www.cryptopro.ru/products/cades/plugin
41. Виды браузеров для интернета и какой лучше выбрать для работы – Режим доступа : https://prooneplus.ru/other/kakie-susestvuut-brauzery-pohozie-na-google-chrome
42. Что такое Хэширование? Под капотом блокчейна – Режим доступа : https://habr.com/ru/post/345740/
43. С. П. Серёдкин, Г. Н. Шурховецкий Обеспечение защиты информации в информационной системе // Информационная безопасность цифровой экономики : Материалы XVIII научно-теоретической конференции (в рамках IX Пленума регионального отделения Федерального учебно-методического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» по Сибирскому и Дальневосточному федеральным округам (СибРОУМО)), г. Хабаровск, 29 июня – 01 июля 2022 года. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2022. – 407 с. – ISBN 978-5-91434-074-9

Ярмак А.В.
СПбПУ Петра Великого, аспирант,
yarmak.av@ibks.spbstu.ru

КРИПТОГРАФИЧЕСКИЙ КОНТРОЛЬ ДОСТУПА К ДАННЫМ В СИСТЕМАХ С ИЕРАРХИЧЕСКОЙ СТРУКТУРОЙ НА ОСНОВЕ ИЗОГЕНИЙ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Аннотация: Представлены промежуточные результаты реализации научного проекта «Структурно-адаптивное управление доступом к данным в промышленном Интернете Вещей на основе постквантовых математических преобразований», направленного на обеспечение защиты от угроз, связанных с недоверенным облачным провайдером, при хранении данных в облачном хранилище. В качестве базовых постквантовых математических преобразований используются операции вычисления изогений эллиптических кривых, для которых задача поиска изогении, предположительно, является стойкой по отношению к атакам на квантовом компьютере.

Ключевые слова: криптографический контроль доступа, изогении эллиптических кривых, облачное хранилище, иерархия.

Актуальность темы исследования. Современные киберсреды, к которым можно отнести киберфизические системы, крупномасштабные АСУ ТП, системы Интернета Вещей и др., как правило, базируются на принципах облачного хранения данных для обеспечения централизованного доступа к информации в условиях географической распределенности компонентов-участников информационного взаимодействия. Широкое распространение такого способа хранения информации обусловлено отсутствием необходимости развертывания и обслуживания собственной инфраструктуры, меньшими затратами на персонал и ресурсы, возможностью обеспечения быстрого доступа к данным с различных устройств. Провайдеры облачных ресурсов, как правило, предоставляют традиционные инструменты по контролю доступа к информации. Такие программные решения функционируют на доверенном сервере, который хранит данные в открытом виде и по входящему запросу предоставляет информацию пользователю. Однако в случае недоверенного облачного провайдера или компрометации сервера возникает угроза несанкционированного доступа к данным.

Схемы криптографического контроля доступа возникли при попытке разработать систему многоуровневой защиты данных, способные обеспечить безопасность в различных окружениях, не требуя значительных изменений фундаментальной архитектуры [1]. Основная идея такого подхода – использование для контроля доступа к данным криптографических алгоритмов и протоколов. Схемы криптографического контроля доступа оказываются особенно полезны в ситуациях, требующих аутсорсинга данных, поскольку информация может быть зашифрована дважды, чтобы предотвратить ее просмотр поставщиком услуг, но при этом иметь возможность выполнять запросы или другие операции с данными и возвращать результат пользователю, который может расшифровать информацию, используя имеющиеся ключи. К достоинствам такого подхода можно отнести совместимость с любой классической моделью контроля доступа, хранение данных в облаке в зашифрованным виде, независимость от архитектуры файловой системы серверов облачного хранилища. Однако, при использовании классических алгоритмов шифрования возникает проблема увеличения цепочки хранимых ключей, более того, такой подход не позволяет учитывать иерархию прав пользователей, которая свойственна крупномасштабным системам.

Математический аппарат эллиптических кривых представляет собой объект изучения алгебраической геометрии, нашедший свое прикладное применение при построении асимметричных криптографических систем, а также представляющий интерес с точки зрения перспективности их использования в схемах постквантовой криптографии, предположительно стойких по отношению к атакам на квантовом компьютере [2].

Одной из вычислительно трудных задач постквантовой криптографии является задача поиска изогении эллиптических кривых. На данный момент не существует исследований, посвященных криптографическому контролю доступа, основанному на изогениях эллиптических кривых, и не известны адаптации подобных алгоритмов для облачных хранилищ с учетом структуры групп пользователей, что и обуславливает актуальность работы.

Степень разработанности темы исследования. Исследованиям в области изогений эллиптических кривых и возможности их применения для построения криптографических протоколов посвящены труды таких отечественных и зарубежных специалистов как О.Н. Василенко, А.Г. Ростовцев, А.Г. Столбунов, Л. де Фео, Д. Яо, С. Галбрайт, В. Кастрик, В. Сухарев, Д. Кохель, К. Костелло и других. Задача криптографического контроля доступа исследуется в трудах С.В. Запечникова, М. Каллахала, К. Сайя, Ю. Жень, Д. Бефенкурт, А. Кайем, В. Гойял.

Одним из основных примитивов, используемых при реализации контроля доступа на основе математических преобразований, является шифрование на основе атрибутов, при котором пользователь может получить доступ к информации только в том случае, если его набор атрибутов удовлетворяет определенным условиям. При этом политика доступа может как определяться закрытым ключом пользователя [3], так и содержаться в самом шифртексте [4]. Многие схемы атрибутного шифрования не решают проблему частых изменений в составе пользователей и динамического доступа, не позволяют обеспечить высокую пропускную способность при обработке запросов, иерархию [5-8].

В работе [9] учитывается иерархия пользователей при организации управления доступом на основе математических преобразований, но не поддерживаются операции обновления ключей и параметров доступа, что делает предлагаемую схему статической и ресурсозатратной в условиях крупномасштабных систем.

В публикации [10] решена проблематика динамического управления доступом, однако процедуры отзыва ключа требовали обновления параметров для узлов, расположенных по иерархии ниже, что влекло за собой большие вычислительные и коммуникационные издержки. В исследовании [11] авторы предлагают модель иерархии ролевых ключей, представляющую собой модификацию ролевой модели контроля доступа с использованием дополнительных математических преобразований на основе атрибутов и личностной информации. Выбранный аппарат эллиптических кривых позволил сделать схему масштабируемой, однако не обеспечивает постквантовый уровень стойкости.

Цель исследования – обеспечение защиты данных от угрозы несанкционированного доступа в иерархических системах на основе изогений эллиптических кривых.

Задачи исследования:

1. Анализ специфики организации управления доступом в иерархических системах, использующих принцип облачного хранения данных.
2. Разработка модели представления узлов в иерархической системе, определяющей возможные права доступа и кластеризацию участников системы.
3. Разработка метода криптографического контроля доступа к данным в облачном хранилище с учетом иерархической структуры групп пользователей на основе изогений эллиптических кривых.

В отличие от известных схем криптографического контроля доступа предлагаемый метод основан на вычислительно сложных задачах постквантовой криптографии и разработан с учетом специфики иерархических систем. Предлагаемый подход основан на создании модели представления узлов, использующей принцип кластеризации участников в группы по критериям, и задании отношений иерархии между группами. Контроль доступа на основе такого подхода осуществляется с помощью предварительных математических преобразований, осуществляемых над данными перед их отправкой в облако, с возможностью обновления параметров при реорганизации иерархии и изменения в составе участников и/или в политике доступа.

Научная новизна подчеркивается математическим аппаратом, используемым для решения данной проблемы: анализ аналогичных работ показал, что большая часть разработок основана либо на программных решениях, делегирующих право управления доступом облачному провайдеру, либо на математических задачах дискретного логарифмирования и разложения на множители, уязвимых к атакам с использованием квантового компьютера. На настоящий момент неизвестны научные работы, предлагающие постквантовые защитные преобразования для реализации контроля доступа к данным. Использование изогений эллиптических кривых позволяет обеспечить постквантовый уровень стойкости, а также реализовать дополнительные функциональные возможности. В частности, учет иерархии может быть достигнут за счет свойств графа изогений эллиптических кривых.

Теоретическая значимость работы состоит в установлении соответствия между характеристиками графа изогений эллиптических кривых и структурой графа иерархии. Практическая значимость результатов работы заключается в возможности применения предложенного метода в промышленном Интернете Вещей как примера распределенной системы с многоуровневой иерархической структурой для обеспечения защиты от угрозы несанкционированного доступа в условиях недоверия к облачному провайдеру.

Методология и методы исследования. Для решения поставленных задач использовались методы теории чисел, алгебры, алгебраической геометрии, математической логики, теории вероятностей и теории сложности.

Степень достоверности и апробация результатов. Достоверность и обоснованность результатов подтверждается всесторонним анализом предшествующих научных работ в данной области, полученными экспериментальными данными и апробацией результатов в научных публикациях и докладах на конференциях.

Промежуточные результаты проекта были представлены на следующих конференциях: всероссийской конференции «Информационные технологии в управлении, ИТУ-2022» (Санкт-Петербург, 2022 гг.), международной конференции «Sixth World Conference on Smart Trends in Systems, Security and Sustainability WorldS4» (Лондон, 2022 г.), а также отражены в двух публикациях, в том числе в рецензируемом издании из перечня Scopus, издании, индексируемом в РИНЦ, и свидетельстве о регистрации программы для ЭВМ.

Целью диссертационного исследования «Групповая аутентификация и криптографический контроль доступа в системах с иерархической структурой на основе изогений эллиптических кривых» является обеспечение защищенного группового взаимодействия и доступа к данным в иерархических системах на основе изогений эллиптических кривых.

Объектом исследования являются крупномасштабные системы с иерархической структурой участников. Предмет исследования – методы групповой аутентификации информации и криптографического контроля доступа к данным.

Положения, выносимые на защиту:

1. Модель группового взаимодействия узлов в условиях иерархии на основе аппарата атрибутивных метаграфов.
2. Метод иерархической групповой аутентификации информации на основе изогений эллиптических кривых.
3. Метод криптографического контроля доступа к данным на основе ролевой модели сущностей с использованием изогений эллиптических кривых.
4. Архитектура системы иерархической групповой аутентификации и контроля доступа к данным в промышленном Интернете Вещей.

Для описания структуры иерархии используется аппарат атрибутивных метаграфов [12], в рамках которого метаграф вложенности *n* представляет собой пару $G =< X, E >$, где:

– $X = \{x_1, ..., x_n\}$ – множество вершин;

– $E = \{e_1, ..., e_m\}$ – множество ребер.

Каждое ребро метаграфа $e_k = (V_i, W_i)$, $V_i, W_i \subseteq X$, соединяет два подмножества вершин. Задание вложенности вершин и ребер в некоторую метавершину осуществляется с помощью функций: $f_i^j : g_i^j(x_i^j, e_i^j) \to x_k^m$. Каждой вершине и ребру сопоставляется набор атрибутов: $x_i \leftarrow \{attr_j\}, e_k \leftarrow \{attr_l\}$. В рамках предложенной модели вершинами метаграфа являются ключи, соответствующие некоторой группе (роли) пользователей, что указывается с помощью атрибутов. В качестве атрибутов вершины могут быть: группа (роль) пользователей, обладающих этим ключом, права доступа. Отношение вложенности в данном случае представляет собой отношение, задающее иерархию ключей и возможность доступа к данным, зашифрованным на конкретном ключе.

В общем случае, криптосистемы (КС) с открытым ключом на изогениях эллиптических кривых можно разделить на три семейства: CRS-схемы [13-14], SIDH-схемы [15] и CSIDH-схемы [16]. Они отличаются типом кривых, используемых в конструкции, принципами построения протоколов (Табл. 1), требованиями к параметрам, используемыми вычислительно сложными задачами (Табл.2).

Построение графа изогений позволяет рассмотреть действие отображений на множестве эллиптических кривых с равным числом точек. Граф изогений эллиптических кривых $G_l(K) = (V_l(K),\ E_l(K))$ – неориентированный (так как для каждого отображения существует дуальное) граф, множество вершин $V_l(K)$ которого представляет собой классы изоморфизмов кривых, заданных над полем K, а множество ребер $E_l(K) \subseteq V_l \times V_l$ – изогении степени l. Вид графа зависит от типа эллиптических кривых: несуперсингулярных (т.е. кривых, для которых след эндоморфизма Фробениуса $t \equiv 0 \ mod\ p$), или суперсингулярных (имеющих след $t \equiv 0 \ mod\ p$).

Вычисление графа изогений суперсингулярных и несуперсингулярных кривых формализованы в виде алгоритма 1 и 2.

Табл. 1. Типы криптосистем на изогениях

	CRS-схемы	**SIDH-схемы**	**CSIDH-схемы**
Поле	F_p	F_{p^2}	F_p
Вид характеристики	Любое простое число	$p = l_A^{e_A} l_B^{e_B} f \pm 1,$ $l_A^{e_A} \approx l_B^{e_B}$	$p = 4l_1 l_2 \ldots l_n \pm 1,\ \ l_1, l_2, \ldots, l_n$ – малые простые, $p \equiv 3 \pmod 8$
Длина характеристики	$p \approx 2^{4\lambda}$ для уровня безопасности в λ бит	$p \approx 2^{6\lambda}$ для уровня безопасности в λ бит	$p \approx 2^{512}, 2^{1024}, 2^{1792}$ для уровня безопасности в 64, 96, 128 бит
Тип кривых	Несуперсингулярные	Суперсингулярные	Суперсингулярные
Степени изогений	$l_i : \left(\frac{T^2 - 4p}{l_i} \right) = 1,$ где $T -$ след эндоморфизма Фробениуса	Степени l_A, l_B (как правило, $l_A = 2,$ $l_B = 3$)	$l_1, l_2, \ldots, l_n$

Табл. 2. Задачи, положенную в основу безопасности криптосистем на изогениях

Обозначение	**Описание**	**Тип КС**	**Дано**	**Найти**
GAIP	Аналог задачи дискретного логарифмиро-вания	CRS, CSIDH	$E_1/\mathbb{F}_q$ и $E_2/\mathbb{F}_q$ –кривые, $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q),$ $End(E_1) = End(E_2) \cong O_D$	$\beta \in Cl(O_D)$: $\beta * E_1 \cong E_2$
DSSI	Задача распознавания изогении ЭК	SIDH	$E/\mathbb{F}_{p^2}$ и $E_A/\mathbb{F}_{p^2}$ – суперсинулярные кривые	$\exists \varphi_A : E \xrightarrow{?} E_A,$ $deg\varphi = l_A^{e_A}$
CSSI	Задача поиска изогении ЭК	SIDH	$E/\mathbb{F}_{p^2}, E_A/\mathbb{F}_{p^2},\ \varphi_A(P_B),$ $\varphi_A(Q_B),$ где: $\varphi_A : E \to E_A,$ $\#Ker\varphi_A = l_A^{e_A},$ $< P_B, Q_B > \ = E[l_B^{e_B}],$ $p = l_A^{e_A} l_B^{e_B} f \pm 1$	образующую $< R_A > = Ker\varphi_A$ ядра изогении $\varphi_A,$ где $R_A \in E[l_A^{e_A}]$
SSDDH	Аналог задачи распознавания Диффи-Хеллмана	SIDH	$E/\mathbb{F}_{p^2}, E_A/\mathbb{F}_{p^2}, E_B/\mathbb{F}_{p^2},$ $\varphi_A(P_B), \varphi_A(Q_B), \varphi_B(P_A),$ $\varphi_B(Q_A),$ $E_C/\mathbb{F}_{p^2},$ где $E_C \cong E/ < m'_A P_A + n'_A Q_A, m'_B P_B + n'_B Q_B >,$ $\varphi_A : E \to E_A,$ $\varphi_B : E \to E_B$	Верно ли, что $E_{AB} \cong E_C,$ где $E_{AB} \cong E/ < m_A P_A + n_A Q_A, m_B P_B + n_B Q_B >;$
SSCDH	Аналог вычислительной задачи Диффи-Хеллмана	SIDH	$E/\mathbb{F}_{p^2}, E_A/\mathbb{F}_{p^2}, E_B/$ $\mathbb{F}_{p^2}, \varphi_A(P_B), \varphi_A(Q_B),$ $\varphi_B(P_A), \varphi_B(Q_A),$ где $\varphi_A : E \to E_A,$ $\varphi_B : E \to E_B$	$j(E_{AB}),$ где $E_{AB} = E/ < m_A P_A + n_A Q_A, m_B P_B + n_B Q_B >$
CSI-CDH	Аналог вычислительной задачи Диффи-Хеллмана	CSIDH	$E/\mathbb{F}_p, E_A/\mathbb{F}_p, E_B/\mathbb{F}_p,$ $End(E) \cong End(E_A) \cong End(E_B) \cong O_D$	$E_C = [\alpha][\beta] * E,$ где: $\alpha, \beta \in Cl(O_D),$ $E_A = [\alpha] * E,$ $E_B = [\beta] * E$

Обозначение	Описание	Тип КС	Дано	Найти
CSI-DDH	Аналог задачи распознавания Диффи-Хеллмана	CSIDH	$E/\mathbb{F}_p, E_A/\mathbb{F}_p, E_B/\mathbb{F}_p,$ $E_C/\mathbb{F}_p$, где $E_A = [\alpha] * E,$ $E_B = [\beta] * E$	Верно ли, что $E_C \stackrel{?}{=} E_{AB}$, где $E_{AB} = [\alpha][\beta] * E$
SS-EndRing	Задача вычисления кольца эндоморфизмов кривой	SIDH, CSIDH	$E/\mathbb{F}_p$ (или $E/\mathbb{F}_{p^2}$) – суперсингулярная кривая	$End(E)$

Алгоритм 1. Построение графа изогении несуперсингулярных кривых.

Вход: ограничение h_{max} на число классов h_{D_π}.

Выход: граф G_l изогений для степени l.

1. Подобрать характеристику поля p и значение следа $T < 2\sqrt{p}$ таким образом, чтобы дискриминант эндоморфизма Фробениуса $D_\pi = T^2 - 4p$ был фундаментальным (т.е. $D_\pi \equiv 1 (mod\, 4)$ и свободен от квадратов, либо $D_\pi \equiv 0 (mod\, 4)$, где $D_\pi / 4 \equiv 2,3 (mod\, 4)$ и свободно от квадратов).

2. Найти число классов $h_{D_\pi} = \#Cl\left(O_{D_\pi}\right)$, проверить, что оно является простым числом и $h_{D_\pi} < h_{max}$. Если число классов составное, то перейти на шаг 1.

3. Вычислить полином Гильберта $H_{D_\pi}(X)$, задающий поле классов, и над F_p найти его корни, представляющие собой j-инварианты изогенных эллиптических кривых. Выбрать начальную кривую с j-инвариантом j_0.

4. Построить цепочку j-инвариантов изогенных кривых $j_0 \to j_1 \to j_2 \to \ldots \to j_0$ путем нахождения корней модулярного полинома $\Phi_l(j_i, Y) (mod\, p), i = 0,1,\ldots,h_{D_\pi} - 1$. Для выбора направления движения задать одно из собственных значений π_1, π_2 эндоморфизма Фробениуса.

5. Построить граф $G_l = (V_l,\ E_l)$ с множеством вершин $V_l = \left\{ j_0, j_1, \ldots, j_{h_{D_\pi}-1} \right\}$ и множеством ребер E_l, элементы которого представляют пары $(j_i, j_k) : \Phi_l(j_i, j_k) \equiv 0 (mod\, p)$.

Результат: граф G_l.

Алгоритм 2. Вычисление графа изогений суперсингулярных кривых.

Вход: суперсингулярная кривая $E\left(\mathrm{F}_{p^2}\right),\ j_0 = j(E)$.

Выход: граф G_l изогений степени l.

1. Инициализировать структуры для хранения вершин (посещенных и вершин на очереди для посещения): $visited \leftarrow \{\varnothing\}, queue \leftarrow \{j_0\}$.

2. Задать структуру графа $G_l = (V_l,\ E_l),\ V_l \leftarrow \{\varnothing\},\ E_l \leftarrow \{\varnothing\}$.

3. Пока структура $queue$ не пуста, выполнить следующие шаги:

   3.1. Извлечь первый элемент из множества вершин на очереди: $j_i \leftarrow queue.pop(0)$.

   3.2. Добавить элемент j_i в список посещенных: $visited \leftarrow visited \cup \{j_i\}$, а также в список вершин графа: $V_l \leftarrow V_l \cup \{j_i\}$.

   3.3. С помощью модулярного полинома вычислить всех изогенных с j_i вершин-соседей (вершины указываются с учетом кратности): $j_{nbrs} \leftarrow \left\{ j_{nbrs}^{(1)}, j_{nbrs}^{(2)}, \ldots, j_{nbrs}^{(m)} \right\}$.

   3.4. Для каждой вершины-соседа $j_{nbrs}^{(k)}$ из j_{nbrs} выполнить:

3.4.1. Если $j_i < j_{nbrs}^{(k)}$ или $j_i = j_{nbrs}^{(k)}$, то $V_l \leftarrow V_l \cup \left\{ j_{nbrs}^{(k)} \right\}$, $E_l \leftarrow E_l \cup \left(j_i, j_{nbrs}^{(k)} \right)$.

3.4.2. Если $j_{nbrs}^{(k)} \notin visited$ и $j_{nbrs}^{(k)} \notin queue$, то $queue \leftarrow queue.add\left(j_{nbrs}^{(k)} \right)$.

Результат: граф G_l.

Для установления общего ключа группы (роли), состоящей из n пользователей, была разработана схема на изогениях (Рис.1). Предлагаемый протокол является оптимистичным, т. е. предполагает доверие к менеджеру группы. Сам процесс установления группового ключа требует от менеджера группы больших вычислительных мощностей.

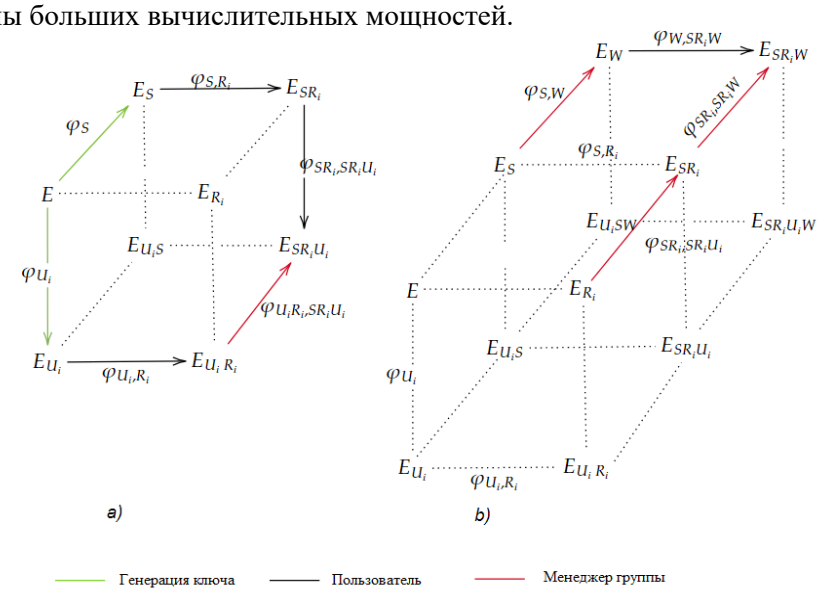


Рис. 1. Вычисление изогений a) аутентификация b) установление ключа группы

В Табл. 3 приведены сводные данные о количестве операций, необходимых на каждом этапе, где IG — вычисление изогении согласно формулам Велу, IC — вычисление образа точки, H — вычисление хэш-значения, SE — симметричное шифрование/расшифрование, BM — вычисление билинейного отображения. Следует отметить, что при расчете не учитывались операции сложения точек, генерации ядра изогении, вычисления координат точек.

Табл. 3. Базовые операции в схеме установления ключа группы

Раунд	**Менеджер группы**	**Пользователь**
Генерация ключей	1IG+6IC	1IG+2IC
1	—	4IG+6IC+1H+1SE
2	(3n+1)IG+2nH+2nSE+3nIC	1IG+2H+1SE+1BM

Поскольку количество операций, выполняемых менеджером, зависит от размера группы, данная схема имеет ограничения, которые необходимо учитывать исходя из вычислительных возможностей доверенной стороны. Также недостатком является тот факт, что при удалении члена группы необходимо перегенерировать общий ключ группы.

На основе ролевой модели доступа была разработана схема криптографического контроля доступа с использованием изогений эллиптических кривых, поддерживающая следующие функции:

- добавление субъектов (пользователей);
- добавление ролей
- добавление объектов (файлов);
- назначение ролей пользователям;
- назначение разрешений ролям;
- исключение пользователей из ролей;
- отмену назначенных разрешений.

В качестве модели криптографического контроля доступа была выбрана модель гибридного шифрования, так как для её реализации можно использовать существующую криптосистему с открытым ключом на изогениях. В предлагаемой схеме, являющейся развитием работы [17], в облачном хранилище в зашифрованном виде размещаются файлы, а также политика безопасности, управление которой осуществляет администратор. Выделяются следующие сущности: пользователи

(U), роли (R), файлы (F), таблица FK (FileKeys), связывающая роли и файлы, и таблица RK (RoleKeys), ассоциирующая пользователи и роли.

Основная идея схемы заключается в том, что для шифрования в таблице FK и аутентификации используется некоторая кривая $E_R^{'}$, которая известна только администратору и участникам роли. Данную кривую можно использовать для подтверждения членства в группе: Пользователь сначала вычисляет данную кривую, затем, используя хэш-значение измененного файла, вычисляет изогенную кривую, которая будет использоваться при внесении изменений в данные. На основе этого администратор может сделать вывод, что пользователю известны ключи роли, а также что пользователь подтверждает внесённые изменения. Результаты тестирования программного прототипа, реализованного в системе компьютерной алгебры SageMath, показывают, что скорость операций в случае введенных оптимизаций увеличилась в 1,5 – 2,5 раза. Такой подход позволяет реализовать модель контроля доступа на основе ролей даже при ограниченном наборе инструментов, представленных облачным провайдером. Дальнейшее направление исследования связано с анализом безопасности предложенных схем, а также установлением ограничений и требований к параметрам в случае использования в промышленном Интернете Вещей.

СПИСОК ЛИТЕРАТУРЫ

1. Kayem, A. V. D. M. Adaptive cryptographic access control/ A. V. D. M. Kayem, S. G. Akl, P. Martin. — NY.: Springer Science & Business Media, 2010. — 138 с.
2. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer //SIAM review. —1999. — Т. 41. — №. 2. — С. 303-332.
3. Goyal, V. et al. Attribute-based encryption for fine-grained access control of encrypted data/ V. Goyal, O. Pandey, A. Sahai, B. Waters //Proceedings of the 13th ACM conference on Computer and communications security. – Acm, 2006. — С. 89-98.
4. Bethencourt, J. Ciphertext-policy attribute-based encryption/ J. Bethencourt, A. Sahai, B. Waters //2007 IEEE symposium on security and privacy (SP'07). — IEEE, 2007. — С. 321-334.
5. Fan, C. I. Arbitrary-state attribute-based encryption with dynamic membership/C.I. Fan, V. S. M. Huang, H. M. Ruan //IEEE Transactions on Computers. — 2013. — Т. 63. — №. 8. — С. 1951-1961.
6. Jin, X., A unified attribute-based access control model covering DAC, MAC and RBAC/ X. Jin, R. Krishnan, R. Sandhu //IFIP Annual Conference on Data and Applications Security and Privacy. — Springer, Berlin, Heidelberg, 2012. — С. 41-55.
7. Xie, X. et al. An Efficient Ciphertext-Policy Attribute-Based Access Control towards Revocation in Cloud Computing/ X. Xie, H. Ma, J. Li, X. Chen //J. Univers. Comput. Sci. — 2013. — Т. 19. — №. 16. — С. 2349-2367.
8. Qi, S. Efficient data access control with fine-grained data protection in cloud-assisted IIoT / S. Qi, Y. Lu, W. Wei, X. Chen //IEEE Internet of Things Journal. — 2020. — Т. 8. — №. 4. — С. 2886-2899.
9. Gudes, E. The design of a cryptography based secure file system //IEEE Transactions on Software Engineering. — 1980. — №. 5. — С. 411-420.
10. Atallah, M. J. Dynamic and efficient key management for access hierarchies/ M. J. Atallah, M. Blanton, N. Fazio, K. B. Frikken //ACM Transactions on Information and System Security (TISSEC). — 2009. — Т. 12. — №. 3. — С. 1-43.
11. Новохрестов, А. К.Многоуровневая модель информационной системы на основе атрибутивных метаграфов/ А. К. Новохрестов, А. А. Конев //Электронные средства и системы управления. Материалы докладов Международной научно-практической конференции. – федеральное государственное бюджетное образовательное учреждение высшего образования Томский государственный университет систем управления и радиоэлектроники, 2015. — №. 1-2. — С. 184-188.
12. Zhu, Y. Cryptographic role-based security mechanisms based on role-key hierarchy / Y. Zhu, G. J. Ahn, H. Hu, H. Wang //Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. — 2010. — С. 314-319.
13. Couveignes J. M. Hard homogeneous spaces //Cryptology ePrint Archive. —2006.
14. Rostovtsev, A.Public-key cryptosystem based on isogenies/ A. Rostovtsev, A. Stolbunov//Cryptology ePrint Archive. — 2006.

15. De Feo, L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies/ L. De Feo, D. Jao, J, Plut // Post-Quantum Cryptography. – Lecture Notes in Computer Science. — 2006. — Vol.4341. — P.193-210.
16. Castryck, W. CSIDH: an efficient post-quantum commutative group action/ W. Castryck, T. Lange, C. Martindale, L. Panny, J. Renes //International Conference on the Theory and Application of Cryptology and Information Security. – Springer, Cham, 2018. — С. 395-427.
17. Qi, S. Crypt-DAC: cryptographically enforced dynamic access control in the Cloud/ S. Qi, Y. Zheng //IEEE Transactions on Dependable and Secure Computing. — 2019. — Т. 18. — №. 2. — С. 765-779.

РАЗДЕЛ 4. НАУЧНЫЕ ДОКЛАДЫ ГРАНТОПОЛУЧАТЕЛЕЙ 2022 ГОДА – СОИСКАТЕЛЕЙ УЧЁНОЙ СТЕПЕНИ КАНДИДАТА НАУК

Аверьянов В.С.
ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф.Решетнева», аспирант,
averyanov124@mail.ru

О НЕКОТОРЫХ ВОПРОСАХ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ БЕЗОПАСНОСТИ С ФАЗО-ВРЕМЕННЫМ И ПОЛЯРИЗАЦИОННЫМ КОДИРОВАНИЕМ ИНФОРМАЦИИ

Аннотация: В настоящем исследовании автором представлен ряд существующих проблем по распределению ключей безопасности в случаях организации защищенных каналов связи наземного и космического исполнения. Сегодня они требует передовых - прогрессивных технических решений, в первую очередь на программно-аппаратном уровне, включающем в себя более совершенные, отличные от классических механизмов обмена данными между легитимными пользователями. К одному из таких относятся киберфизические системы и сети связи построенные на постулатах квантовой механики, физики, оптики и теории информации включая организационно-технический комплекс мероприятий по обеспечению информационной безопасности. Автором отмечено, что оптико-электронные устройства в составе таких систем генерируют, транслируют, детектируют и осуществляют измерения кодированных последовательностей, представленных элементарными световыми частицами - фотонами. В том числе к основным проблемам относится: формирование частиц, как правило, однофотонным источником ослабленного лазерного излучения, несовершенство фотоприемных устройств, существующие уязвимости аутентичных каналов связи, когда факт перехвата фотона критическим образом сказывается на процедурах приема и согласования, где легитимный пользователь не получает никакой полезной информации, а услуга связи предоставляется некачественно.

Ключевые слова: безопасность, квантовые сети, киберфизическая система, поляризационное кодирование, распределение ключей, утечка информации, фазо-временное кодирование, элементарные частицы.

Возможность передачи секретной информации, или организация конфиденциального общения так, чтобы два легитимных пользователя (человека, субъекта) проводили обмен данными, не опасаясь за их сохранность, а третья сторона не узнала и малой части содержимого таких сообщений волновало человечество с самого начала своего существования. В разные эпохи были придуманы различные ухищрения, например шифр Цезаря (шифр подстановки в котором каждый символ текста заменяется символом, находящимся в алфавите на некотором постоянном числе позиций левее или правее от основного знака), или то, что сейчас всем известно как трафареты, книги шифров и стеганография, но математические вычисления указывают на то, что все эти способы закрытия/раскрытия информации являются не достаточно криптостойкими [1], то есть не гарантируют надежной защиты информации и обеспечения надлежащими механизмами безопасности транслируемых данных. Возвращаясь к современным методам сокрытия информационного потока от злоумышленника, относительно недавно - в середине прошлого века, в России и США практически одновременно экспериментально был установлен абсолютно секретный способ организации удаленного обмена сообщениями [2]. К основным его принципам относится выполнение трёх условий:

1. Первое - ключ безопасности и его компоненты. То есть та последовательность логических символов или информационных бит (0 и 1), которые и защищают информацию. При этом набор символов в такой последовательности должен быть абсолютно случайным и произвольным, что может гарантировать хоть какую-то информационную безопасность и имитостойкость ключей к машинным вычислениям.
2. Ко второму условию относится длина ключа, которая должна быть не меньше чем длина самого защищаемого сообщения.
3. И третье условие это однократность применения. Здесь подразумевается то, что ключ безопасности должен быть использован один раз для каждой новой информационной посылки.

Эти три простых условия являются довольно сильными в контексте механизмов защиты, но так или иначе реализуемы в существующих телекоммуникационных системах. Например, всем известная

по литературе и по фильму история с немецкой шифровальной машиной «Enigma», которая была вскрыта именно потому, что ключ безопасности использовался неоднократно. Из вышеизложенных постулатов, наиболее сильным является однократность применения ключа. На практике это означает, что два пользователя обмениваются закрытым ключом безопасности в каждой новой информационной посылке, то есть когда инициирована процедура передачи данных (секретных сообщений). Данное обстоятельство указывает на то, что субъекты должны организовать канал связи с явным и понятным обеим сторонам распределением ключа, или того самого трафарета который упоминается в отечественной и зарубежной литературе по информационной безопасности. Распределение ключевой последовательности и есть важное обстоятельство, над которым трудятся научные коллективы и объединения многих стран.

В настоящее время к одному из способов, гарантирующих высокий уровень информационной безопасности относится квантовое распределение ключевой последовательности. Для того, чтобы понять что происходит внутри технологии рассмотрим каноническую схему работы телекоммуникационной системы по протоколу BB84 [3], например с поляризационным кодированием [4, 11] представленную на рисунке 1.

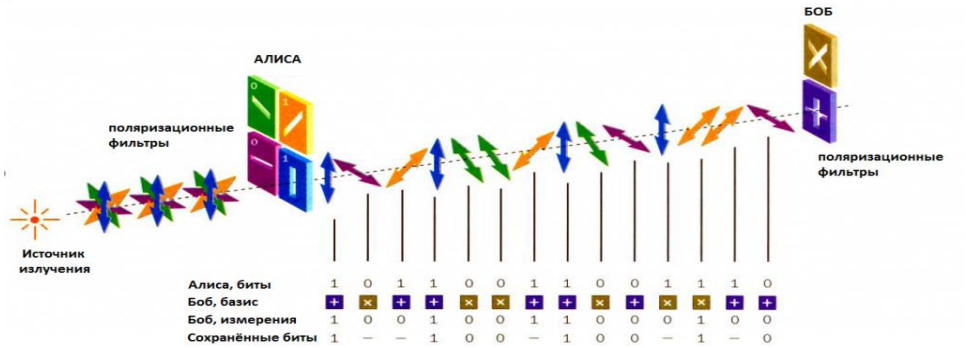


Рис. 1. Схема квантового распределения ключей безопасности по протоколу BB84

Стоит отметить, что это не криптографическая технология. В её основе лежат фундаментальные принципы квантовой физики, механики, оптики, теории информации, информационной безопасности. Новые механизмы защиты информационного потока в квантовых системах с КРК достижимы механическим кодированием последовательности фотонов, который находится в одном из четырех различных поляризационных состояний, два из которых ортогональны. Принято, что существуют два ортонормированных базиса $|0\rangle$ и $|1\rangle$, а также соответствующие им состояния поляризации L и R (левосторонняя и правосторонняя). Обозначим сторону отправитель как А, сторону получатель Б, тогда, алгоритмическая часть обмена информационными данными представлена в следующем виде:

1. А готовит кодированную ключевую последовательность фотонов в виде кубит в произвольных базисах $|0\rangle$, $|1\rangle$ с состояниями поляризации L либо R после чего отправляет готовые информационные пакеты Б;
2. Б регистрирует фотоны на фотодетекторах, проводит измерения полученной ключевой последовательности в случайно выбранных базисах для логического 0 и 1 с поляризацией L или R;
3. А по аутентичному классическому каналу связи сообщает Б о базисах для каждой информационной посылки, не раскрывая основной информации о состояниях фотонов;
4. Б обменивается информацией с А о выбранных базисах процедуры измерений, сам результат при этом остается на стороне Б;
5. А и Б обладая информацией о переданных и измеренных базисах инициируют процедуру «просеивания» ключевой последовательности, результат такой операции – формирование предварительного ключа безопасности;
6. А и Б по классическому открытому каналу связи проводят сравнение базисных состояний фотонов из конечной последовательности, не соответствие результатов сигнализирует о присутствии нарушителя в системе, в таком случае информационный обмен данными прерывается, а канал связи блокируется.

После выполнения вышеизложенных пунктов из предварительного ключа безопасности исключаются не совпавшие базисы, оставшаяся последовательность является основным ключом безопасности.

Современные исследования в области «квантовых технологий» указывают на то, что детектирование любых попыток подслушивания квантового канала связи приводит к искажению состояний последовательности фотонов, как следствие возникновению системных сбоев на стороне

измерений. Данный факт обусловлен теоремой о запрете копирования [5]. Обнаружение атакующих воздействий в полной мере проявляется в процедуре «просеивания», где отправленные синхропосылки сопоставляются с результатом измерений. Телекоммуникационные системы с КРК на постулатах квантовой механики позволяют связать наблюдаемые величины (координаты, импульс частиц, ток, электрическое и магнитное поле) через соотношение неопределенностей Гейзенберга с утечкой информации к злоумышленнику. Экспериментально доказано, если процент ошибок ниже отметки в 11% [6] от общего числа отправленных информационных синхропосылок, возможно их «исправление» посредством перемешивания и разбиения ключевой последовательности на отдельные фрагменты, которые легитимные пользователи проверяют на тактовую чётность в нескольких временных окнах, отбрасывая каждый раз не совпавшие значения. Таким образом, отброшенные значения уменьшают длину основного секретного ключа, что соответствует процедуре «сжатия». В результате у пользователей формируется «очищенный ключ», а злоумышленник получает только часть ключевой последовательности, не нарушая криптостойкости основного секретного ключа безопасности.

Вместе с тем существуют атаки на оптико-электронную аппаратуру и физические состояния фотонов, эффективность которых подтверждена фундаментально и экспериментально. Например, в инициированной процедуре «исправления» ошибок длительность синхроимпульса и его положение по временной оси внутри единичного строба формируется таким образом, что квантовое состояние не попадает в зону чувствительности детектора. Данный факт указывает на невозможность детектирования фотона приемной стороной [7]. Здесь, злоумышленники, действуя в паре подменяют ранее перехваченные чистые однофотонные состояния – ложными, с опережением по времени и продолжительности сигнала, навязывая скомпрометированный информативный сигнал фотодетекторам приемной стороны. В результате атаки на техническую реализацию, используя разную временную зависимость чувствительности фотодетекторов атакующие субъекты получают полный доступ к кодированной последовательности. Несанкционированные действия распространяются не только на поляризационное кодирование, но и фазовое. Экспериментальная система связи с КРК и способ разрушающего воздействия описаны в научной статье “Quantum hacking: Experimental demonstration of time-shift attack against practical quntum-key-distribution systems” [8]. Серии экспериментов для случаев фазового и поляризационного кодирования подтверждают факт того, что при трансляции кодированных последовательностей от стороны А к Б сама попытка злоумышленника перехватить и произвести подмену базисных состояний фотона регистрируются пользователями [9, 10] в виде существенного повышения уровня системных ошибок на приемной стороне.

СПИСОК ЛИТЕРАТУРЫ

1. Аверьянов В.С., Карцан И.Н. Оценка защищенности киберфизических систем на основе общего графа атак // Южно-Сибирский научный вестник. 2022. Т.1. С.30-35.
2. Averyanov V. S., Kartsan I. N. et al. Quantum technologies in the NGSO class orbits //Journal of Physics: Conference Series. – IOP Publishing, 2020. – Т. 1515. – №. 2. – С. 022032.
3. C.H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (IEEE Press, New York, 1984), pp. 175-179.
4. Sebastien Sauge, Lars Lydersen, Andrey Anisimov, Johannes Skaar and Vadim Makarov. “Controlling an actively-quenched single photon detector with bright light” // Optics Express Vol.19, Issue 23, pp.23590-23600, 2011.
5. W.K. Wootters, W.H. Zurek – “A single quantum cannot be cloned” // Nature – 1982 – Vol. 299 – P.802-803.
6. Shor P. W., Preskill J.” Simple proof of security of the BB84 quantum key distribution protocol” //Physical review letters. – 2000. – Т. 85. – №. 2. – С. 441.
7. Vadim Makarov, Andrey Anisimov and Johannes Skaar, Physical Review, A74, 022313, 2006.
8. Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen and Hoi-Kwong Lo. “Quantum hacking: Experimental demonstration of time-shift attack against practical quntum-key-distribution systems” // Physical Review A(78), 042333, 2008
9. Vadim Makarov and Johannes Skaar. “Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols”, 2007
10. Vakhitov A., Makarov V., Hjelme D. R. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography //Journal of modern optics. – 2001. – Т. 48. – №. 13. – С. 2023-2038.
11. Kronberg D. A., Molotkov S. N. Duality of quantum communication channels and a collective intercept-resend attack on quantum key distribution with differential phase shift //JETP letters. – 2014. – Т. 100. – №. 4. – С. 279-284.

Банокин П.И.
Томский государственный университет систем управления и радиоэлектроники,
Научно-инжиниринговый центр «Интеллектуальные системы доверенного взаимодействия»,
младший научный сотрудник
pavel805@gmail.com

ИСПОЛЬЗОВАНИЕ ПОВЕДЕНЧЕСКИХ ДАННЫХ ДЛЯ ИДЕНТИФИКАЦИИ ВНУТРЕННИХ УТЕЧЕК ДАННЫХ

Аннотация: Рассмотрены методы поиска посторонних значений в массиве поведенческих данных. Предложен процесс идентификации утечек данных на основе анализа текстовых документов и графа переходов между программными приложениями

Ключевые слова: утечки данных, поведение пользователей.

Цель исследования – разработка алгоритмов анализа закономерностей поведения пользователей корпоративных информационных систем и их программная реализация в виде программного комплекса для контроля действий пользователей. Для достижения цели исследования необходимо решение следующих задач: создание набора поведенческих данных, создание модели профиля поведения пользователя, разработка алгоритмов, сравнение эффективности разработанных алгоритмов. Цель исследования непосредственно связана с диссертационной работой – решением задачи идентификации внутренних утечек данных.

Внутренней утечкой данных является передача конфиденциальных данных неуполномоченным лицу или группе лиц вследствие умышленных действий сотрудника предприятия [1]. Необходимость защиты от внутренних утечек данных обусловлена рисками репутационных потерь, финансовыми убытками, которые могут в том числе включать штрафы от надзорных организаций, и ростом активности преступников в области информационной технологий [2].

Деятельность по предотвращению утечек данных включает разграничение прав доступа, шифрование, использование сетевых экранов и антивирусного программного обеспечения. Однако, эти меры не могут полностью исключить риски внутренних утечек данных, так как сотрудники предприятия обладают авторизованным доступом к информационным ресурсам предприятия, а копирование данных может быть осуществлено без использования электронный почты или портативных носителей данных путем фотографирования экрана и переписывания на бумагу. Один из способов ранней идентификации – анализ профессионального поведения пользователя – основан на предположении, что поведение пользователя меняется в момент совершения утечки данных. Изменения могут быть выражены в виде обращения к ранее не используемым категориям данных или элементам корпоративной информационной системы (в дальнейшем КИС) или нетипичной последовательностью действий при выполнении бизнес-процессов.

Задача идентификации утечек данных в зависимости от доступного набора данных может быть задачей классификации или задачей поиска посторонних элементов в потоке действий пользователя. В случае отсутствия примеров аномальных значений задача сводится к поиску аномальных значений [3] Для многих задач поиска посторонних значений, аномалии не известны заранее или могут возникать спонтанно как новые явления на этапе тестирования программного обеспечения [4]. По результатам поиска посторонних элементов поведение пользователя относится к одному из двух классов: аномального или обычного поведения.

Поведенческие данные соответствуют критериям документно-ориентированной и графовой моделям хранения данных. Категориальные, числовые и текстовые характеристики действия пользователя могут быть сохранены в виде документа, атрибуты которого содержат параметры действия пользователя. Графовая составляющая модели данных представлена последовательностями переключения пользователя между программами или отдельными элементами графического интерфейса.

Впервые модель программного инструмента для предотвращения утечек данных и анализа поведения пользователя на основе лог-записей описана специалистом по информационной безопасности Dorothy Denning [5]. В работе [6] в качестве источника данных также используются записи лог-файлов. Категориальные атрибуты действия и числовые характеристики (дата и время совершения) анализируются с использованием метода главных компонент совместно с ранжированием событий по важности на основе статистическая меры TF-IDF, последовательность возникновения событий не учитывается. В работе отмечается, что при анализе поведения в выходные и

предпраздничные дни могут возникнуть осложнить применение алгоритмов, чувствительных к количеству входных данных. Достоинством упомянутой выше работы является хорошая объясняющая способность предложенного авторами решения и способ визуализации.

Анализ текстовых документов, с которыми работает пользователь, позволяет определить данные, находящиеся под угрозой потери конфиденциальности. Для анализа текстовых данных широко используются тематическое моделирование с использованием латентного семантического индексирование и латентного размещения Дирихле. В работе [7] в качестве источника данных о поведении используются архивы писем корпоративной электронной почты. Отклонения в поведении определяются как изменение тематического распределения текста электронной переписки сотрудника. В работе [8] также анализируется электронная переписка: для каждого пользователя создается индивидуальный классификатор на основе опорных векторов.

Методы теории графов могут быть применены при исследовании последовательностей действий пользователя при переключениях между программами и при переходах между элементами пользовательского интерфейса отдельной программы. Для отслеживания событий переключения между окнами и нажатия на элементы интерфейса могут быть применены средства интерфейса программирования операционной системы, такие как Windows Accessibility API [9]. Обработка графа может включать выделение значимых узлов (программных приложений и их элементов) [10] и прогнозирование действий пользователя [11]. Изменения в списке значимых узлов и повышение ошибок прогнозирования могут свидетельствовать об аномалии поведения.

Приведенный выше анализ существующих исследований подтверждает актуальность задачи разработки алгоритмов анализа закономерностей поведения пользователей, совместно использующих поведенческие данные графовой и документной моделей для учета последовательности работы пользователей с элементами интерфейса КИС и их текстового содержимого. Для получения текстовых данных узлов графа (элементов пользовательского интерфейса клиента КИС) необходима предварительная обработка данных, включающая создания экранного снимка и выделение из него текстового содержимого с помощью средств оптического распознавания символов и определение инструмента (составной части) используемой программы. Для получения текстовых данных могут быть использованы программные средства оптического распознавания символов [12], [13].

Обобщенный процесс идентификации утечек данных (рис. 1) учитывает графовую и документную модели. Процесс идентификации утечек данных включает два основных этапа:

1. Накопления данных и построение на их основе модели поведения. Построение модели включает вычисление и отбор признаков, определяющих поведение пользователя. Получение данных о поведении пользователя происходит с помощью программ-агентов, работающих в фоновом режиме. Для каждого пользователя создается профиль поведения, в котором содержится индивидуальный набор поведенческий признаков. Отбор признаков позволяет снизить размерность и исключить из входных данных элементы, снижающие точность классификации [14].
2. Мониторинг поведения пользователей. После создания профиля запускается мониторинг действий пользователя для проверки текущего поведения на соответствие признакам.

Рис. 1. Обобщенный процесс идентификации утечек данных

Дальнейшая работа по проектированию и реализации алгоритма идентификации утечек данных включает выбор оптимальных способа кодирования текста, структуры профиля поведения и разработку алгоритма поиска посторонних значений в текстовых данных.

СПИСОК ЛИТЕРАТУРЫ

1. Shabtai A., Elovici Y., Rokach L. A survey of data leakage detection and prevention Solutions. - Berlin, Germany: Springer, 2012.
2. Исакова Т., Королев Н. На работу как на фишинг // Газета «Коммерсантъ». - 2022. - 08.08. - Ст. 18.
3. Wressnegger C., Schwenk G., Arp D., Rieck K. A Close Look on n-Grams in Intrusion Detection: Anomaly Detection vs. Classification // AISec '13: Proceedings of the 2013 ACM workshop on Artificial intelligence and security. - Berlin, Germany: ACM, 2013. - С. 67–76.
4. Goldstein M., Uchida S. A Comparative Evaluation of Unsupervised Anomaly Detection Algorithms for Multivariate Data // PLOS ONE. - 2016. - № 11(4).
5. Denning D. E. An Intrusion Detection Model // IEEE transactions on software engineering. - 1987. - №SE-13, 2. - С. 222-232.
6. Hu J., Tang B., Lin D. Anomalous User Activity Detection in Enterprise Multi-Source Logs // International Conference on Data Mining Workshops. - New Orleans, LA, USA: IEEE, 2017.
7. Kim J.; Park M.; Kim H.; Cho S., Kang P. Insider Threat Detection Based on User Behavior Modeling and Anomaly Detection Algorithms. // Applied Sciences. - 2019. - №9(19).
8. BrocardoM.L., Traore I., Woungang I. Authorship verification of e-mail and tweet messages applied for continuous authentication // Journal of Computer and System Sciences. - 2015. - №81. - С. 1429–1440.
9. Event Constants (Winuser.h) // Microsoft Docs URL: https://docs.microsoft.com/en-us/windows/win32/winauto/event-constants (дата обращения: 13.08.2022).
10. Ефремов А.А., Лунева Е.Е., Банокин П.И., Кочегурова Е.А. Использование процедуры ранжирования Кендалла–Уэя для идентификации ключевых игроков социального графа // Доклады ТУСУР. - 2018. - №1. - С. 80-85.
11. Liu Y., Shi X., Pierce L., Ren X. Characterizing and Forecasting User Engagement with In-App Action Graph: A Case Study of Snapchat // KDD '19: Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. - New York, USA: ACM, 2019. - С. 2023–2031.
12. NormCap // GitHub URL: https://github.com/dynobo/normcap (дата обращения: 15.08.2022).
13. TextSnatcher // GitHub URL: https://github.com/RajSolai/TextSnatcher (дата обращения: 15.08.2022).
14. Alkurd R., Abualhaol I. A Synthetic User Behavior Dataset Design for Data-Driven AI-Based Personalized Wireless Networks // IEEE International Conference on Communications Workshops (ICC Workshops). - Shanghai, China: IEEE, 2019.

Барков В.В.
МТУСИ, старший преподаватель,
v.v.barkov@mtuci.ru

КЛАССИФИКАЦИЯ ТРАФИКА НЕЖЕЛАТЕЛЬНЫХ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ МЕТОДОМ МАШИННОГО ОБУЧЕНИЯ В ПОТОКОВОМ РЕЖИМЕ

Аннотация: Исследование направлено на повышение функциональной эффективности методов машинного обучения при автоматической классификации в потоковом режиме сетевого мобильного трафика и выявление нежелательных приложений. Научная новизна состоит в разработке и исследовании улучшенных алгоритмов классификации трафика мобильных приложений методами машинного обучения. Результатом проекта станет программный комплекс для автоматической классификации трафика мобильных устройств, сформированная экспериментальная база данных сетевого трафика выбранных мобильных приложений, новый алгоритм обнаружения смены концепта.

Ключевые слова: мобильный сетевой трафик, классификация, мобильные приложения, нежелательные мобильные приложения, потоковый режим классификации, машинное обучение, обнаружение смены концепта.

Введение

Целью работы является повышение функциональной эффективности методов машинного обучения при автоматической классификации в потоковом режиме сетевого мобильного трафика и выявлении нежелательных приложений.

Научная задача – разработка и исследование улучшенных алгоритмов классификации трафика мобильных приложений методами машинного обучения.

В настоящее время в геометрической прогрессии возрастает поток сетевого трафика, генерируемый в том числе мобильными устройствами. В связи с этим задача выявления нежелательных и вредоносных приложений в этом потоке приобретает особую актуальность.

Для сотовых операторов информация об использовании тех или иных приложений пользователями сети необходима для составления статистики по наиболее часто используемым приложениям. Для работодателей такая информация может быть использована для выявления нежелательных приложений с целью запрета использования определённых приложений (например, социальных сетей) в рабочее время. Для обычного пользователя мобильного устройства – для запрета доступа определённых приложений, способных контролировать передаваемые персональные данные.

В настоящее время для решения подобных задач получили распространение методы, основанные на технологиях машинного обучения (Machine Learning, ML) и интеллектуального анализа данных (Data Mining, DM). С их помощью даже неизвестные нежелательные или вредоносные приложения могут быть выявлены с определенной степенью точности. Эти технологии, как показывает анализ, обеспечивают более эффективные классификацию, анализ и фильтрацию сетевого трафика в сравнении с такими методами, как Deep Packet Inspection (DPI) или анализ номеров портов.

Теоретическую базу исследования в области методов ML и DM составили работы таких ученых, как Айвазян С.А., Айзерман М.А., Барсегян А.А., Загоруйко Н.Г., Вапник В.Н., Воронцов К.В., Mitchell T. 1[1], Hastie T., Tibshirani R., Friedman J.T., Xu K., Zhang Z. [2], Bhattacharyya S., Heckerman J.D. и др. Эти исследования были выполнены преимущественно в области экономики и оказалось, что некоторые их результаты можно встроить в предмет сетевых и телекоммуникационных исследований.

Отдельные вопросы исследования трафика посредством метода ML рассматривались в трудах Большева А.К., Гетьмана А.И., Зубкова Е.В., Котенко И.В., Козьмовского Д.В., Михайлова А.Ю., Маркина Ю.В., Назарова А.О., Петровского М.И., Санарова А.С., Шелухина О.И., Щербаковой Н.Г., M. Pietrzyk, Z. Chen, B. Yang, J. Erman, K. Balachandran, J.H. Broberg, T. Bujlow, V. Carela-Español, C.C. Aggarwal, Y. Wang [3], G.S.o Han, M. Arlitt, A. Mahanti и др [4-8]. Однако задаче автоматической классификации трафика мобильных приложений уделено недостаточно внимания.

Решение этой научной задачи невозможно без формирования экспериментальной базы данных (БД) для выбранных мобильных приложений – сетевого трафика, предназначенного для обучения и тестирования алгоритмов машинного обучения. БД может использоваться в системах обнаружения вторжений, для фильтрации вредоносных и нежелательных приложений, блокировки заданных приложений, передающих в том числе зашифрованный трафик.

Вышесказанное обусловливает актуальность настоящего исследования, направленного на повышение эффективности классификации трафика мобильных приложений методами машинного обучения и интеллектуального анализа данных в режиме реального времени.

Для решения поставленных задач использовались методы теории вероятности, математической статистики, машинного обучения и интеллектуального анализа (обработки) данных, имитационное моделирование.

Научная новизна исследования заключается в следующем:

1. Классификация зашифрованного трафика мобильных Android приложений без расшифрования трафика.
2. Поиск ограничений для структуры анализируемых данных как по количеству потоков, так и по количеству пакетов в потоке.
3. Разработке нового алгоритма обнаружения смены концепта и классификации мобильных приложений в потоковом режиме с обработкой в скользящем окне в режиме накопления с «конечной памятью» как с равномерной, так и неравномерной интенсивностью поступления данных, учитывающий «старение» данных в окне обработки.

Формирование экспериментальной базы данных сетевого трафика мобильных приложений

Для автоматизации процесса исследования алгоритмов классификации трафика мобильных приложений был разработан программный комплекс [9-14].

Взаимодействие приложений с базой данных показано на рис. 1.

Рис. 1. Взаимодействие приложений с базой данных

В состав программного комплекса входит база данных, Web-приложение и мобильный клиент. Для развертывания базы данных была выбрана СУБД MySQL. Web-приложение разработано с использованием технологии Java Enterprise Edition. Мобильное приложение с функцией сбора трафика была разработано для смартфонов и планшетов под управлением ОС Android.

Для формирования базы данных трафика мобильных устройств было выбрано 18 мобильных приложений. Приложения можно разделить на три группы: шифрующие, не шифрующие и частично шифрующие трафик.

С использованием разработанного программного комплекса в течение одного месяца был собран трафик 110 мобильных приложений, включающий 95 447 потоков и 7 119 169 пакетов. 71 667 потоков и 6 989 991 пакетов составляют 18 основных приложений – по 6 приложений для каждой группы. Количество потоков для каждого из 18 приложений составляет примерно 5 000 потоков.

Выбор атрибутов

В качестве атрибутов классификации были выбраны атрибуты, указанные в таблице 1.

Табл. 1. Описание признакового описания

ID	Название
1	Общий объем полезной нагрузки на сетевом уровне от клиента.
2	Общий объем полезной нагрузки на сетевом уровне от сервера.
3	Общий объем полезной нагрузки на транспортном уровне от клиента.
4	Общий объем полезной нагрузки на транспортном уровне от сервера.
5	Средний размер пакета со стороны клиента.
6	Средний размер пакета со стороны сервера.
7	Средний размер порции данных со стороны клиента.

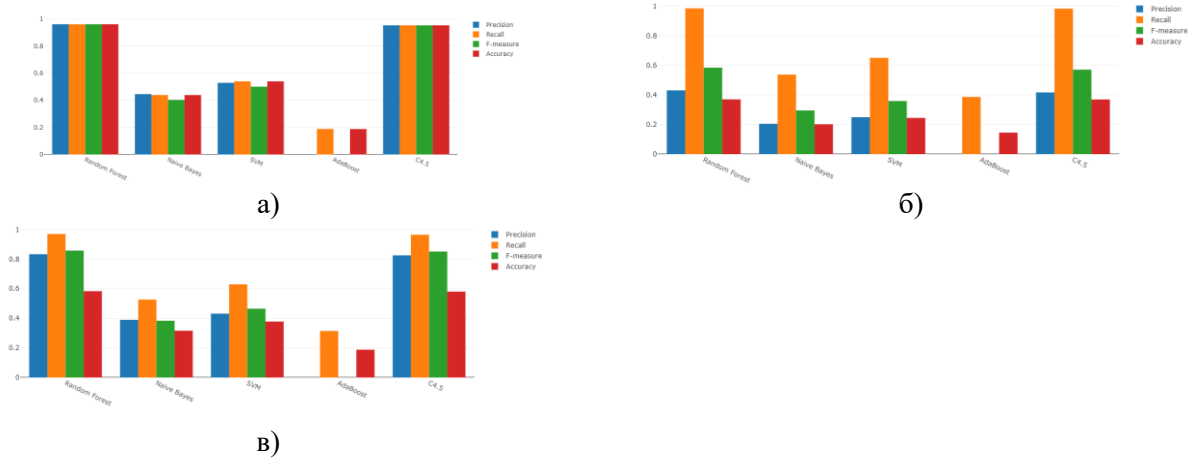
ID	Название
8	Средний размер порции данных со стороны сервера.
9	Стандартное отклонение размера пакета со стороны клиента
10	Стандартное отклонение размера пакета со стороны сервера
11	Стандартное отклонение размера порции данных со стороны клиента
12	Стандартное отклонение размера данных со стороны сервера
13	Среднее число пакетов на порцию данных со стороны клиента
14	Среднее число пакетов на порцию данных со стороны сервера
15	КПД клиента
16	КПД сервера
17	Соотношение байт
18	Соотношение полезной нагрузки
19	Соотношение пакетов
20	Общее количество переданных сегментов транспортного уровня со стороны клиента
21	Общее количество переданных сегментов транспортного уровня со стороны сервера
22	IP-адрес источника
23	IP-адрес назначения

В ходе исследования влияния алгоритма выбора признаков на качество классификации сетевого трафика были проведены исследования алгоритмов отбора признаков CFS, PCA, Wrapper, InfoGain [15]. Оценка проводилась с использованием алгоритмов классификации: Naive Bayes; C4.5; Random forest; SVM на шифрованном [16-17] и нешифрованном [12] наборе данных. В результате алгоритм CFS отобрал атрибуты 22 и 23, алгоритм PCA – атрибуты 1-12, алгоритм Wrapper – 10, 14, 15, 19, 22, 23, алгоритм InfoGain с порогом 0,8 – атрибуты 1-12, 15-18, 22, 23, с порогом 1 – атрибуты 2-4, 6, 8-12, 16, 18, 22, 23.

Влияние фонового трафика на качество классификации

Для выявления факта влияния фонового трафика на процесс классификации мобильного трафика, были проведены эксперименты [18-19] по классификации мобильного трафика по приложениям без и при наличии фонового трафика при наличии и отсутствии класса «Неизвестное приложение», а также исследовано влияние фонового трафика на классификацию различных приложений.

Для классификации использовались классификаторы Random Forest; Naive Bayes; SVM; AdaBoost; C4.5. В качестве набора данных были выбраны 12 приложений без фонового трафика, включающего 19900 потоков и 12 приложений с фоновым трафиком, включающего 48500 потоков. В ходе экспериментов были получены результаты, представленные на рисунке 2.



а) б)

в)

Рис. 2. Гистограмма средних значений метрик алгоритмов классификации: а) при отсутствии фонового трафика; б) при наличии фонового трафика; в) при наличии фонового трафика и наличии класса «Неизвестное приложение»

В ходе исследования влияния фонового трафика на качество классификации выявлено, что лучшими из рассмотренных алгоритмов классификации являются Random Forest и C4.5, как для классификации без фонового трафика, так и в наборах с фоновым трафиком. Дальнейшие исследования показали, что алгоритм C4.5 качественнее и быстрее работает на данных наборах мобильного трафика чем Random Forest.

Класс «Неизвестное приложение» значительно увеличивает качество классификации с фоновым трафиком по сравнению с качеством классификации с фоновым трафиком, но без класса «Неизвестное приложение». Однако он добавляет ложно положительные распределения по классам, что в свою очередь негативно сказывается на качестве классификации. Однако в целом наличие класса «Неизвестное приложение» однозначно положительно сказывается на качество классификации при наличии фонового трафика.

Наиболее подверженными влиянию фонового трафика являются Интернет-браузер; Социальные сети; Мессенджеры. Наиболее влияющими являются Интернет-браузер; Новостные ленты; Социальные сети.

Будущая работа.

Для расширения перечня доступных алгоритмов машинного обучения, в частности для возможности использовать алгоритмы машинного обучения, реализованных не на языке программирования Java, а также для проведения экспериментов с потоковыми данными, в том числе для исследования алгоритмов обнаружения смены концепта, планируется доработка существующего программного обеспечения, внедрение его в учебный процесс и получение свидетельства о государственной регистрации программы для ЭВМ на доработанную систему.

С использованием доработанного программного обеспечения провести актуализацию исследования алгоритмов классификации в потоковом режиме [20-21], а также исследование алгоритмов обнаружения смены концепта [22].

СПИСОК ЛИТЕРАТУРЫ

1. Mitchell, T. M. Machine learning[Текст]. 1997 /T. M. Mitchell et al; Burr Ridge, IL: McGraw Hill. – 1997. – Т. 45. – №. 37. – С. 870-877.
2. Chi, M. Nonlinear Online Classification Algorithm with Probability Margin[Текст]/M. Chi, H. He, W. Zhang; Asian Conference on Machine Learning. – 2011. – С. 33-46.
3. Wang H. Concept drift detection for streaming data [Текст]/H.Wang, Z. Abraham; Neural Networks (IJCNN), 2015 International Joint Conference on. – IEEE, 2015. – С. 1-9.
4. Risso, F. Lightweight, Session-Based Traffic Classification [Текст]/ F. Risso, A. Baldini, M. Baldi, P. Monclus, O. Morandi; - [б.и.]. - [б.м.]
5. Gomes, H. Adaptive random forests for evolving data stream classification [Текст]/H. M. Gomes et al; Machine Learning. – 2017. – Т. 106. – №. 9-10. – С. 1469-1495.
6. Breiman, L. Random forests [Текст]/L. Breiman; Machine learning. Kluwer Academic Publishers. Manufactured in The Netherlands. – 2001. – Т. 45. – №. 1. – С. 5-32.
7. Гудфеллоу, Я. Глубокое обучение [Текст]/Я.Гудфеллоу, Б. Иошуа, А. Курвилль; М: ДМК-Пресс, 2017, 652с.
8. Oza Nikunj, C. Online bagging and boosting. Jaakkola Tommi and Richardson Thomas, editors [Текст]/C. Oza Nikunj, J. Russell Stuart; Eighth International Workshop on Artificial Intelligence and Statistics. – 2001. – С. 105-112.
9. Шелухин, О.И. Создание базы данных сетевого трафика для автоматизации классификации мобильных приложений под управлением операционной системы Android / О.И. Шелухин, С.Д. Ерохин, В.В. Барков // Нейрокомпьютеры: разработка, применение. 2019. №1. С.40-51.
10. Шелухин, О.И., Ерохин, С.Д., Барков В.В. Программный комплекс для онлайн классификации сетевого трафика // Свидетельство о государственной регистрации программы для ЭВМ № 2019615330 от 24 апреля 2019 г.
11. Шелухин, О.И. Разработка инфраструктуры для классификации сетевого трафика мобильных приложений с применением алгоритмов машинного обучения / О.И. Шелухин, В.В. Барков // Телекоммуникационные и вычислительные системы - 2017. Тр. межд. научно-тех. конф. – 2017. – С.180-181.
12. Шелухин, О.И. Экспериментальные исследования и создание базы данных сетевого трафика мобильных устройств под управлением операционной системы Android / О.И. Шелухин, В.В. Барков // Фундаментальные проблемы радиоэлектронного приборостроения: «INTERMATIC-2018». – М.: МИРЭА. 2018. Т. 18. №4. С.1011-1017.
13. Шелухин, О.И. Методы сбора сетевого трафика с мобильных устройств под управлением операционной системы Android с целью классификации по типам приложений / О.И. Шелухин, В.В. Барков //. Сб. тр. XII Межд. отраслевой науч.-тех. конф Технологии информационного общества (14-15 марта 2018 г., Москва). М.: МТУСИ. Т.2. С.20-21.

14. Барков, В.В. Проектирование и разработка экспертно-аналитической системы "Система анализа трафика" для исследования алгоритмов классификации трафика мобильных устройств под управлением операционной системы Android // Безопасные информационные технологии: Сб. тр. 9-й всерос. науч.-тех. конф. – М.: МГТУ им. Н.Э. Баумана, 4-5 декабря 2018 г., С. 2-12.
15. Шелухин О.И., Барков В.В., Полковников М.В. Сравнительный анализ алгоритмов оценки количества и структуры атрибутов в задачах классификации мобильных приложений // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 2. С. 90–100.
16. Шелухин, О.И. Классификация зашифрованного трафика мобильных приложений методом машинного обучения / О.И. Шелухин, В.В. Барков, М.В. Полковников // Вопросы кибербезопасности. 2018. №4(28). С.21-28.
17. Барков, В.В. Исследование алгоритмов классификации зашифрованного трафика мобильных устройств по типам приложений методами машинного обучения / В.В. Барков, М.В. Полковников // Тр. Межд. научно-тех. конф. «Телекоммуникационные и вычислительные системы 2018». – М.: Горячая линия – Телеком, 2018. – С.310-312.
18. Sheluhin, O.I. Experimental Studies of Network Traffic of Mobile Devices with Android OS / O.I. Sheluhin, S.D. Erokhin, A.V. Osin, V.V. Barkov // Systems of Signals Generating and Processing in the Field of on Board Communications. – 2019
19. Sheluhin, O.I. Influence of Background Traffic on the Effectiveness of Mobile Applications Traffic Classification Using Data Mining Techniques / O.I. Sheluhin, V.V. Barkov // T-Comm. 2018. vol.12, no.10. pp.52-57.
20. Sheluhin O.I. The Online Classification of the Mobile Applications Traffic Using Data Mining Techniques. / O.I. Sheluhin, V.V. Barkov, S.A. Sekretarev // T-Comm. 2019. vol. 13. no.10. pp.60-67.
21. Барков, В.В. Классификация трафика мобильных устройств по типам приложений методами машинного обучений в режиме онлайн / В.В. Барков, С.А. Секретарёв // Межд. форум информатизации (МФИ-2018) 6 Тр. конф. «Телекоммуникационные и вычислительные системы 2018». – М.: Горячая линия – Телеком, 2018. – С.319-321.
22. Шелухин, О.И., Барков, В.В., Секретарев, С.А. Алгоритмы обнаружения дрейфа концепта при потоковой классификации трафика мобильных приложений // REDS: Телекоммуникационные устройства и системы 2020. №3. С.19-27.

Белова Е. П.
БашГУ, ассистент кафедры управления
информационной безопасностью
yelenabelova92@gmail.com

НАЧАЛЬНЫЕ ПОЛОЖЕНИЯ СИСТЕМЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ПО ПАРАМЕТРАМ РЕЧИ И ВИДЕОИЗОБРАЖЕНИЮ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Аннотация: статья содержит основные положения диссертационного исследования. В ней представлены цели и задачи исследования, анализируются источники, предлагаются методы повышения эффективности процедуры аутентификации. Основная роль отводится комбинации различных биометрических методов без привлечения дополнительного оборудования. Для пользователей с административными привилегиями предлагаются несколько ступеней аутентификации. Представлены решения, позволяющие проверить подлинность биометрических данных.

Ключевые слова: биометрическая аутентификация, голос, речь, видеоизображение, геометрия лица, жесты рук, формантные характеристики, фонема, результаты вейвлет-преобразования, искусственная нейронная сеть.

На сегодняшний день системы аутентификации являются базовыми компонентами информационных систем. Согласно [1] каждое предприятие должно быть информатизированно, то есть все основные бизнес-процессы должны осуществляться через информационные системы учреждений, вся основная документация должна быть переведена в цифровой формат, что, в свою, очередь, подразумевает верификацию личности каждого сотрудника при осуществлении им своих профессиональных обязанностей в информационной системе предприятия.

С ростом применения искусственных нейронных сетей развиваются и биометрические методы аутентификации. Нейросетевые технологии, копирующие мыслительные процессы человека, позволяют распознать объект по тем же признакам, что и органы чувств человека, но сделать это с большей эффективностью, так как их функционирование полностью основывается на математических соотношениях.

Диссертационная работа «Система биометрической аутентификации по параметрам речи и видеоизображению на основе нейросетевых технологий» ведётся в рамках конкурса «Гранты ИБ МТУСИ» и направлена на поддержание информационной безопасности предприятия при решении задач цифровой экономики.

Целью комплекса диссертационных исследований является повышение эффективности аутентификации пользователей с административными привилегиями в локальной сети предприятия при помощи системы биометрической аутентификации по параметрам речи и видеоизображению на основе нейросетевых технологий.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Провести глубокий анализ литературных источников, ГОСТов и нормативных документов.
2. Разработать уникальный биометрический образ личности пользователя для системы аутентификации по голосу.
3. Разработать уникальный биометрический образ личности пользователя для системы аутентификации по видеоизображению лица.
4. Разработать архитектуру системы аутентификации пользователя по голосу на базе комплекса искусственных нейронных сетей.
5. Разработать архитектуру системы аутентификации пользователя по видеоизображению лица на базе комплекса искусственных нейронных сетей.
6. Разработать систему распознавания жестов по их видеоизображению.
7. Разработать программный комплекс системы биометрической аутентификации по параметрам речи и видеоизображению на основе нейросетевых технологий.

Биометрическая система аутентификации состоит из трёх модулей. Два из которых используют речевые параметры: формантные характеристики гласных звуков и результаты вейвлет-преобразования. Третий модуль предназначен для распознавания геометрии лица по видеоизображению.

Отдельно стоит отметить многоуровневую систему защиты биометрических данных от фальсификаций:

1. В ходе работы модуля аутентификации по формантным характеристикам гласных звуков, специальный генератор случайным образом предлагает пользователю произнести некую последовательность гласных звуков. Полученные результаты используются как для верификации личности пользователя, так и для доказательства того, что процедура проходит в режиме реального времени.
2. Аналогично работе модуля аутентификации по формантным характеристикам, модуль распознавания по результатам вейвлет-преобразования также включает встроенную защиту от фальсификаций. Для этого генерируются числа в определённом порядке и проверяется совпадает ли произносимое пользователем с заданием.
3. В модуле аутентификации по видеоизображению лица для проверки подлинности предъявления биометрических данных аутентифицируемым, ему предлагается показать случайные жесты.

Так как в информационной системе пользователи обладают разными правами доступа, наибольшее внимание стоит уделять аутентификации пользователей с административными привилегиями. Как правило, количество сотрудников данной категории в локальной сети предприятия не превышает 10 человек.

Говоря о локальной сети предприятия, в которой осуществляются основные бизнес-процессы, стоит отметить, что система биометрической аутентификации должна защищать не только локальную сеть, но и те части информационной инфраструктуры предприятия, которые находятся непосредственно в Интернете, от несанкционированного доступа.

В настоящее время данная система аутентификации не имеет аналогов. Но, в некоторой степени похожими на неё, можно считать [2, 3].

Большой вклад в исследование систем аутентификации по голосу и возможности выделения параметров речи внесли В. Н. Сорокин, Ю. Н. Матвеев, С. Л. Марпл, Л. Р. Рабинер и Р. В. Шафер [4-7].

Наиболее известными системами аутентификации по голосу являются [8-10].

Работ, посвящённых комбинированному использованию формантных характеристик и результатов вейвлет-преобразования не выделено.

В области распознавания по лицу следует отметить исследования [11-15].

В ходе диссертационного исследования используются следующие методы:

1. Для выделения формантных характеристик применяется быстрое преобразование Фурье.
2. Для подтверждения подлинности личности пользователя используются формантные характеристики гласных звуков. Исследование, посвящённое применению согласных звуков, ведётся. Также осуществляется исследование эмоционального состояния человека (используются базовые эмоции: «зло», «счастье», «грусть») и стиля произношения («громкий», «нормальный», «тихий», при этом «нормальный» является тем стилем, в котором произносятся звуки в остальных экспериментах).
3. Ведутся работы по выбору способа вейвлет-преобразования.
4. Для распознавания геометрии лица по видеоизображению также выбираются методы за счёт проведения экспериментов и анализа их результатов. Анализируется опыт отечественных и иностранных исследователей.
5. Выбор архитектуры нейронных сетей также осуществляется непосредственно в экспериментах.

Новизна биометрического образа пользователя информационной системы заключается в комплексировании характеристик формант и частот лидирующих формант произнесённых пользователем гласных звуков, полученных значений вейвлет-преобразований гласных звуков, вейвлет-преобразований заданного текста и наиболее информативных параметров геометрии лица, что позволяет обеспечить уникальность образа для системы биометрической аутентификации.

Новизна метода биометрической аутентификации, основанного на использовании предложенного уникального биометрического образа, заключается в разработке нейросетевого комплекса.

Новизна системы биометрической аутентификации, построение которой основывается на предложенном методе, заключается в разработанной архитектуре системы.

Тем самым система биометрической аутентификации по параметрам речи и видеоизображению на основе нейросетевых технологий позволит сберечь и финансовые средства от киберзлоумышленников при становлении цифровой экономики в России.

Ожидаемые результаты представлены современным многоуровневым инструментом на базе искусственных нейронных сетей, способным свести максимальные показатели ошибки 1-го рода и

ошибки 2-го рода к 1%. Простота в использовании и отсутствие необходимости сохранять в уме какие-либо сложные данные (например, комбинации паролей из 20 различных символов), не только упразднят процесс аутентификации для пользователей и снизят их нервно-психическую напряжённость, но и существенно уменьшат возможность попадания аутентификационных данных к третьим лицам.

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы».
2. Единая биометрическая система от Ростелеком. — Режим доступа: https://habr.com/ru/company/rostelecom/blog/424751/.
3. Система учёта идентификации и аутентификации личности по голосу и лицу в Эквадоре. — Режим доступа: https://rg.ru/2020/03/24/reg-szfo/rossijskaia-sistema-identifikacii-po-golosu-ne-ostavit-shansov-prestupnikam.html.
4. Сорокин В. Н. Распознавание личности по голосу: аналитический обзор [Текст] / В. Н. Сорокин, В. В. Вьюгин, А. А. Тананыкин // Информационные процессы. – 2012. – Т. 12, №1. – С. 1-30.
5. Матвеев, Ю. Н. Исследование информативности признаков речи для систем автоматической идентификации дикторов [Текст] / Ю. Н. Матвеев // Известия вузов. Приборостроение. – 2013. – Т. 56, №2. – С. 47-51.
6. Марпл С. Л. Цифровой спектральный анализ и его приложения. / С. Л. Марпл. – М.: Мир, 1990.
7. Рабинер Л. Р. Цифровая обработка речевых сигналов. /Л. Р. Рабинер, Р. В. Шафер – М.: Радио и связь, 1981. – 496 с.
8. Аппаратно-программный комплекс криминалистического исследования фонограмм речи «ИКАР Лаб», разработанный компанией «Центр речевых технологий» [Электронный ресурс]. – Режим доступа: http://www.speechpro.ru/upload/productspecificationdocument/file/ikar_lab_broshyura.pdf.
9. Программное обеспечение «GritTec Speaker-ID» от компании ООО «ГритТек» [Электронный ресурс]. – Режим доступа: http://www.grittec.ru/pdf/Manual_GritTec's%20Speaker-ID_The%20mobile%20Client_RU.pdf.
10. Платформа мультимодальной биометрической аутентификации пользователей в каналах дистанционного обслуживания «VoiceKey» от компании «Центр речевых технологий» [Электронный ресурс]. – Режим доступа: http://www.speetech.by/technologies/voice-key#fragment-1.
11. Smith R. S. Facial Expression Detection using Filtered Local Binary Pattern Features with ECOC Classifiers and Platt. / Raymond S. Smith, Terry Windeatt – 2010 [Электронный ресурс]. – Режим доступа: http://proceedings.mlr.press/v11/smith10a/smith10a.pdf.
12. Trigeorgis G. A Deep Semi-NMF Model for Learning Hidden Representations. / George Trigeorgis, Konstantinos Bousmalis, Stefanos Zafeiriou, Bjorn W. Schuller [Электронный ресурс]. – Режим доступа: http://proceedings.mlr.press/v32/trigeorgis14.pdf.
13. Wang H. Robust and Discriminative Self-Taught Learning. / Hua Wang, Feiping, Heng Huang [Электронный ресурс]. – Режим доступа: http://proceedings.mlr.press/v28/wang13g.pdf.
14. Masood M. A. A Particle-Based Variational Approach to Bayesian Non-negative Matrix Factorization. / Muhammad A Masood, Finale Doshi-Velez – 2019 [Электронный ресурс]. – Режим доступа: https://www.jmlr.org/papers/volume20/18-153/18-153.pdf.
15. Larsen A. B. L. Autoencoding beyond pixels using a learned similarity metric. / Anders Boesen Lindbo Larsen, Søren Kaae Sønderby, Hugo Larochell, Ole Winther.[Электронный ресурс]. – Режим доступа: http://proceedings.mlr.press/v48/larsen16.pdf.

Бирих Э.В.
СПбГУТ, старший преподаватель кафедры ЗСС
be1982@mail.ru

Информационная безопасность данных, передаваемых через открытые телекоммуникационные каналы связи

Аннотация: На сегодняшний день существуют правила и требования по обеспечению безопасности, но они с учетом развития информационных технологий и новых угроз национальной безопасности (в том числе военные угрозы, угрозы утраты национальной и культурной идентичности российских граждан) полноценно не охватывают информационную безопасность данных, передаваемых по открытым телекоммуникационным каналам связи.

Ключевые слова: информационная безопасность (ИБ), угрозы ИБ, модель нарушителя ИБ, критически важные объекты (КВО), модель угроз ИБ, телекоммуникационная безопасность, кибернетическая разведка (КР).

Цель работы. Систематизация информации об анализе и оценке рисков, их важности для построения системы защиты; изучение рекомендаций в области риск-менеджмента и проектирования защищенных информационно-вычислительных сетей (далее ИВС) с учетом прогнозирующих моделей; анализ и сравнение широко используемых методик оценки и анализа рисков ИБ в контексте построения системы управления ИБ организации.

Задача – разработать методику оценки безопасности масштабируемой ИВС организации для принятия решения о необходимости категорирования на основе Банка данных угроз безопасности информации, разработанного Федеральной службой по техническому и экспортному контролю (ФСТЭК России).

Предмет исследования. Обеспечение информационной безопасности данных, передаваемых в масштабируемой ИВС организации, развернутой на открытых телекоммуникационных каналах связи (далее - ОТКС).

Значительный вклад в решение вопросов, связанных с созданием теоретического и практического задела обеспечения информационной безопасности данных, передаваемых по ОТКС, внесли работы отечественных ученых И.В. Котенко, В.И. Коржика, Н.А. Соколова, В.Г. Шведа, В.А. Яковлева, В.А. Липатникова, А.В. Красова. Работы Б.С. Гольдштейна, Д.В. Сахарова подняли тему возникновения угроз ИБ в процессе использования общего канала сигнализации (далее – ОКС) [1, 2]. Однако научных исследований в данном направлении проводится недостаточно. Вопросы обеспечения информационной безопасности данных, передаваемых в масштабируемой ИВС организации, в процессе использования ОКС ОТКС требуют дальнейшего разрешения. Появилась потребность в поиске способов повышения скрытности работы интегрированных ИВС организации, обеспечения безопасности информации с учетом развития методов и средств КР. Актуальность данной работы значительной возрастает с учетом проведения в настоящее время специальной военной операции, использования иностранными государствами против РФ методов ведения информационной войны, в том числе на ОТКС.

Переходя к предмету исследования можно сказать, что ОКС осуществляет обмен сигнальными сообщениями систем разнообразных применений, включая телефонию, передачу данных, услуги ISDN, услуги для абонентов сетей мобильной связи, а также функции эксплуатационного управления сетью ОКС.

Общеканальная сигнализация – это метод сигнализации, в котором один канал путем адресации сообщений, в специально построенной выделенной сети в Единой сети электросвязи Российской Федерации (далее – ЕСЭ), передает сигнальную информацию, относящуюся к множеству каналов или другую информацию для управления ЕСЭ. ОКС может рассматриваться как форма передачи данных, которая специализирована для различных типов сигнализации и передачи информации между распределенными в пространстве процессорами, управляющими различными ресурсами ЕСЭ.

Общеканальная сигнализация полностью удаляет сигнализацию из разговорного тракта, используя отдельный общий канал сигнализации для передачи всех сигналов нескольких трактов.

Отличительной чертой протокола ОКС является высокая надежность передачи информации с минимальной задержкой, без потерь и без дублирования сигнальных сообщений.

В ОКС присутствуют данные об информационных каналах и об абонентах ЕСЭ. Сведения о характеристиках и параметрах канала ОКС (сигнальных сообщениях – типах, структурах и длинах

сообщений), чувствительная информация, связанная с информацией загрузки и биллинга, со структурой сети, управлением ее оборудованием или с данными пользователей могут использоваться для деструктивных воздействий на ОКС ЕСЭ и на информационные каналы и абонентов.

Система ОКС предназначена для управления информационными каналами и подключения (соединения и разъединения) абонентов путем обмена служебными сообщениями, а информационные потоки – только для обмена информационными сообщениями. Информационные каналы являются объектом управления от ОКС.

Сеть ОКС не является закрытой сетью. Доступ к ней имеют пользователи других сетей, построенных на разных технологиях, например, традиционная телефония, интеллектуальные сети, сети сотовой связи, сети VoIP, ATM, ISDN, сети телекоммуникаций NGN и сети мобильной связи. Рост числа точек доступа между сетью ОКС и другими сетями увеличивает потенциальные угрозы безопасности и подверженность сетей ОКС внешним атакам. Например, конвергенция телефонных сетей общего пользования и сети Интернет позволяет применять разные технологии взлома с учетом уязвимостей ОКС. Злоумышленник может модифицировать или перехватывать данные, а также вносить глобальные изменения в подсистему управления сигнализацией. Уязвимости в ОКС позволяют нарушать установление соединения, блокировать с большой степенью вероятности процесс передачи информации и управления сетью [2].

Атака на ОКС ОТКС и входящие в нее объекты может повлечь за собой непоправимые последствия – по нарушению целостности, доступности данных защищаемой ИВС как коммерческих, так и государственных организаций. Многие субъекты из категорий критической информационной инфраструктуры могут коммерческими. К примеру, атака на субъекты коммерческого здравоохранения или коммерческого транспорта может повлечь за собой человеческие жертвы.

Таким образом, причинами основных уязвимостей сетей ОКС является большое количество и сложность интерфейсов, использование новых сервисов, подключение к сети Интернет.

Вышеуказанным определяется актуальность исследования.

Изучение потенциальных угроз ИБ и их классификация необходимы для научно-обоснованного выбора мероприятий, методов, механизмов и средств обеспечения ИБ, а также для выявления наиболее опасных угроз, противодействовать которым должна система обеспечения ИБ сети ОКС.

В задачу обеспечения ИБ сетей ОКС входит защита их функционирования от угроз безопасности и защита программно-аппаратного обеспечения сетей ОКС, так как основным источником отказов сети являются ошибки в программном обеспечении реализации ОКС. Необходимо с высокой достоверностью определять факты удаленных атак. Признаками наличия атак являются несанкционированные цифровые последовательности, путем выявления которых реализуется обнаружение преднамеренных деструктивных воздействий.

Методы исследования базируются на положениях теории вероятности, математического моделирования, теории системного анализа и методологии теории рисков.

В работе будут разрабатываться риск-модели для экстремальных значений критических переменных состояния. В сравнении с порогами их допустимости оцениваются ожидаемые ущербы и вероятности их возникновения [3].

Современные методологии риск - анализа систем сейчас во многом ориентированы на анализ ущербов. В этой связи будет сделана попытка осуществить оценку переменных состояния. Динамика критических переменных и ее прогнозирование обязательны для мониторинга систем, функционирующих в реальном времени, в том числе объектов критической инфраструктуры.

Следующим шагом описывается линейная модель, а затем находится ущерб в нормированном виде и рассчитывается риски, определяется дискретизация значений КПС, повышается ее точность. Приводятся альтернативные варианты подхода к дискретизации на основе математического ожидания. Рассматриваются параметры и характеристики риска одной из переменных состояния. После этого рассчитывается оценка риска для множества переменных состояния, затем проводится Аналитическая оценка функций чувствительности критичных переменных состояния. Все методы подкрепляются формулами и графиками.

Заключительным этапом является управление рисками атакуемой информационно-технологической инфраструктуры критически важных объектов, т.е. рассматриваются аспекты управления рисками превышения критичных переменных состояния пороговых значений кризисного диапазона для информационно-технологической инфраструктуры критически важного объекта.

Научная новизна результатов

1. Будет предложен метод защиты канала связи масштабируемой ИВС организации, развернутой на ОТКС, который в отличие от известных минимизирует риски вскрытия защищаемой сети методами КР;

2. Будет разработана методика защиты канала связи масштабируемой ИВС организации, которая в отличие от известных учитывает: - модели элементарных информационных потоков, учитывающая всевозможные каналы взаимодействия;

- модель угроз конфиденциальности информации, с учетом всех типовых угроз элементам системы и каналам передачи информации;

- модель угроз целостности и доступности информации, с учетом угроз доступности как подмножество угроз целостности информации, направленных на канал передачи информации.

3. Будут разработаны научно-технические предложения по реализации метода защиты канала связи масштабируемой ИВС организации, развернутой на ОТКС.

По результатам исследования будет предложена Методика оценки угроз безопасности информации, которая предполагает анализ возможных угроз безопасности информации, с учетом уточняющих методических документов, таких как Типовые модели угроз безопасности информации или Базовые модели угроз безопасности типового объекта КИИ, учитывающая минимизацию рисков в области информационной безопасности.

В дальнейшем результаты исследования можно будет применять в преподавании дисциплин по программам подготовки инженеров и преподавателей исследователей по специальностям 10.03.01 «Информационная безопасность» и 10.06.01 «Информационная безопасность», а также учитывать при внедрении в цифровую экономику.

В настоящее время основные результаты работы опубликованы в 11 печатных трудах, рецензируемых журналах ВАК, РИНЦ и Scopus [4-16].

СПИСОК ЛИТЕРАТУРЫ

1. *Гойхман В.Ю., Гольдштейн Б.С., Сибирякова Н.Г.* Протоколы стека ОКС7: подсистема MAP. Серия «Телекоммуникационные протоколы». Книга 10. – СПб.: БХВ-Петербург, 2014. – 200 с.: ил.

2. *Глуховский М.Д., Сахаров Д.В.* К вопросам информационной безопасности SS7 в современном мире // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 331-335.

3. *Ермилов Е.В.,* Анализ и управление рисками нарушения информационной безопасности критически важного объекта: автореферат дис. ... кандидата технических наук: 05.13.19 / Ермилов Евгений Викторович; [Место защиты: Воронеж. гос. техн. ун-т]. - Воронеж, 2014. - 17 с.

4. *Pavel Sh., Audrey K., Artem G., Ernest B.* A technique for detecting the substitution of a java-module of an information system prone to pharming with using a hidden embedding of a digital watermark resistant to decompilation // В сборнике: International Congress on Ultra Modern Telecommunications and Control Systems and Workshops. 13. Сер. "2021 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT 2021" 2021. С. 219-223.

5. *Сахаров Д.В., Красов А.В., Ушаков И.А., Бирих Э.В.* Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе ipv6 // Защита информации. Инсайд. 2020. № 1 (91). С. 51-57.

6. *Бирих Э.В., Гаврилов А.С., Сацук Е.Н.* Современные проблемы обеспечения внутренней безопасности распределенной сети органов государственной власти // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 104-107.

7. *Бирих Э.В., Кошурин А.Д., Кушнир Д.В., Стародубова Д.Д.* Исследование вопросов повышения уровня защищенности органов исполнительной власти // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 107-110.

8. *Бирих Э.В., Ферапонтова С.С.* К вопросу об аудите персональных данных // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 111-114.

9. *Бирих Э.В., Виткова Л.А., Сахаров Д.В., Шашкин В.С.* Алгоритмы BIG DATA и мониторинг ит инфраструктуры предприятия // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 100-103.

10. *Бирих Э.В., Рябов Е.Ю., Сахаров Д.В.* Методология формирования модели угроз безопасности информационных систем // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 103-107.

11. *Бирих Э.В., Виткова Л.А., Гореленко В.В., Казаков Д.Б.* Защита информации в базах данных // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 89-92.

12. *Бирих Э.В., Виткова Л.А., Левин М.В., Чмутов М.В.* Развитие стандартов и руководств в сфере облачных технологий // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 92-95.

13. *Бирих Э.В., Виткова Л.А., Сахаров Д.В., Сергеева И.Ю.* Метод повышения безопасности распределенной вычислительной системы на базе СППР и с учетом прогнозирования состояния // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 96-100.

14. *Герлинг Е.Ю., Кулишкина Е.И., Бирих Э.В., Виткова Л.А.* Модели нарушителей информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности. 2017. Т. 35. № 1. С. 27-30.

15. *Бирих Э.В., Сахаров Д.В.* Модель нарушителя распределенной информационно-вычислительной сети // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 235-238.

16. *Карев А.С., Бирих Э.В., Сахаров Д.В., Виткова Л.А.* Проблемы информационной безопасности в интернете вещей // В сборнике: Интернет вещей и 5G. 2016. С. 66-70.

Голембиовский М.М.
Аспирант кафедры”СИБ”
Брянский государственный технический университет
maksim32region@yandex.ru

Разработка методики расследования компьютерных инцидентов

Аннотация: Аннотация проекта.

Проект выполняется в рамках национальной программы «Цифровая экономика Российской Федерации» (федеральные проекты "Информационная безопасность", "Искусственный интеллект").

Основным направлением является обеспечение информационной безопасности на основе отечественных разработок при передаче, обработке и хранении данных, гарантирующей защиту интересов личности, бизнеса и государства.

Проект направлен на разработку методики, позволяющей выявить следы инцидента информационной безопасности, ведущие к возможному злоумышленнику.

Методика включает в себя следующие этапы:

1.Сбор и анализ исходных данных (планируется формулирование новых параметров для определения инцидентов ИБ).

2.Разработка классификатора инцидентов ИБ с возможностью наполнения базы инцидентов ИБ.

3.Разработка и наполнение базы сценариев инцидентов

4.Формализация работы алгоритма выявления инцидента (типовые и нетиповые случаи).

5. Автоматизирование методики, включающей вышеперечисленные действия с инцидентами.

Ключевые слова: компьютерная криминалистика, информационная безопасность.

Введение

Глобальная информатизация общества с каждым годом набирает обороты. Все большее количество данных переводится в электронный вид, в котором после хранится и обрабатывается. Это в свою очередь упрощает процесс их уничтожения или кражи и значительно усложняет процессы расследования подобных преступлений, поскольку данные действия нарушитель может совершить, не имея физического доступа к объекту.

Согласно статистике МВД, число киберпреступлений за 2021 поднялось на треть. По приведенной ведомством информации, злоумышленники на 39% чаще использовали мобильные сети для осуществления своих целей, а сеть интернет - на 51,3% чаще. Кроме того, наибольшая доля прироста показателей подобных преступлений зафиксирована в Северной Осетии (87%), а также в Севастополе - 77% и Тульской области - 71%. Ранее в СК заявили о росте уровня киберпреступности в 20 раз за семь лет.

Данная статистика показывает, что проблема расследования компьютерных инцидентов стоит очень остро. Необходимо внедрение новых подходов и методик.

Компьютерная криминалистика является относительно новым направлением как в правовом поле, так и в качестве ответвления сферы информационной безопасности. Тем не менее само понятие компьютерного преступления существует уже достаточно давно в Российской Федерации имеется ряд статей УК РФ, регламентирующих порядок их расследования и назначения наказаний (Ст. 272. Неправомерный доступ к компьютерной информации и другие), а также рекомендации по проведению процедуры расследования.

Основная часть.

На данный момент такое направление, как выявление следов инцидентов в компьютерной криминалистике находится на пути своего становления. Большинство публикаций в данной области направлены на поиски следов компьютерных инцидентов, так называемых цифровых следов.

Инцидент информационной безопасности (инцидент ИБ) – событие и/или серия событий, которые привели, приводят или могут привести с высокой долей вероятности к нарушению бизнес процессов и реализации угроз информационной безопасности.

Цифровой след — это уникальный набор действий в Интернете или на цифровых устройствах, информация, оставленная в результате просмотра веб-страниц и сохраненная в виде куков [1].

В статье Чуваткина Б.Ю. «Следы компьютерных инцидентов при проведении компьютерно-технических исследований» определяется перечень следов, которые можно обнаружить, зафиксировать, изъять и исследовать при проведении экспертизы.

Основное направление публикаций носит теоретический характер, в то время как компьютерная криминалистика больше зависит от практических составляющих.

В результате анализа диссертационной работы «Тактика производства следственных действий при расследовании киберпреступлений» [4] - Шевченко Е.С. можно сделать вывод о том, что есть острая необходимость ответвления компьютерной криминалистики от общих следственных действий, поскольку качественное расследование требует особых знаний и подготовки в сфере информационной безопасности и наличия специального оборудования.

Баранов В.А. в диссертационной работе «Обнаружение инцидентов информационной безопасности как разладки процесса функционирования системы» [5] предлагает организовать определение момента времени перехода из регулярного режима работы в аномальный путем исследования математической модели разладки случайного процесса.

На основе первичного анализа существующей нормативно-правовой базы и научных трудов, можно сделать вывод, о том, что на данный момент времени нет единой методики, содержащей структурированный подход к расследованию компьютерных преступлений, учитывающей одновременно все аспекты уголовного делопроизводства и компьютерной экспертизы. В целом наблюдается недостаток как нормативно-правовой, так и научной базы. Существующие документы и научные труды содержат только общие рекомендации по данному вопросу.

В разработке методики расследования компьютерных инцидентов предлагается:

- Классификация компьютерных инцидентов;
- Разработка алгоритмов расследования компьютерных преступлений;
- Подбор средств и методов расследования компьютерных преступлений;
- Практические инструкции методов расследования.

Объектом исследования являются компьютерные инциденты (зафиксированные события, связанные с нарушением или прекращением функционирования объектов КИИ; нарушения безопасности обрабатываемой объектом информации, в том числе произошедший в результате компьютерной атаки).

Целью исследования является разработка методики расследования компьютерных инцидентов.

Для достижения поставленной цели необходимо решить следующие **задачи:**

1. Провести анализ существующей нормативно-правовой базы, научной литературы и диссертационных работ в области компьютерной криминалистики.
2. Разработать методику расследования компьютерных инцидентов (создание классификации компьютерных инцидентов).
3. Провести анализ имеющихся исходных данных в сфере компьютерной криминалистики.
4. Определить топологии инцидентов информационной безопасности.
5. Создать методику восстановления этапов реализации инцидента.
6. Сформировать отчет по полученным инцидентам

Основные научные результаты и их научная новизна состоят в следующем:

- Разработка методики расследования, включающую алгоритмы классификации, подбора средств и методов расследования инцидентов ИБ, отличающихся от известных.
- Формализация и автоматизация процесса выявления инцидентов

Практическая значимость выражается в повышении эффективности расследования компьютерных преступлений и раскрываемости подобных дел, а также в сокращении количества компьютерных преступлений за счет их оперативного раскрытия.

В рамках проекта планируется использование:

1. Методов научных исследований, включающих системный анализ, математическое моделирование.
2. Метода формализации в части анализа исходных данных для определения возможного ущерба от реализации инцидента ИБ.
3.. Метода классификации в части разработки классификаторов инцидента и его сценариев.

ЗАКЛЮЧЕНИЕ

После рассмотрения нормативно-правовой базы и результатов научных исследований в сфере компьютерной криминалистике связанных с инцидентами информационной безопасности, был сделан вывод о том, что на данный момент времени нет единой методики, содержащей структурированный подход к расследованию компьютерных инцидентов, учитывающей одновременно все аспекты уголовного делопроизводства и компьютерной экспертизы. В целом наблюдается недостаток как нормативно-правовой, так и сформированной практической базы расследования инцидентов.

Существующие документы и научные труды содержат только общие рекомендации по данному вопросу. Выявлена необходимость внедрения новых методик.

В рамках данной работы планируется описание разработки методики расследования компьютерных инцидентов.

В ходе выполнения данной работы разрабатывается методика расследования компьютерных инцидентов, включающая алгоритмы классификации, подбора средств и методов расследования инцидентов ИБ, отличающихся от известных своей скомпонованностью.

СПИСОК ЛИТЕРАТУРЫ

1. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф.. — Саратов : Профобразование, 2019. — 543 c. — ISBN 978-5-4488-0074-0.
2. Селезнев А.В. Современные проблемы криминалистики: учебное пособие / Селезнев А.В., Сысоев Э.В.. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2012. — 160 c.
3. Мальцагов, И. Д. Современные технологии в расследовании преступлений: компьютерная криминалистика / И. Д. Мальцагов // Экономика. Бизнес. Право. – 2018. – № 4-6(26). – С. 44-48.
4. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений[Электронный ресурс] – URL:https://www.dissercat.com/content/taktika-proizvodstva-sledstvennykh-deistvii-pri-rassledovanii-kiberprestuplenii
5. (Дата обращения: 8.07.2022).
6. Баранов В.А. Обнаружение инцидентов информационной безопасности как разладки процесса функционирования системы [Электронный ресурс] – URL: https://www.dissercat.com/content/modeli-i-algoritmy-kontrolya-intsidentov-informatsionnoi-bezopasnosti-v-korporativnoi-teleko (Дата обращения: 10.07.2022).
7. Кришталюк, А. Н. Правовые аспекты системы безопасности: курс лекций / А. Н. Кришталюк. — Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 204 с.
8. Монахова М.М. Модели и алгоритмы контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети [Электронный ресурс] – URL: https://www.dissercat.com/content/modeli-i-algoritmy-kontrolya-intsidentov-informatsionnoi-bezopasnosti-v-korporativnoi-teleko (Дата обращения: 8.07.2022).
9. Майорова, Е. В. Методические аспекты реагирования на инциденты информационной безопасности в условиях цифровой экономики / Е. В. Майорова // Петербургский экономический журнал. – 2020. – № 1. – С. 155-162.
10. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, 30.05.2014 г.
11. Ваценко, А. А. Обзор техник компьютерной криминалистики / А. А. Ваценко // Бюллетень науки и практики. – 2020. – Т. 6. – № 6. – С. 167-174.

Домуховский Н.А.
Уральский федеральный университет, старший преподаватель
N.A.Domukhovsky@urfu.ru

ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ ПУТЕМ МОДЕЛИРОВАНИЯ КОМПЛЕКСНЫХ АТАК

Аннотация: Задача оценки уровня защищенности компьютерных систем актуальна на стадии создания системы и во время ее эксплуатации. Известны различные методы, решающие указанную задачу на всех стадиях жизненного цикла компьютерной системы, но эти методы обладают рядом недостатков. Наиболее распространены методы моделирования угроз (в большей степени для создаваемых компьютерных систем) [1] и оценки рисков (в большей степени для эксплуатируемых систем) [2].

Оба подхода представляют реальную систему в виде некоторой упрощенной математической модели, для которой определяются возможные негативные последствия и действия, приводящие к ним. Создание модели, а также определение негативных последствий и действий требует участия экспертов, способных оценить качественно или количественно те или иные параметры модели или вредоносного воздействия на нее. Развитие методов моделирования направлено на снижение роли субъективных экспертных оценок в общей оценке защищенности компьютерной системы, одновременно с повышением точности моделирования, чтобы учесть как можно больше значимых параметров системы: состав ее компонентов, сетевую топологию, реализованные защитные меры и пр.

Описанная в статье работа направлена на разработку метода моделирования комплексных атак в отношении проектируемой или эксплуатируемой компьютерной системы, являющейся автоматизированной системой управления технологическим процессом. Метод опирается на сведения о составе и топологии системы, известные техники и тактики действий нарушителей и представление ущерба системе в виде совокупности базовых негативных событий, объединенный в общее дерево неисправностей [3].

Ключевые слова: Информационная безопасность. Оценка рисков. Моделирование комплексных атак. Дерево атак. Уязвимости.

Целью описываемой работы является разработка метода оценки защищенности компьютерных систем, обладающего следующими свойствами:

- метод должен реализовать количественную оценку остаточного риска информационной безопасности (ИБ), для возможности сравнения разных стратегий уменьшения рисков ИБ;
- метод должен быть инвариантен по отношению к оцениваемой системе, что означает, что метод должен применяться без модификаций алгоритмов расчета и моделирования при изменении исходных данных об оцениваемой системе;
- метод должен минимально использовать количественные экспертные оценки, приоритетно использование оценок из внешних доверенных источников (например, оценки уязвимостей по методике CVSS [4], банка данных угроз и уязвимостей ФСТЭК России [5] или сведения о тактиках и техниках злоумышленника из матрицы MITRE ATT&CK [6]).

Применение обоснованной количественной оценки рисков ИБ позволяет подобрать оптимальную стратегию обработки рисков, которая является задачей определения парето-оптимального множества стратегий обработки риска [7]. В итоге это позволяет подобрать эффективную стратегию инвестирования в систему обеспечения ИБ, которая снизит риски до заданного уровня, затратив на это минимальное количество ресурсов.

Традиционные методы оценки рисков ИБ предполагают наличие априорной информации о ценности защищаемых активов и вероятности реализации угроз ИБ в отношении этого актива. В [2] в примечании к определению риска ИБ указано, что он «измеряется исходя из комбинации вероятности события и его последствия». Все дальнейшие методики, представленные в [2] исходят из того, что вероятность события и последствия его реализации известны эксперту до проведения процедуры оценки рисков.

Известны работы, где пытаются задачу оценки вероятности наступления достаточно сложного события в отношении активов свести к более простым. Например в [8] предлагается рассматривать вероятность нежелательного события как комплексную случайную величину, которая формируется из более простых случайных величин (соответствующих вероятности реализации конкретной угрозы в отношении конкретного актива). Однако и такой метод не лишен недостатков: вероятность реализации одной и той же угрозы в отношении одного и того же актива может зависеть от множества дополнительных факторов.

Эти особенности классического риск-ориентированного подхода отмечают в [7] и в [9]. В частности, вероятность события нанесения ущерба некоторому активу будет зависеть от местоположения нарушителя относительно этого актива: если он расположен за периметром локальной сети, то нарушителю доступен ограниченный набор уязвимостей, с которыми он может попытаться преодолеть периметр сети. Если же нарушитель уже проник во внутреннюю сеть и, например, успешно закрепился на другом активе, который функционирует под управлением аналогичной операционной системы (ОС), то вероятность успешной атаки на исходный актив существенно возрастает.

Таким образом, для моделирования комплексной атаки на актив, позволяющей корректно оценить вероятность ее успешной реализации, необходимо учитывать топологию активов компьютерной системы (их взаимное расположение), а также расположение нарушителя относительно активов компьютерной системы. При этом нужно корректно учитывать изменение положения нарушителя относительно активов по мере реализации комплексной атаки.

В [7] указанная задача решается путем формирования дерева атак, где:

- корнем дерева является начальное положение нарушителя (например, сеть Интернет);
- вершинами дерева являются активы (сетевые устройства, программное обеспечение или информационные активы, обрабатываемые на этих устройствах);
- переходами же являются элементарные атаки нарушителя, которые характеризуются условной вероятностью их реализации, а также последствиями от их реализации (для дальнейшей оценки ущерба).

При этом условная вероятность перехода зависит от сетевой топологии (расположены ли активы в одном сетевом сегменте или их разделяют средства обеспечения сетевой безопасности), а также от уже проведенных успешных атак. Соответственно, для описания дерева атак по методу, приведенному в [7] требуется априорное знание условных вероятностей элементарных атак вида «вероятность успешного взлома клиентской рабочей станции при условии успешного взлома рабочей станции такого же типа» и т.п. Указанные условные вероятности предлагается определять экспертным методом. Также надо отметить, что состав этих условных вероятностей должен определяться для каждой оцениваемой системы индивидуально, что требует адаптировать метод для каждой новой оцениваемой системы и повторно привлекать эксперта для оценки условных вероятностей.

В [9] предложен схожий метод, но существенным отличием является то, что результатом применения метода к описанию сетевой топологии компьютерной системы будет не дерево, а ориентированный граф атак – так как злоумышленник вполне может двигаться к одной цели различными путями. Вершинами графа также являются активы, которые теперь представляют собой потенциальные цели для атак. Ребра графа – это элементарные атаки, которые проводит нарушитель.

Оценку вероятности комплексной атаки в [9] предлагается осуществлять качественно, используя оценку CVSS [4]. CVSS определяет ряд параметров для каждой уязвимости – метрик. В частности, метрику сложности атаки (Attack Complexity – AC), принимающую значения Low (простая атака) и High (сложная атака). В [9] предлагается качественно оценивать вероятность успеха комплексной атаки следующий образом:

- если в составе комплексной атаки присутствует хотя бы одна элементарная атака, метрика AC которой имеет значение High, то вероятность реализации такой комплексной атаки – низкая;
- в ином случае вероятность реализации комплексной атаки высокая.

Несмотря на использование достаточно грубой качественной оценки, предложенный в [9] подход хорош тем, что он позволяет использовать внешние базы данных уязвимостей, содержащие оценки CVSS для них, что снижает требования к эксперту, определяющему исходные данные для моделирования комплексных атак.

Некоторые методы моделирования угроз рассмотрены в [10]. В частности, к наиболее развитым методам отнесены TRIKE и PASTA (Process for Attack Simulation & Threat Analysis). Метод TRIKE, несмотря на свои преимущества, в настоящее время не развивается и признан нерекомендуемым к использованию (deprecated). PASTA –более обобщенная методика, которая включает следующие этапы:

- определение «действующих лиц» (т.е. пользователей и потенциальных нарушителей);
- оценка активов (с помощью анализа влияния на бизнес, но сразу оговаривается, что это за рамками методики PASTA);
- определение набора легальных действий в системе (use cases);
- построение дерева атак, которое определяет конечное нежелательное событие для актива (нарушение конфиденциальности, целостности или доступности) и далее всю цепочку

элементарных событий, которые приводят к достижению этого конечного события; при этом элементами дерева являются не только эксплуатация уязвимостей системы, но также некорректное использование легальных действий в системе (abuse cases);

– на финальном этапе задаются доступные действия (корректные и некорректные), а также присутствующие в системе уязвимости, затем рассчитываются все достижимые для этого нарушителя виды ущерба для активов; при этом финальная оценка вероятности или величины последствий (по сути – оценка рисков) не является частью методики.

Таким образом, методика PASTA также имеет явные минусы: деревья атак, перечень легальных и некорректных действий должны определяться экспертами для каждой оцениваемой системы. Кроме того, результаты использования методики PASTA не самодостаточны, так как требуются отдельные методики оценки последствий нанесения ущерба активам и расчета конечного риска для актива.

В рамках исследовательского проекта предлагается реализовать альтернативный метод комплексного моделирования атак, основанных на построении ориентированного графа комплексных атак, который использует сведения об уязвимостях, например, представленные в формате CVSS и позволяет проводить количественную оценку вероятности реализации комплексной атаки.

Для построения ориентированного графа комплексных атак предполагается использовать следующие исходные данные (включая экспертные оценки):

– сведения о компьютерной системе: состав компонентов и сведения об их взаимном расположении;
– описание актуальных уязвимостей (в частности, на основе публичных баз данных уязвимостей, например, БДУ ФСТЭК России), включая оценку параметров уязвимостей по стандарту CVSS;
– сведения об эффективности защитных мер, которые могут быть как детерминированные (в этом случае мера либо предотвращает/обнаруживает эксплуатацию уязвимости), так и вероятностные, когда эффективность меры задана вероятностью успешного обнаружения/предотвращения уязвимости (также может являться экспертной оценкой);
– сведения об ущербе системе в целом, задаваемые посредством дерева неисправностей [3];
– сведения о начальном положении злоумышленника.

Для моделирования комплексных атак, на основе исходных данных строится граф атак, учитывающий топологию оцениваемой системы, сведения об уязвимостях и начальном положении злоумышленника по алгоритму, описанному в [11]. Представление всех возможных атак в виде ориентированного графа позволяет находить оптимальные стратегии проведения комплексной атаки для нарушителя, а значит выявлять слабые места оцениваемой системы. Указанный подход не зависит от конкретной компьютерной системы и требует минимального участия эксперта для проведения оценки защищенности.

СПИСОК ЛИТЕРАТУРЫ

1. Shostack A. Threat modeling: designing for security. Indianapolis, IN: Wiley, 2014. 590 с.
2. ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. Москва: Стандартинформ, 2016.
3. ГОСТ Р 27.302-2009 Надежность в технике. Анализ дерева неисправностей. Москва: Стандартинформ, 2012.
4. CVSS v3.1 Specification Document // FIRST — Forum of Incident Response and Security Teams. URL: https://www.first.org/cvss/v3.1/specification-document (дата обращения: 26.08.2022).
5. Банк данных угроз и уязвимостей ФСТЭК России. URL: https://bdu.fstec.ru/ (дата обращения: 26.08.2022).
6. MITRE ATT&CK®. URL: https://attack.mitre.org/ (дата обращения: 26.08.2022).
7. Musman S., Turner A. A game theoretic approach to cyber security risk management // Journal of Defense Modeling & Simulation. 2018. Vol. 15, № 2. P. 127–146.
8. Немиткина, В. В. Анализ и управление рисками в области защиты информации[Текст]: дис. канд. экон. наук / В. В. Немиткина. – М., 2009. – 230 с.
9. Котенко И.В., Степашкин М.В., Богданов В.С. Оценка Безопасности Компьютерных Сетей На Основе Графов Атак И Качественных Метрик Защищенности // Труды Спииран. 2006. Том 2, № 3.
10. Afnan Siddique. Threat Modeling Methodologies for Network Security. URL: https://www.researchgate.net/publication/350891779_Threat_Modeling_Methodologies_for_Network_Security (дата обращения: 26.08.2022).

11. Domukhovskii N. Optimal Attack Chain Building Algorithm // Препр. / 2022 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2022.

Жерлицын С.А.
КубГТУ, аспирант,
kpytoooooo@gmail.com

РАЗРАБОТКА СИСТЕМЫ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ НА ОСНОВЕ БИОМЕТРИЧЕСКИХ ХАРАКТЕРИСТИК ДЛЯ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ.

Аннотация: в данной работе описывается система биометрической идентификации личности, пригодной для эксплуатации в распределенных информационных системах. Описываются основные цели исследования, а также задачи, поставленные в ходе разработки. Приводится описание основных механизмов, методов и подходов, применяемых в ходе разработки. Приводится решение основных проблем, связанных с удаленным применением нейросетевых алгоритмов в задачах обработки биометрии, характерных для работы с распределенными системами. Предлагается модульная архитектура системы, состоящая из нескольких блоков: модели, гибридизатор, модуль алгоритмов обучения, модуль тестирования, каждый из которых решает свою подзадачу. Также в исследовании представлены анализ современного состояния исследований в области, новизна предлагаемой методологии и ожидаемые научные результаты реализации проекта.

Ключевые слова: идентификация личности, биометрия, информационная безопасность, машинное обучение, искусственный интеллект, роевой интеллект, нейронные сети, анализ данных.

Основной целью исследования является разработка методов построения систем биометрической идентификации личности для распределенных систем, обладающих рядом свойств. Во главе данного списка находится надежность и безопасность, достигаемая путем построения защищенной централизованной архитектуры для идентификации личности, пригодной для применения в распределенных системах. Также не менее важной характеристикой является унифицированный обобщенный механизм реализации идентификации личности по биометрическим характеристикам разного вида в целях достижения масштабируемости, гибкости и единообразия.

В качестве основных задач исследования выделяется непосредственно разработка модулей для идентификации личности по рисунку вен ладони, сетчатке и радужке глаза, отпечатку пальца, геометрии лица, клавиатурному и экранному почерку и другим биометрическим характеристикам. Исследование способов повышения автономности нейросетевых систем для возможности безопасного применения на оконечных устройствах, в том числе защищенной системы удаленной обработки биометрических данных. Разработка системы автоматизированного обучения и дообучения опознающих модулей, программная и программно-аппаратная реализация оконечных устройств биометрической идентификации, а также централизованного сервера биометрической идентификации. Для надежного взаимодействия полученных компонентов выделяется этап разработки протокола авторизации на основе разработанных систем.

В числе последних тенденций развития механизмов аутентификации нельзя не выделить повышение спроса на методы, использующие биометрические характеристики субъекта [2, 3, 4]. Среди их особенностей можно выделить следующие пункты:

- неотъемлемость – носителем данных является сам человек, за счёт чего носитель нельзя забыть или потерять, за исключением критических случаев, зачастую опасных для здоровья;
- нечёткость – биометрические характеристики не всегда могут быть определены точно и имеют естественный диапазон допустимого колебания;
- невозможность перевыпуска – при компрометации данных такого типа становится невозможно использовать соответствующий тип биометрической аутентификации, так как злоумышленник сможет в любой момент получить выдать себя за истинного носителя.

Существует целый ряд публикаций, описывающих математический аппарат или детали реализации идентификации личности по тому или иному биометрическому параметру: на основе распознавания лиц [4], по рисунку вен ладони [5], по голосу [6], на основе анализа поведения [7] и многие другие. Однако ни в одной из них не решается задача унификации и разработки единого подхода к идентификации по нескольким различным биометрическим характеристикам.

Также в рамках исследования было проведен анализ способов идентификации личности по одной из биометрических характеристик – рисунку вен ладони. В данный момент существует 2 наиболее популярных метода идентификации личности по рисунку вен ладони: на основе вычисления

расстояния (с учетом таких параметров, как косинусное расстояние, евклидово расстояние, масштабирование и поворот изображения на произвольный угол) и графовый метод.

Недостатками данных методов являются высокая вычислительная сложность при эксплуатации из-за необходимости сравнения предъявленного образца с каждым из эталонных изображений, необходимость доступа к базе эталонных биометрических данных при прохождении процедуры идентификации и зависимость от качества освещения, угла и изгиба ладони, зашумлённости изображения, фона, общая неустойчивость работы [8].

В исследовании Р. Фуксис [9] представлена информация по изучению влияния типа освещения руки на качество изображения (отражение и пропускание): схема пропускания более громоздка в реализации, однако полученные изображения отличаются более высокой контрастностью и точностью.

Предложенные в исследовании методы были построены на основе ресурсоёмких математический преобразований по нахождению сходства исходного изображения с элементарными фильтрами, вследствие чего полученная система для успешного сопоставления нуждалась в хранении некого шаблона, идеального образца, по которому и вычисляется проверка личности. При данном подходе сокращается время обучения модели, однако не применяются последние достижения машинного обучения: элементарные фильтры составляются вручную, в следствие чего создаётся жёсткая завязка программной и аппаратной реализаций, повышается прихотливость и неустойчивость работы модели, затрудняется процесс модернизации и модификации.

Для реализации опознающих нейросетевых модулей предлагается использовать глубокую нейронную сеть, структура которой зависит непосредственно от рассматриваемого биометрического идентификатора и включает в свой состав несколько компонентов: вариативную часть и общую. Архитектура вариативного компонента сети является индивидуальной для каждого отдельного типа идентификатора (рекуррентная для голоса и поведенческих признаков, свёрточная для рисунка вен ладони и т.д.), его цель состоит в первичной обработке предоставленного образца, удалении шумов и посторонней информации а также приведению выделенной информации к единому для всех видов идентификаторов формату карты признаков. Общая часть имеет единую архитектуру, но отличается весами от модуля к модулю, её задача заключается в установлении соответствия между полученной от вариативного блока карты признаков и пространством субъектов.

В силу изменчивости как самих биометрических идентификаторов, так и набора пользователей системы, для недопущения деградации её надёжности и эффективности необходима система автоматизированного обучения и дообучения распознающих модулей. Для реализации данной системы предлагается использовать модульную систему автоматизированного машинного обучения с применением как классических, так и эвристических алгоритмов. Предложенная система состоит из нескольких блоков: модели, гибридизатор, модуль алгоритмов обучения, модуль тестирования, каждый из которых решает свою подзадачу. Отдельно стоит обратить внимание на модуль гибридизации, позволяющий вносить изменения как в способ обучения модели, так и в её строение, если показатели точности по результатам проверок в модуле тестирования перестают расти. Особенно эффективно раскрываются в данной системе алгоритмы роевого интеллекта, также включенные в модуль алгоритмов обучения в силу простоты их гибридизации и адаптивности.

Для реализации безопасного обмена биометрическими параметрами в условиях работы с удалённым сервером идентификации предлагается использовать систему полностью гомоморфного шифрования [10], позволяющую отправить на сервер биометрические персональные данные в зашифрованном виде, обработать их при помощи нейронной сети, получить зашифрованный результат вычислений и уже локально расшифровывать его и сравнивать с пространством субъектов идентификации.

Новизна исследования складывается из следующих характеристик и особенностей разрабатываемой технологии:

- Построение инновационной безопасной клиент-серверная архитектуры системы биометрической идентификации личности.
- Разработка единого универсального подхода к обработке биометрических идентификаторов на основе нейронных сетей.
- Использование современных актуальных и эффективных моделей и архитектур нейронных сетей.
- Применение новых, мало исследованных, но показавших свою эффективность в ряде прикладных задач эволюционных алгоритмов и алгоритмов роевого интеллекта.
- Разработка систем идентификации по ряду слабо проработанных и редко применяемых биометрических характеристик с использованием современных технологий и возможностей методов

искусственного интеллекта (например, идентификация по рисунку вен ладони, по экранному почерку, по радужке глаза и так далее).

- Построение модульной системы автоматизированного машинного обучения для распознающих модулей.
- Исследование и практическая реализация способов гибридизации алгоритмов обучения для повышения их эффективности в рамках работы с конкретной моделью.
- Разработка протокола биометрической идентификации личности с применением новых систем гомоморфного шифрования.

В рамках исследования проведен анализ и патентный поиск, разработан и получен патент на способ биометрической идентификации личности по рисунку вен ладони (RU 2761776 C1).

Ожидаемым результатом по итогам выполнения проекта является обеспечение безопасного применения идентификации личности по биометрическим параметрам, затруднение компрометации биометрического идентификатора. Унификация подхода к применению систем биометрической идентификации. Повышение безопасности биометрических персональных данных. Повышение надежности и эргономичности систем разграничения и предоставления доступа.

СПИСОК ЛИТЕРАТУРЫ

1. Jain, A K, Ross A and Pankanti S Biometrics: a tool for information security, Trans. Inf. Forensics Secur 1(2), 2006, p. 125–143.
2. Hassanat, A.B., Albustanji, A., Tarawneh, A.S., Alrashidi, M., Alharbi, H., Alanazi, M., Alghamdi, M., Alkhazi, I.S., & Prasath, V., Deep learning for identification and face, gender, expression recognition under constraints, ArXiv, abs/2111.01930, 2021.
3. Soleymani, S., Dabouei, A., Taherkhani, F., Iranmanesh, S.M., Dawson, J.M., & Nasrabadi, N.M., Quality-Aware Multimodal Biometric Recognition, ArXiv, abs/2112.05827, 2021.
4. Mugalu, B.W., Wamala, R.C., Serugunda, J., & Katumba, A. (2021). Face Recognition as a Method of Authentication in a Web-Based System. ArXiv, abs/2103.15144.
5. Marattukalam, F., Abdulla, W.H., & Swain, A.K. (2021). N-shot Palm Vein Verification Using Siamese Networks. 2021 International Conference of the Biometrics Special Interest Group (BIOSIG), 1-5.
6. Meng, Z., Altaf, M.U., & Juang, B. (2020). Active voice authentication. ArXiv, abs/2004.12071.
7. Stragapede, G., Vera-Rodríguez, R., Tolosana, R., Morales, A., Acien, A., & Lan, G.L. (2022). Mobile Behavioral Biometrics for Passive Authentication. ArXiv, abs/2203.07300.
8. Im S, Park H, Kim Y, Han S, Kim S, Kang C, Chung C, A Biometric identification system by extracting hand vein patterns, J Korean Phys Soc 28(3), 2001, p. 268-272
9. R. Fuksis, M. Pudzs, M. Greitans, Palm Vein Biometrics Based on Palm Infrared Imaging and Complex Matched Filtering, The 12th ACM Workshop on Multimedia and Security, Rome, 2009, p. 27.
10. Частикова, В.А. Разработка архитектуры машинного обучения с использованием гомоморфного шифрования для обеспечения конфиденциальности данных / В.А. Частикова, С. А. Жерлицын, А. Н. Пешков, А. С. Карапетян // Электронный сетевой политематический журнал "Научные труды КубГТУ". — 2022. — №2. — 135-147.

Иванов С.О.
ФГБОУ ВО ЧГУ им. И.Н. Ульянова, старший преподаватель
v101-11@mail.ru

РАЗРАБОТКА ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ЦИФРОВОЙ ЭЛЕКТРИЧЕСКОЙ ПОДСТАНЦИИ, ДЛЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ И НАРУШЕНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Аннотация: Предлагается разработать методы применения искусственных нейронных сетей для выявления угроз и нарушений информационной безопасности в локальной вычислительной сети цифровой электрической подстанции. Основными задачами проекта являются: сбор и анализ данных имеющихся в трафике локальной вычислительной сети цифровой электрической подстанции в штатном режиме и при наличии угроз и нарушений; разработка методов конфигурирования и обучения искусственных нейронных сетей для выявления нарушений и аномалий в работе; тестирование разработанных методов в испытательной лаборатории. На практике результаты работы могут быть использованы в качестве дополнительного средства контроля состояния цифровой электрической подстанции, а также средством предотвращение вторжений (компьютерных атак) требуемым для объектов критической информационной инфраструктуры.

Ключевые слова: цифровая подстанция, нейросетевое моделирование, киберугрозы, выявление аномалий, вычислительные методы, нарушение информационной безопасности, объекты критической информационной инфраструктуры, машинное обучение, анализ данных.

Цифровая электрическая подстанция это электрическая станция, где обмен данными между вторичным оборудованием осуществляется в цифровой форме, что дает возможность организовать более эффективную работу первичного за счет автоматизации технологических процессов [1]. Для реализации технологий цифровой подстанции используются компьютеры и компьютерные сети, из-за чего в работе цифровой подстанции появляются риски информационной безопасности приводящие к физическим последствиям.

Среди различных подходов к кибербезопасности цифровой электрической подстанции можно выделить:

- выполнение требований федеральных законов, в частности ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" [2], которые определяют необходимые защитные меры;
- обеспечение устойчивости и восстанавливаемости при киберинцидентах [3, 4];
- контроль и анализ информационного обмена во вторичном оборудовании [5, 6, 7, 8,];

Применение обычных средств защиты информации недостаточно, так как они осуществлять защиту на уровне технологического процесса, но не мешать ему. Необходимо контролировать состояние элементов цифровой электрической подстанции, а также выявлять аномальные режимы работы элементов цифровой электрической подстанции и данных сетевого трафика.

Основным объектом контроля в цифровой подстанции является сетевой трафик. В соответствии с требованиями приказа ФСТЭК [9], для предотвращения вторжений (компьютерных атак) следует использовать средства обнаружения вторжений (СОВ). Методы работы СОВ основаны на обнаружении следов атак и/или выявление аномалий [10, 11].

В настоящее время, для обнаружения вторжений в сетевом трафике используются методы машинного обучения, в частности, аппарат искусственных нейронных сетей (ИНС) [12,13].

Методы интеллектуального анализа данных (МИАД) могут применяться для задач классификации, кластеризации и прогнозирования в огромных массивах данных, в том числе в реальном времени. Однако, информационные потоки цифровых электрических подстанций могут включать в себя большое разнообразие режимов работы оборудования, как штатных (изменение нагрузки, коммутация) [14], так и аварийных (срабатывание релейной защиты) [15]. Поэтому наиболее перспективным является применение ИНС, для которой достаточно использовать репрезентативную выборку данных о штатном и аварийных режимах работы оборудования.

Обеспечить достаточный набор данных для обучения возможно либо на основе основе математических моделей работы цифровой подстанции [14], либо использовать специальное лабораторные стенды для генерации сетевого трафика [11].

Целью научного проекта является разработка, обоснование и тестирование искусственных

нейронных сетей для обнаружения аномалий сетевого трафика в локальной вычислительной сети цифровой электрической подстанции, для противодействия угрозам и нарушениям информационной безопасности.

Основные задачи:

- Сбор и анализ данных имеющихся в трафике локальной вычислительной сети цифровой электрической подстанции в штатном режиме и при наличии угроз и нарушений;
- Разработка методов конфигурирования и обучения искусственных нейронных сетей для выявления нарушений и аномалий в работе;
- Тестирование эффективности разработанных методов на базе «Испытательной лаборатории» организации ООО «Интеллектуальные сети».

Данный проект связан с темой диссертации автора "Распознавание искусственной нейронной сетью аномалий и нарушений в локальной вычислительной сети цифровой электрической подстанции". Полученные результаты будут использованы для создания программно-аппаратного комплекса выявления аномалий в сетях цифровой электрической подстанции.

Предлагается разработать методы применения искусственных нейронных сетей для отслеживания состояния элементов цифровой подстанции. По выявленным отклонениям в данных, содержащихся в сетевом трафике, ИНС должна определять режимы работы подстанции, а так же атаки и нарушения.

Необходимо определить оптимальную конфигурацию ИНС, а так же разработать методы обучения ИНС и программно-аппаратные средства анализа сетевого трафика для выявления аномалии в данных.

Новизна исследования заключается в обнаружении аномалий в совокупности параметров работы электрооборудования. Особенно важны коллективные и контекстные аномалии в данных.

Необходимо адаптировать ИНС для анализа различных промышленных протоколов (IEC 81650, IEC 60870-5-104, modbus, OPC)

Разрабатываемые методы конфигурирования и обучения ИНС помогут разработать средства контроля состояния цифровой электрической подстанции, которое может выявлять аномалии и нарушения в информационном обмене.

Будет определена конфигурация ИНС и требуемые программно-аппаратные средства, которые могут применяться для анализа сетевого трафика.

Исследования сетевого трафика цифровой подстанции в штатном и аварийных режимах работы оборудования позволит сформировать модель информационную обмена между вторичным оборудованием.

На практике результаты работы могут быть использованы для создания программно-аппаратного средства дополнительного контроля состояния цифровой электрической подстанции, а также средства предотвращение вторжений (компьютерных атак) требуемого для объектов критической информационной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

1. Что такое цифровая подстанция? // Цифровая подстанция. - URL: http://digitalsubstation.com/blog/2018/12/28/chto-takoe-tsifrovaya-podstantsiya/
2. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ (последняя редакция)26 июля 2017 года N 187-ФЗ
3. Назаров И.Г., Суслов Д.В., Никандров М.В., Славутский Л.А. Комплекс обеспечения контролируемой деградации системы управления энергообъекта при киберинцидентах // вестник чувашского университета. 2018. № 1. С. 146-152.
4. Колосок Ирина Николаевна, Коркина Елена Сергеевна Анализ кибербезопасности цифровой подстанции с позиций киберфизической системы // Информационные и математические технологии в науке и управлении. 2019. №3 (15). URL: https://cyberleninka.ru/article/n/analiz-kiberbezopasnosti-tsifrovoy-podstantsii-s-pozitsiy-kiberfizicheskoy-sistemy
5. Dharmendra K., Moushmi K., Zadgaonkar A.S. Analysis of generated harmonics due to transformer load on power system using artificial neural network // International journal of electrical engineering. – 2013. N 4, 1. – pp. 81-90
6. Grammatikis P. R. An Anomaly Detection Mechanism for IEC 60870-5-104. / P.R. Grammatikis, P. Sarigiannidis, A. Sarigiannidis, D. Margounakis, A. Tsiakalos, G. Efstathopoulos // 2020 9th

International Conference on Modern Circuits and Systems Technologies (MOCAST), Bremen, Germany. – 2020. – pp. 1-4. – doi: 10.1109/MOCAST49295.2020.9200285.
7. Kulikov A. L., Loskutov A. A., Mitrovic M. Improvement of the technical excellence of multiparameter relay protection by combining the signals of the measuring fault detectors using artificial intelligence methods // International Scientific and Technical Conference Smart Energy Systems 2019 (SES-2019). – 2019. N 124. – doi: https://doi.org/10.1051/e3sconf/201912401039
8. Voropai N.I. Issues of cybersecurity in electric power systems / N.I. Voropai, I.N. Kolosok, E.S. Korkina, A.B. Osak // Energy systems research. – 2020. 3, №2 (10). – pp.19-28
9. Приказ от 25 декабря 2017 г. N 239 "Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации"
10. Иванов С.О., Никандров М.В., Славутский Л.А. Способы выявления нарушений и аномалий протоколов МЭК 61850 // информационные технологии в электротехнике и электроэнергетике. материалы xii всероссийской научно-технической конференции. Чебоксары, 2020. С. 441-443.
11. O A Lysenko, A V Simakov and V V Kharlamov. Algorithm for testing digital substation protection devices in conditions of network distortions in the process bus. https://iopscience.iop.org/article/10.1088/1742-6596/1901/1/012014
12. Кожевникова, И. С. Применение машинного обучения для обнаружения сетевых аномалий / И. С. Кожевникова, Е. В. Ананьин, А. В. Лысенко, А. В. Никишова. — Текст : непосредственный // Молодой ученый. — 2016. — № 24 (128). — С. 19-21. — URL: https://moluch.ru/archive/128/35376/.
13. Кусакина Н. М. Применение методов нейронных сетей для построения систем выявления аномалий сетевого трафика // Colloquium-journal. 2019. №2-1 (26). URL: https://cyberleninka.ru/article/n/primenenie-metodov-neyronnyh-setey-dlya-postroeniya-sistem-vyyavleniya-anomaliy-setevogo-trafika
14. Laruhin A. Anomalous modes recognizing secondary equipment in electric power industry: adaptive neuro algorithms / A. Laruhin, M. Nikandrov, L. Slavutskii // 2019 International Ural conference on electrical power engineering: Proceedings URALCON. – 2019. – pp. 399-403.
15. Yadav A., Dash Y. An overview of transmission line protection by artificial neural network: fault detection, fault classification, fault location, and fault direction discrimination // Advances in Artificial Neural Systems. – 2014. – pp. 20.

Иниватов Д.П.
ОмГТУ, младший научный сотрудник,
daniilini@mail.ru

ИДЕНТИФИКАЦИЯ ДИКТОРА НА ОСНОВЕ АНСАМБЛЯ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Аннотация: в работе приведено описание проекта исследования, разобраны подходы к построению ПБК (преобразователя биометрия-код доступа), проанализированы проблемы обучения нейросетевых ПБК и предложен подход построения НПБК с предобучением. Также проведено сравнение существующих методов биометрической аутентификации дикторов и обосновывается актуальность использования ансамблирования комитетов нейронных сетей в задаче идентификации субъекта по голосовым параметрам.

Ключевые слова: аутентификация, ансамблирование, искусственные нейронные сети, биометрические образы, глубокое обучение, идентификация, квадратичные нейроны, сверточные сети.

С каждым годом информация и данные на электронных носителях продолжают играть все более заметную роль в нашей повседневной жизни, защита конфиденциальных данных становится всё более важной составляющей предприятий и пользователей, в связи с этим, способы осуществления аутентификации претерпевают революционные изменения. Классическим приёмом решения проблемы является защита данных с помощью паролей, шифрования либо аппаратных ключей. Применение данных методов для предоставления доступа – очень простое и универсальное решение, однако при их использовании ключи будут отчуждаемыми от владельца, а в случае попадания паролей третьим лицам защищенная информация будет скомпрометирована. Данную проблему пытаются решить с помощью аутентификации по биометрическим признакам. В дополнение к безопасности, движущей силой биометрической проверки является удобство, поскольку нет паролей, которые нужно помнить, или ключей (аппаратных аутентификаторов), которые необходимо всегда носить с собой.

Настоящая исследование посвящено решению комплекса проблем, связанных с надежностью биометрической аутентификации, защищенностью биометрических образов от компрометации и обучением биометрических систем на малых выборках биометрических данных.

Цели:

- Разработать нейросетевой преобразователь «биометрия-код» (НПБК) на основе голосовых паролей с использованием сверточных нейронных сетей с целью идентификации диктора;
- Разработать метод определения некоторых психофизиологических состояний при использовании голосовых образов дикторов;

Задачи:

- Разработать и обучить на разных формах представления голосовых записей различные архитектуры нейронных сетей;
- Оценить информативность полученных признаков в ходе обучения ИНС;
- Произвести анализ полученных нейронных сетей и составить из наиболее оптимальных из них комитет;
- Разработать программный комплекс для обеспечения удобного доступа и использования наработок.

Преобразователь «биометрия – код доступа» (ПБК) – преобразователь, осуществляющий перевод неоднозначных биометрических данных, принадлежащих множеству «Свой», в однозначный код – биометрический пароль. В случае подачи на вход данного преобразователя биометрических параметров, относящихся к множеству «Чужой», на выходе следует ожидать вектор случайных значений [1, 2]. НПБК представляет собой искусственную нейронную сеть, которая обучается для того, чтобы вырабатывать криптографический ключ или сильный пароль при поступлении на ее входы биометрического образа пользователя. Количество входов этой нейронной сети равно числу признаков, а количество выходов – длине личного ключа (пароля).

К сегодняшнему дню существует два основных подхода к построению ПБК: на основе нечеткого экстрактора и на основе нейронных сетей. Использование нечётких экстракторов даёт возможность восстанавливать секретный ключ из сырых или неточно воспроизводимых биометрических данных [3]. Данный метод не способен извлечь из одних биометрических данных более одного ключа и может быть подвержен некоторым классам атак [1, 4].

Одним из наиболее перспективных методов распознавания диктора являются глубокие нейронные сети [5]. Для практических целей существует необходимость в создании аппаратов

аутентификации пользователей на незамкнутом множестве. Любой человек должен иметь возможность обучить НПБК «под себя», чтобы система аутентификации могла отличить конкретного субъекта от любых других. К сожалению, при такой постановке задачи использовать глубокие сети оказывается затруднительно. Для устойчивого обучения многослойной нейронной сети требуется большой объем обучающей выборки и соблюдение баланса между количеством обучающих примеров «Свой» и «Чужие». Однако на практике пользователь не может повторить голосовой пароль тысячу раз (с разными интонациями). Объем обучающей выборки «Свой», как правило, ограничен 20-30 примерами. Кроме того, на базе глубоких сетей при двухклассовой идентификации («Свой»/«Чужие») невозможно построить НПБК, удовлетворяющий всем свойствам генерации длинных ключей и паролей.

НПБК имеют преимущество перед нечёткими экстракторами при определении биометрических характеристик в процессе обучения, так как нейронные сети приспособлены учитывать реальное распределение ошибок при анализе биометрических данных в то время как самокорректирующие коды способны работать в случае равновероятного распределения ошибок. В отличие от нечетких экстракторов, нейросетевой преобразователь может исправить более 50% ошибочных бит в полученном ключе доступа [1].

Как показывает практика, далеко не все голосовые характеристики информативны. В случае применения НПБК появляется необходимость в сильных признаках. Информативность признаков, получаемых при помощи традиционных подходов (спектральный анализ, быстрое оконное преобразование Фурье, мел-кепстральные коэффициенты, вейвлет-анализ) оказывается недостаточной для построения высоконадежного НПБК. Именно поэтому встаёт необходимость в разработке новой модели НПБК с использованием подхода с предобучением. Такую модель можно реализовать на базе так называемых автокодировщиков. В отличии от базовых архитектур глубоких сетей, направленных на решение задач идентификации образов, автокодировщик «учится» раскладывать звуковые сигналы на составляющие и восстанавливать их почти без потерь. В результате эти составляющие можно использовать непосредственно в качестве признаков, информативность которых может оказаться значительно выше амплитудно-частотных характеристик голосовых паролей.

Далее приведены краткие сопоставительные данные о надежности биометрической аутентификации на основе рукописных и голосовых образов:

- Метод, разработанный в ЦРТ (обобщённый метод моментов + SVM + совместный факторный анализ + вариационный байесовский анализ): EER=0,022 [6];
- Нечеткий экстрактор: EER=0,2 [7];
- Сверточные нейронные сети (с 3d-свертками): EER=0,211 [8];
- Сверточные нейронные сети: EER=0,03 [9];
- Сверточные нейронные сети: EER=0,105 [10].

Любой биометрический образ предварительно обрабатывается для устранения незначимой информации и повышения отношения сигнал/шум. Далее из образа извлекаются признаки – биометрические параметры, которые должны содержать информацию, пригодную для идентификации личности.

Для извлечения признаков будут апробированы различные типы автокодировщиков. Автокодировщик – это архитектура свёрточной нейронной сети, которая обучается эффективно сжимать поданный на вход сигнал в низкоразмерный код, а затем восстанавливает его в представление, максимально близкое к исходному.

Также для достижения целей исследования предлагается способ ансамблирования нескольких предварительно обученных сверточных нейронных сетей, которые обучаются на разных репрезентациях биометрических образов. Будет сформировано несколько автокодировщиков, каждый из которых ориентирован на извлечение признаков из репрезентаций, получаемых определенным способом. При аутентификации тайный биометрический образ преобразуется сразу в несколько репрезентаций, каждая из которых поступает на вход соответствующему кодировщику, который вычисляет вектор признаков. Далее векторы признаков объединяются и поступают на вход преобразователя «биометрия-код» (ПБК), который преобразует объединенный вектор в личный ключ или пароль пользователя.

В качестве результатов исследования планируется определить зависимость между голосовыми параметрами диктора и его психоэмоциональным состоянием, выявить изменчивость голоса посредством сравнения голосовых записей дикторов, находящихся в разных состояниях (нормальное, алкогольное опьянение, усталость, недомогание и т.д.), определить закономерности в изменении

точности распознавания субъекта, находящегося в приведённых состояниях и построить модель НПБК для обработки голосовых образов на основе квадратичных нейронов.

СПИСОК ЛИТЕРАТУРЫ

1. Волчихин В.И. Перспективы использования искусственных нейронных сетей с многоуровневыми квантователями в технологии биометриконейросетевой аутентификации / В. И. Волчихин, А. И. Иванов, В. А. Фунтиков, Е. А. Малыгина // Известия высших учебных заведений. Поволжский регион. Технические науки. 2013. № 4(28). С. 88–99.
2. ГОСТ Р 52633.5-2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа. М.: Стандартинформ, 2012. 20 с.
3. Иванов А. И. О многообразии метрик, позволяющих наблюдать реальные статистики распределения биометрических данных «нечетких экстракторов» при их защите наложением гаммы / А. И. Иванов, С. А., Сомкин, Д. Ю. Андреев, Е. А. Малыгина // Вестник УрФО. Безопасность в информационной сфере, № 2(12), 2014, С. 16-23.
4. Меркушев О.Ю. Защита биометрических подсистем управления доступом, реализующих схему нечеткого экстрактора / О.Ю. Меркушев, И.Г. Сидоркина // Вестник волжского университета им. В.Н. Татищева. - 2011. - №18. - С. 104-109.
5. Сулавко А.Е. Генерация криптографических ключей на основе голосовых сообщений / А.Е. Сулавко, А.В. Еременко, Р.В. Борисов // Прикладная информатика / НОУ ВПО «МФПУ «Синергия», Москва, 2016, №5, С. 76-89.
6. Матвеев Ю.Н. Технологии биометрической идентификации личности по голосу и другим модальностям // Вестник МГТУ им. Н.Э. Баумана. Сер. “Приборостроение”. 2012. № 3(3). — С. 46-61.
7. Monrose F. Cryptographic key generation from voice. / F. Monrose, M. K. Reiter, Q. Li, S. Wetzel //Proceedings of the 2001 IEEE Symposium on Security and Privacy. — 2001.
8. Torfi A. Text-independent speaker verification using 3d convolutional neural networks / A. Torfi, J. Dawson, N. M. Nasrabadi // IEEE In-ternational Conference on Multimedia and Expo (ICME). - 23-27 July 2018
9. Lukic Y. Speaker identification and clustering using convolutional neural networks / Y. Lukic, C. Vogt, O. D¨urr, T. Stadelmann // IEEE 26th In-ternational Workshop on Machine Learning for Signal Processing (MLSP). SALERNO, ITALY. - 13-16 September 2016
10. Salehghaffari H. Speaker Verification using Convolutional Neural Networks // arXiv:1803.05427v2 [eess.AS] 10 Aug 2018

Караулова О.А.
ФГБОУ ВО ПГУТИ, старший преподаватель каф. ИБ.
olya4369@yandex.ru

ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ДВУХКОМПОНЕНТНЫХ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ

Аннотация: В статье рассматривается вопрос актуальности стеганографии в системах реального времени, в частности систем VoIP. Приведен анализ количества публикаций в базе Scopus, по разным ключевым словам. На основе проведенного анализа по публикациям определена задача встраивания сообщения в покрывающий объект в реальном времени, решение которой достигается предложенной схемой двухкомпонентной стеганографической системы, в основе которой лежит принцип инвариантности. Определены перспективы исследования.

Ключевые слова: стеганография, принцип инвариантности, двухкомпонентная стеганографическая система, работа в реальном времени.

Развитие и повсеместное распространение проводных и беспроводных сетей передачи данных, а также интеграция цифровых процессов в доминирующее количество областей жизни общества привело к значительному росту преступлений в области информационных систем. Сохранение доверия населения к информационным системам обеспечивается интенсивным развитием систем информационной безопасности. На сегодняшний день круг вопросов, решаемых в рамках информационной безопасности охватывает не только административные и технические аспекты обеспечения безопасности передачи данных, но и ряд смежных научных областей, включающих сети передачи данных, кодирование информации, особенности физических сред и др. Основным средством защиты информации в сетях передачи данных, в соответствии с ГОСТ является криптографическое шифрование информации, предоставляющее гарантию на конфиденциальность передачи данных. Однако, в ряде случаев, криптография не способна гарантировать сохранность передачи данных. Это происходит в случае активного злоумышленника, когда он способен разрушить сообщение или канал передачи информации. К таким случаям можно отнести: разрушение управляющих сигналов беспилотных летательных аппаратов, секретная коммуникация, шпионаж и др. Также возможен запрет на использование криптографии на законодательном уровне. В каждом из этих случаев, эффективным решением защищённой передачи информации является стеганография.

Классической задачей стеганографии является скрытая передача сообщения, замаскированного под информацию, не представляющую интереса для третьей стороны. Передача скрытых сообщений существует уже достаточно давно, однако с развитием цифровых систем появилось направление цифровой стеганографии, получившее интенсивное развитие в конце XX и начале XXI столетия. На ранних этапах в рамках направления были проанализированы типовые цифровые контейнеры (изображения, текст, звук и др.) и определены области встраивания скрытого сообщения. На сегодняшний день стеганография начала преобразовываться в отдельное серьёзное научное направление, насчитывающее десятки методов маскировки информации и методы обнаружения встроенной информации. Особенно значимый толчок развитию направления дала фундаментальная работа [1], показавшая перспективы развития стеганографических методов, и предопределившая новые подходы к развитию стеганографии. На рис. 1 показан рост количества публикаций в год, проведённый по ключевому слову «steganography» в базе цитирования Scopus.

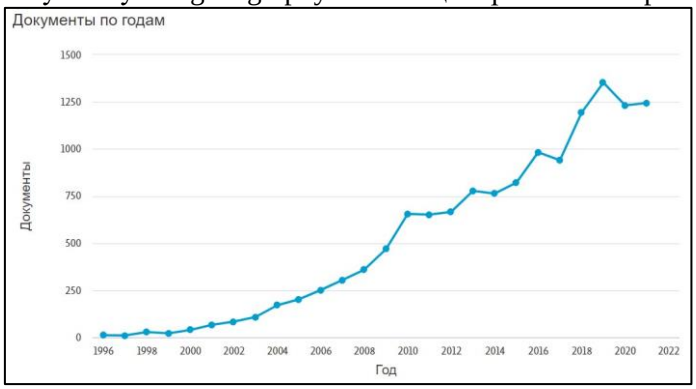


Рис. 1. Количество публикаций в базе Scopus по ключевому слову «steganography»

На основе методов данной работы был предложен метод HUGO (Highly Undetectdble steGO) [2] позволяющий реализовывать высоко необнаруживаемые стеганографические системы. Таким образом, произошёл качественный переход от «наивных» подходов к реализации стеганографических систем, к разработке высокоэффективных стеганографических систем на основе масштабных статистических и экспериментальных исследований.

Важно заметить, что стеганография в целом и стеганографические методы в частности жёстко привязаны к конкретным форматам контейнеров, в отличие от криптографии, диктующей условия к каналу передачи информации, исследования жёстко привязываются к форматам данных. То есть, появление каждого нового формата контейнера подразумевает исследование возможности скрытой передачи сообщения в рамках данного формата. В этом свете работа [1] спровоцировала не только бурное развитие направления, но и значительный перекос в исследованиях в область стационарных изображений, как наиболее распространённого формата передачи данных (формат jpeg). Это видно по рис. 2, где представлено количество публикаций в базе цитирования Scopus по ключевым словам «steganography» и «image» (изображение).

Однако, последние годы, в связи с пандемией и интенсивным внедрением средств интернет коммуникаций (Zoom, WhatsApp, Viber, Telegram и др.), а также развитием звуковых сообщений, представляется интересным вопрос развития стеганографии в реальном времени и, в частности систем VoIP. Таким образом, на сегодняшний день актуальными являются задачи встраивания информации в звуковые файлы и в звуковой сигнал, передаваемый в реальном времени. Не смотря на это именно направления стеганографии в звуке (рис. 3), стеганографии в реальном времени (рис. 4) и стеганографии в системах VoIP (рис. 5) представлены крайне малым количеством публикаций.

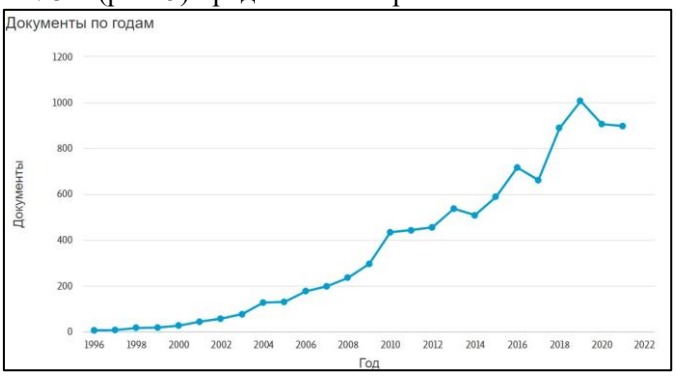


Рис. 2. Количество публикаций в базе Scopus по ключевым словам «steganography» и «image»

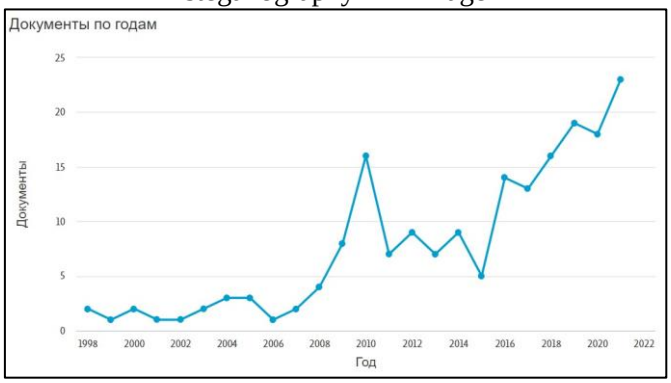


Рис. 3. Количество публикаций в базе Scopus по ключевым словам «steganography» и «sound»

Рассмотрение стеганографических алгоритмов в звуке, как правило, ограничивается использованием форматов без сжатия, представляющих звук в виде потока отсчётов, что позволяет сравнительно простую реализацию известных алгоритмов (например формат WAVE), использование же форматов сжимающих информацию с потерями сильно осложняет разработку алгоритмов в виду высоко сложности описания самих форматов, строящихся на достаточно обширном пласте исследований в области цифровой обработки сигналов и психоакустики (например формат MP3).

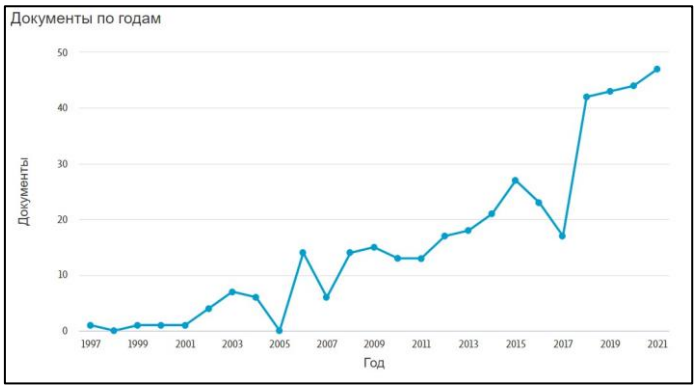


Рис. 4. Количество публикаций в базе Scopus по ключевым словам «steganography» и «real time»

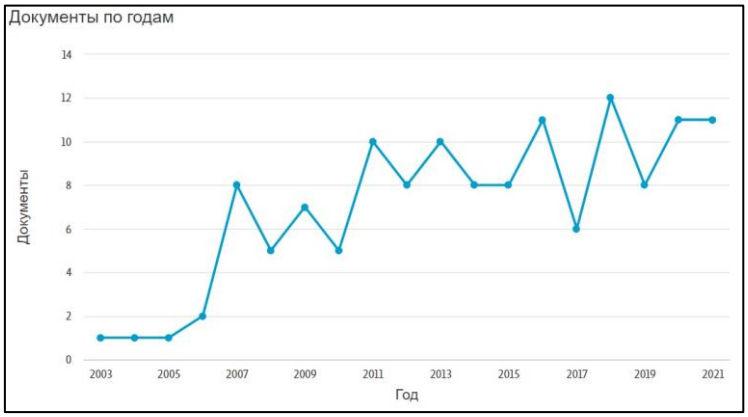


Рис. 5. Количество публикаций в базе Scopus по ключевым словам «steganography» и «VoIP»

В случае перехода на системы реального времени (VoIP), где используются кодеки SILK, OPUS и др., и обработка идёт блоками ограниченного объёма, а сами кодеки имеют сложную модель сжатия, реализация любого известного стеганографического метода представляет собой не только крайне сложную задачу моделирования и исследования, но и сталкивается со значительными ограничениями в применении, так как не представляется возможность анализа самого сигнала, за исключением короткого временного отрезка (OPUS codec – 26,5 миллисекунд по умолчанию).

Таким образом, задача развития стеганографии в системах реального времени является актуальной. В качестве решения задачи встраивания сообщения в передаваемую информацию (покрывающий объект) в реальном времени предлагается использовать инвариантную двухкомпонентную стеганографическую систему [3-6]. Общая структура двухкомпонентной стеганографической системы приведена на рис. 6, где n – номер отсчёта; u – отсчёты встраиваемого секретного сообщения; u_1 – отсчёты первого встраиваемого сигнала; u_2 – значения второго встраиваемого сигнала; ξ – отсчёты маскирующего сигнала; y_1 – отсчёты первой компоненты стеганографического контейнера; y_2 – отсчёты второй компоненты стеганографического контейнера.

Использование двухкомпонентной стеганографической системы обеспечивает работу в реальном времени [5,6], статистическую маскировку встроенного сообщения и обеспечивает защиту сообщения от извлечения даже в случае подозрения на наличие встроенной информации. Моделирование стеганографической двухкомпонентной стеганографической системы на языке Python для звуковых файлов без сжатия подтвердило эффективность предлагаемого метода.

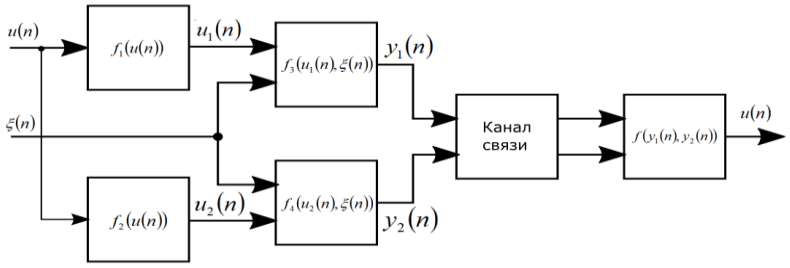


Рис. 6. Структурная схема двухкомпонентной стеганографической системы

Выводы: Проведённый обзор показал, что при значительных успехах стеганографии в изображениях, наиболее актуальные, на сегодняшний день, разделы стеганографии в звуке и в системах VoIP представлены ограниченным количеством публикаций. Более того, в виду сложности моделей сжатия звуковых сигналов, основанных на исследованиях цифровой обработки сигналов и психоаккустики, исследование стеганографии в этих областях являются комплексной задачей и требует тщательного моделирования. Тем не менее, построение простых моделей двухкомпонентной стеганографической системы для встраиваний сообщений в звуковые файлы без сжатия показало эффективность предлагаемого метода и его перспективность в виду адаптированности метода для работы в системах реального времени. Исследование двухкомпонентных стеганографических систем в системах реального времени, позволит реализовать высокоэффективные системы скрытой передачи информации в звуковых покрывающих объектах для последующей и передачи по проводным и беспроводным сетям.

СПИСОК ЛИТЕРАТУРЫ

1. Fridrich, J. Steganography in digital media. Principles, Algorithms and applications / J. Fridrich // Cambridge university press, New York, 2010. – P. 437.
2. Pevny, T. Using High-Dimensional Image Models to Perform Highly Undetectable Steganography /Tomas Pevny, Tomas Filler, Patrick Bas // Information Hiding, Jun 2010, Calgary, Canada. pp.2010.
3. Shakurskiy M.V., Two-channel real-time steganographic system /Shakurskiy, M.V., Shakurskiy, V.K., Volovach, V.I.//Proceedings of IEEE East-West Design and Test Symposium, EWDTS 2014, 2014, 7027074.
4. Шакурский, М.В. Алгоритм сокрытия использования двухкомпонентного контейнера в стеганографической системе / М.В. Шакурский// Научно-практический журнал «Вопросы защиты информации». – 2020. – №3. – С. 3-5.
5. Шакурский М.В. Двухкомпонентная стеганографическая система встраивания информации в младшие биты звукового сигнала / М.В. Шакурский // Журнал «Проблемы информационной безопасности. Компьютерные системы» №4 (48) 2021. Стр. 72-78.
6. Шакурский М.В. Двухкомпонентная стеганографическая система на основе отношения линейных функций двух сигналов, использующая аддитивный вид связи встраиваемых сигналов// Инфокоммуникационные технологии. 2020. №1 Т. 18. С. 56-61.
7. Shakurskiy, M.V. Computer model of steganographic system based on contraction mapping with stream audio container / M.V. Shakurskiy, V.K. Shakurskiy, V.I. Volovach // Proceedings of IEEE East-West Design & Test Symposium (EWDTS’2015) / KNURE, Kharkov 2015 p. 306-309.
8. Ker, A. Moving Steganography and Steganalysis from the Laboratory into the Real World / A. Ker, P. Bas, R. Bohme, R. Cogranne, S. Craver, T. Filler, J. Fridrich, T. Pevny/ ACM IH-MMSEC 2013.
9. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. - М.: Солон-Пресс. 2002.
10. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика/ Г.Ф. Конахович, А.Ю. Пузыренко // - К.: «МК-пресс», 2006 – 288 с.

Карташевская Е.С.
ФГБОУ ВО ПГУТИ,
старший преподаватель кафедры программной инженерии
ka_es@bk.ru

МЕТОД ОБНАРУЖЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ

Аннотация: Данная работа заключается в использовании копул для построения моделей машинного обучения для выявления угроз информационной безопасности в сетях Интернета вещей. Выявление угроз проводится на основе анализа сетевого трафика, для описания которого применяется теория массового обслуживания и теория телетрафика, где трафик представляется в виде некоторого случайного процесса. Многомерные распределения зависимых случайных величин, выраженные через копула-функции, в полной мере раскрывают структуру зависимости между случайными величинами, поэтому оправдано их использование для выявления аномалий.

Ключевые слова: информационная безопасность, Интернет вещей, многомерные вероятностные распределения, копулы, машинное обучение.

Целью работы является исследование существующих методов и моделей машинного обучения, используемых для обнаружения угроз в сетях IoT, а также разработка модели машинного обучения, основанной на применении многомерных распределений зависимых случайных величин, выраженных через копула-функции, для обнаружения угроз информационной безопасности в сетях IoT. Задачами исследования являются: классификация угроз информационной безопасности сетей и устройств IoT, анализ применимости различных моделей машинного обучения к обнаружениям угроз в сетях IoT, разработка математической модели машинного обучения и ее программная реализация, Работы, проводимые в исследовании, являются основной частью диссертационной работы.

Вопросам описания и классификации угроз информационной безопасности (ИБ) Интернета вещей (IoT), промышленного Интернета вещей (IIoT) посвящено достаточно большое количество обзоров [1-5], в которых представлены различные подходы к способам обнаружения различных атак на подобные сети. В качестве основных направлений перспективных исследований в области кибербезопасности Интернета вещей выделяются интеграция Интернета вещей с туманными / облачными средами (IoT – Fog/Cloud), передача данных в беспроводной среде, взаимодействие с промышленным Интернетом вещей и киберфизическими системами (IIoT / CPSs), работа с ошибками пользователей (ботнеты), управление внутренними физическими проблемами (извлечение данных на уровне датчиков) и т.д.[6]

Одним из современных подходов к построению систем защиты информации и обнаружения угроз является концепция XDR «расширенные обнаружение и реагирование» — класс систем информационной безопасности, предназначенных для автоматического проактивного выявления угроз на разных уровнях инфраструктуры, реагирования на них и противодействия сложным атакам [7]. Одна из особенностей XDR – предиктивный анализ, который в основном может осуществляться средствами машинного обучения (МО).

МО представляется многообещающим решением для обнаружения угроз и защиты устройств IoT от кибератак. Ряд публикаций описывает реальное применение данных методов, например, разработку системы контроля и обеспечения безопасности сбора данных, реализующая мониторинг сетевого трафика в реальном времени [8,9], разработку системы обнаружения аномалий на основе алгоритмов машинного обучения для безопасности «умного города»[10]; описание распределенной система обнаружения вторжений в системе сбора данных[11]; анализ сетевых аномалий для обнаружения утечек конфиденциальной информации в энергетической системе [12].

Также стоит отметить ряд публикаций, описывающих определенные типы угроз и варианты применения методов МО для защиты устройств IoT от кибератак. Одним из подходов предотвращения DoS-атак является использование многослойного персептрона (MLP). В [13,14] предлагается алгоритм оптимизации для обучения MLP, для выявления угроз и повышения безопасности беспроводных сенсорных сетей. Для обеспечения защиты от «подслушивания» могут использоваться методы МО, такие как обучение с подкреплением [15] или непараметрические байесовские методы [16,17]. Для создания моделей машинного обучения в основном использовались открытые дампы сетевого трафика, такие как CICIDS-2017, BOT-IOT и др.

Стоит отметить, что существует достаточно большое количество инструментов для тестирования безопасности устройств и сетей IoT, на основе которых могут быть проверены разработанные алгоритмы выявления угроз [18].

Также, в [19] авторы подробно описывают уязвимости в сфере IoT, и, что особенно важно, описывают практические способы «хакинга» устройств, моделируют угрозы и представляют эффективную методологию тестирования умных устройств.

На основе публикаций по тематике предполагается определить: какие именно модели машинного обучения (их ансамбли) могут быть использованы для обнаружения угроз в сетях IoT в режиме реального времени, а также критерии эффективности применения различных моделей МО для решения данных задач.

Обучение планируется проводить на основе открытых датасетов, таких как CICIDS-2017, BOT-IOT и др. Поскольку большинство из них является дампами сетевого трафика, необходимо будет выполнить их предварительную подготовку: удаление пропущенных данных, выделение признаков, понижение размерности и т.д.

Создание модели машинного обучения предполагается на основе копул. Поскольку копулы в полной мере раскрывают структуру зависимости между случайными величинами, их применение может быть весьма перспективным в анализе сетевого трафика для выявления аномалий. Программная реализация планируется с использованием данных, полученных на предыдущем этапе, с учетом результатов применимости моделей МО для различных типов угроз в сетях IoT. Также планируется проведение сравнительного анализа результатов выявления угроз при использовании существующих моделей и разработанной модели МО.

Научная новизна исследования заключается в использовании копул для построения моделей машинного обучения для выявления угроз информационной безопасности в сетях IoT. Выявления угроз проводится на основе анализа сетевого трафика, для описания которого применяется теория массового обслуживания и теория телетрафика, где трафик представляется в виде некоторого случайного процесса. Многомерные распределения зависимых случайных величин, выраженные через копула-функции, в полной мере раскрывают структуру зависимости между случайными величинами, поэтому оправдано их использование для выявления аномалий. Использование копул позволит существенно повысить скорость и точность вычислений для решения задач выявления угроз информационной безопасности.

В качестве результата планируется разработанная модель машинного обучения и ее программная реализация для выявления угроз информационной безопасности. Результаты могут быть использованы в качестве средства обеспечения обнаружения угроз в различных сетях IoT, в том числе промышленного Интернета вещей.

СПИСОК ЛИТЕРАТУРЫ

1. Андреев, Ю.С. Информационная безопасность автоматизированных систем управления технологическими процессами / Ю.С. Андреев, Д.С. Садырин, А.М. Дергачев, Ф.А. Жаров // Известия высших учебных заведений. Приборостроение. – 2019. – Т. 62. – № 4. – С. 331-339.
2. Наралиев, Н.А., Обзор и анализ стандартов и протоколов в области интернет вещей. Современные методы тестирования и проблемы информационной безопасности IoT / Н.А. Наралиев, Д.И. Самаль // International Journal of Open Information Technologies. – 2019. – Vol. 7. – № 8ю – pp. 94-104.
3. Hussain, F. Security Threats in M2M Networks: A Survey with Case Study / F. Hussain, L. Ferdouse, A. Anpalagan, L. Karim, I. Woungang // International Journal of Computer Systems Science and Engineering. – 2016. – 32.
4. Granjal, J. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues / J. Granjal, E. Monteiro, J. Sá Silva // IEEE Communications Surveys & Tutorials. – 2015. – Vol.17. – №3. – pp. 1294-1312.
5. Hassija, V. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures / V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar // IEEE Access. – 2019. – Vol. PP. – pp. 1 -24.
6. Довгаль, В.А. Анализ проблем обеспечения информационной безопасности беспроводных сенсорных сетей и методов обеспечения безопасности Интернета вещей / В.А Довгаль, Д.В. Довгаль // Вестник АГУ. – 2021. – №1 (276). – С. 75-83.
7. Васильев, В.И. Обеспечение информационной безопасности киберфизических объектов на основе прогнозирования и обнаружения аномалий их состояния / В.И. Васильев, А.М. Вульфин,

В.Е. Гвоздев, В.М. Картак, Е.А. Атарская // Системы управления, связи и безопасности. – 2021. – №6. – С. 90-119.
8. Ten, C.W. Anomaly detection for cybersecurity of the substations / C.W. Ten, J. Hong, C.C. Liu // IEEE Transactions on Smart Grid. – 2011. – Vol. 2. – № 4. – pp. 865-873.
9. Ten, C.W. Cybersecurity for critical infrastructures: Attack and defense modeling / C.W. Ten, G. Manimaran, C.C. Liu // IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans. – 2010. – Vol. 40. – № 4. – pp. 853-865.
10. Alrashdi, I. Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning / I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, H. Ming // 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). IEEE. 2019. P. 305-310.
11. Cruz, T. A cybersecurity detection framework for supervisory control and data acquisition systems / T. Cruz, L. Rosa, J. Proença, L. Maglaras, M. Aubigny, L. Lev, P. Simoes // IEEE Transactions on Industrial Informatics. – 2016. – Vol. 12. – № 6. – pp. 2236-2246.
12. Keshk, M. An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems / M. Keshk, E. Sitnikova, N. Moustafa, J. Hu, I. Khalil // IEEE Transactions on Sustainable Computing. – 2019. – Vol. 6. – № 1. – pp. 66-79.
13. Pavani, K. Intrusion detection using MLP for MANETs / K. Pavani, A. Damodaram // Proceedings of Third International Conference on Computational Intelligence and Information Technology (CIIT 2013). – 2013. – pp. 440–444.
14. Kulkarni, R.V. Neural network based secure media access control protocol for wireless sensor networks / R.V. Kulkarni, G. K. Venayagamoorthy // Proceedings of 2009 IEEE International Joint Conference on Neural Networks. – 2009. – pp. 1680–1687.
15. Xiao, L. A mobile offloading game against smart attacks / L. Xiao, C. Xie, T. Chen, H. Dai, H.V. Poor // IEEE Access. – 2016. – Vol. 4. – pp. 2281–2291.
16. Xiao, L. Proximity-based security techniques for mobile users in wireless networks / L. Xiao, Q. Yan, W. Lou, G. Chen, Y.T. Hou // IEEE Transactions on Information Forensics and Security. – 2013. – Vol. 8. – №. 12. – pp. 2089–2100.
17. Xiao, L. Phy-layer spoofing detection with reinforcement learning in wireless networks / L. Xiao, Y. Li, G. Han, G. Liu, W. Zhuang // IEEE Transactions on Vehicular Technology. – Vol. 65. – № 12. – pp. 10 037–10 047.
18. Эберт, К. Тестирование Безопасности / К. Эберт, Ю. Рекик, Р. Караде // Открытые системы. СУБД. – 2020. - № 2. – с. 22-26
19. Chantzis, F. Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things / F. Chantzis, I. Stais, P. Calderon, E. Deirmentzoglou, B. Woods. – 2021. – No Starch Press Inc. – 484p.

Кучкарова Н.В.
ФГБОУ ВО «Уфимский государственный авиационный технический университет»,
старший преподаватель,
nailya_kuchkarov@mail.ru

МЕТОД И АЛГОРИТМЫ ОЦЕНКИ УЯЗВИМОСТЕЙ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ТЕХНОЛОГИЙ СЕМАНТИЧЕСКОГО АНАЛИЗА ТЕКСТОВ

Аннотация: в работе проведен анализ современного состояния исследований в области использования алгоритмов интеллектуального анализа текстов для решения прикладных задач информационной безопасности (ИБ). Обозначены цели научного исследования, поставлены задачи решение которых направлено на разработку интеллектуальной системы поддержки принятия решений для автоматизации оценки и приоритезации актуальных угроз, уязвимостей, тактик (техник) и построения сценариев возможных атак.

Ключевые слова: уязвимости программного обеспечения, угрозы информационной безопасности, Text Mining, векторное представление текстов, модели трансформеры, семантическая близость.

Как показывает статистика последних лет, цифровизация различных отраслей экономики сопровождается ростом киберпреступлений. Так, по данным Лаборатории Касперского количество атакованных компьютеров АСУ увеличилось в 2021 г. по сравнению с 2020 г. на 2,8% [1]. Атакам подвергаются предприятия различных форм собственности и отраслей, чаще всего атакуются госсектор, энергетическая и промышленная отрасли, ВПК [2]. Предприятия упомянутых отраслей, как правило, относятся к объектам критической информационной инфраструктуры (КИИ). Большую группу объектов КИИ составляют промышленные автоматизированные системы управления технологическими процессами (АСУ ТП), требования к обеспечению информационной безопасности (ИБ) которых закреплены в ряде нормативно-правовых документов, принятых в России в последние годы, таких как: Федеральный закон «О безопасности критической информационной инфраструктуры» №187-ФЗ (2017г.), Приказы ФСТЭК России №№ 31, 235 и 239 (2017г.), «Методика оценки угроз безопасности информации» ФСТЭК России от 5 февраля 2021 г. Согласно последней Методике, одним из этапов оценки угроз безопасности информации (БИ) является оценка возможности реализации угроз БИ и определение их актуальности.

На практике при решении данной задачи специалисты по ИБ сталкиваются с необходимостью анализ угроз и уязвимостей в «ручном» режиме, что требует больших временных затрат и сопровождается ошибками обработки, обусловленными человеческим фактором, в связи с чем закономерно желание специалистов по ИБ автоматизировать процесс сопоставления угроз, уязвимостей, тактик и техник их эксплуатации. Одним из перспективных путей решения обозначенной проблемы является использование *методов и технологий интеллектуального анализа текстов (Text Mining)*.

Целью исследования является решение вопросов автоматизации оценки и приоритезации актуальных угроз, уязвимостей, тактик (техник) и построения сценариев возможных атак на основе технологий интеллектуального анализа и обработки слабоструктурированных данных на естественном языке в соответствии с требованиями Методики ФСТЭК.

Для достижения поставленной цели необходимо решить следующие *задачи:*

1. Провести анализ современного состояния применения технологий обработки данных на естественном языке (Natural Language Processing, NLP), методов и алгоритмов интеллектуального анализа (Text Mining) в задачах обеспечения ИБ АСУ ТП.
2. Разработать модели сопоставления угроз нарушения информационной безопасности и уязвимостей программного обеспечения систем управления АСУ ТП на основе семантического анализа их текстовых описаний в открытых базах данных.
3. Разработать алгоритмы и методики оценки и приоритизации актуальных угроз нарушения ИБ АСУ ТП на основе семантического анализа их текстовых описаний в открытых базах данных и связанных с ними уязвимостей ПО.
4. Разработать программное обеспечение систем автоматизации оценки и приоритезации актуальных угроз и уровня опасности уязвимостей согласно требованиям национальных и зарубежных стандартов.

5. Провести экспериментальное исследование с целью оценки эффективности разработанного программного обеспечения, реализующего предложенные алгоритмы и методику оценки уровня защищенности информационно-управляющих систем АСУ ТП.

Научная новизна предложенных решений:

1. Предложены алгоритмы предобработки и анализа текстовых описаний угроз БИ, уязвимостей ПО и тактик (техник) на основе технологий обработки слабоструктурированных данных, отличающиеся применением комплекса нейросетевых моделей-трансформеров для формализации текстовых представления в виде векторных вложений, применение которых позволяет выполнить семантический анализ указанных текстовых описаний в соответствии с требованиями Методики ФСТЭК России.

2. Разработаны метод и алгоритм автоматизированной оценки и приоритезации множества релевантных угроз БИ для выявленных уязвимостей ПО АСУ ТП с использованием технологии семантического анализа текстов, основанные на применении методов кластерного анализа, и отличающиеся использованием матриц оценок попарной семантической близости векторных вложений формализованных текстовых описаний, что позволяет упростить работу эксперта, сократив время на поиск и сопоставление уязвимостей и угроз;

3. Предложен алгоритм построения графовой модели сценария реализации угроз ИБ, основанный на алгоритмах построения графов атак и матриц доступности, отличающийся от существующих моделей формализацией текстовых описаний с помощью методов векторного вложения с последующей обработкой с помощью композиции нейросетевых автоэнкодеров с двусторонним вниманием, применение модели позволяет снизить трудоемкость и когнитивную нагрузку на специалистов по ИБ при формировании перечня актуальных угроз БИ и уязвимостей ПО.

4. Предложена архитектура и состав подсистем ПО ИСППР, применение которой позволяет снизить время и повысить достоверность принимаемых решений при оценке и анализе актуальных угроз БИ и уязвимостей ПО, что подтверждено результатами решения ряда практических прикладных задач.

Далее будут представлены решенные на момент написания статьи задачи.

В рамках решения задачи 1 проведен анализ современного состояния в области обеспечения ИБ АСУ ТП. Проанализированы требования современной нормативно-правовой базы в области ИБ АСУ ТП. Выполнен обзор научных публикаций в области автоматизации оценки, анализа и приоритезации угроз и уязвимостей с использованием методов интеллектуального анализа как зарубежных, так и отечественных ученых. Так, работы [3-7] посвящены выявлению уязвимостей и оценке степени их серьезности (критичности) на основе семантического анализа текстовых описаний уязвимостей. В статьях Селифанова В. В. и др. [8,9,10] предложена методика выявления взаимосвязей между обнаруженными уязвимостями и угрозами безопасности информации. Источником описаний угроз и уязвимостей является БДУ ФСТЭК России.

Дан краткий обзор открытых баз данных NDV, CVE, CAPEC, БДУ ФСТЭК России др., содержащих текстовые описания угроз ИБ, уязвимостей ПО, тактик (техник). Проведен сравнительный анализ алгоритмов для обработки текстовых описаний на естественном языке (ЕЯ): Word2Vec, Doc2Vec, TF-IDF, BERT (трансформеры).

Отмечено, что существующие методы и алгоритмы анализа и оценки угроз и уязвимостей не соответствуют в полной мере требованиям Методики ФСТЭК. Показана необходимость автоматизации процесса оценки и ранжирования (приоритезации) актуальных угроз БИ и уязвимостей ПО с использованием технологий интеллектуального анализа текстов (Text Mining), что позволит снизить трудоемкость работ связанных с определением актуальных угроз и уязвимостей.

В рамках решения задачи 2 разработан алгоритм построения векторного представления текстовых описаний угроз, уязвимостей, тактик (техник) и оценки их семантической близости.

Для оценки наличия устойчивой структуры текстовых описаний в пространстве признаков векторных вложений в виде устойчивых групп, образованных на основе оценки их семантической близости разработан алгоритм кластеризации текстовых описаний угроз, уязвимостей, тактик и техник.

Визуализация алгоритма кластеризации свидетельствует о наличии структуры компактных групп текстовых описаний и подтверждает возможность применения технологии Text Mining для структуризации текстовых описаний угроз и уязвимостей на основе оценки их семантической близости.

Предложены метод и алгоритм оценки и приоритизации множества релевантных угроз ИБ для выявленных уязвимостей ПО объекта АСУ ТП с использованием технологии Text Mining. Метод основан на установлении соответствия между множествами угроз, уязвимостей и тактик (техник),

формализованных с помощью модели построения векторного представления их текстовых описаний на основе анализа матрицы попарных расстояний (оценки их семантической близости).

Разработан алгоритм построения графа соответствия множеств угроз, уязвимостей, тактик и техник их эксплуатации (далее граф соответствия). На вход алгоритма подается корпус текстов, далее происходит выбор модели векторного представления корпуса текстов, предобработка и векторизация корпуса текстов. Далее, в несколько этапов, строится граф соответствия, т.е. происходит соотнесение множеств выявленных уязвимостей и слабостей ПО, затем уязвимостей – слабостей ПО с тактиками и техниками и, в заключении, тактики и техники соотносятся с угрозами на основе оценки семантической близости. На выходе алгоритма экспертами анализируется качество графовой модели.

Задача 3. Разработан алгоритм оценки и приоритизации множества угроз ИБ для выявленных уязвимостей ПО. В основе алгоритма лежит построение матриц оценок попарной семантической близости объектов двух множеств: M^{TT_Vu} тактик (техник) (TT) и уязвимостей (Vul), M^{TT_Th} тактик (техник) (TT) и угроз (Th).

Разработан алгоритм построения графовой модели фрагмента сценария реализации угроз с использованием Word2Vec, Doc2Vec и технологии трансформера.

Построение графовой модели начинается с подготовки текстовых описаний угроз, уязвимостей, тактик и техник. Затем, на основе ссылочных описаний устанавливаются связи между вершинами V_1, V_2, V_3 , V_4 несуществующие прореживаются. Далее строится матрица семантической близости описаний угроз, уязвимостей, тактик и техник, несуществующие связи прореживаются на основе порогового значения.

В заключении проводится оценка и приоритизация множества угроз и уязвимостей.

В рамках решения задачи 4. разработана структурно-функциональная схема исследовательского прототипа ИСППР, предназначенной для автоматизации процесса оценки актуальных угроз БИ.

Ключевым элементом системы является механизм сопоставления текстовых описаний уязвимостей, тактики (техник) и связанных с ними угроз БИ, что позволяет уточнить сценарий реализации угроз, и кроме того, осуществить приоритезацию указанных угроз с учетом дополнительной информации о наличии зависимостей между угрозами и уязвимостями ПО.

Получены результаты экспериментов, проведенных для АСУ ТП объекта нефтепереработки: сопоставления тактик (техник), наиболее близких угроз БИ и уязвимостей ПО, выявленных в ходе анализа ПО АСУ ТП с помощью сканеров безопасности или определенных экспертом.

Семантический анализ текстовых описаний уязвимостей, угроз, тактик (техник) с использованием предлагаемых решений позволяет решить проблему длительного отбора подходящих по текстовым описаниям угроз и уязвимостей, снизив таким образом, трудоемкость работы специалистов по ИБ и улучшив качество их работы.

Перспективы дальнейших исследований. В дальнейших исследованиях планируется изучить и провести научные эксперименты в области суммаризации текстов (извлечение из текста основной информации) с целью мониторинга контента, содержащегося в сети интернет на предмет наличия новых уязвимостей, угроз, тактик (техник), которые еще не были официально включены в официальные базы данных. Предполагается, что использование данного подхода позволит провести углубленную оценку актуальных угроз ИБ, а также позволит специалистам по ИБ принять своевременные меры по защите объектов АСУ ТП от угроз и уязвимостей нулевого дня.

Исследование выполнено при поддержке Гранта ИБ МТУСИ (Соглашение № 40469-18/2022-к).

СПИСОК ЛИТЕРАТУРЫ

1. Ландшафт угроз для систем промышленной автоматизации. Kaspersky ICS CERT. [Электронный ресурс]: — Режим доступа: https://ics-cert.kaspersky.ru/reports/2020/09/15/threat-landscape-for-industrial-automation-systems-h1-2020/#_Toc49436674 (дата обращения 01.08.2022).
2. Актуальные киберугрозы: итоги 2021 года. Positive Technologies. [Электронный ресурс]: — Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/ (дата обращения 01.08.2022).
3. Han, Z Learning to Predict Severity of Software Vulnerability Description / Z. Han, X. Li, Z. Xing, H. Liu, Z. Feng // Proceedings of the 2017 International Conference on Software Maintenance and Evolution (ICSME) — 2017. — P. 125-136.

4. Lee, Y.Toward Semantic Assessment of Vulnerability Severity: A Text Mining Approach / Y. Lee, S. Shin // Proceedings of ACM CIKM Workshop (EYRE ' 18) — 2018. [Электронный ресурс]. — Режим доступа: https://www.CEUR-WS.org/Vol1-2482/papers.pdf (дата обращения 01.08.2022).
5. Spanos, G. Assessment of Vulnerability Severity using Text Mining / G. Spanos, L. Angeis, D. Toloudis // Proceedings of the 21st Pan-Hellenic Conference. — 2017 — P. 1-6.
6. Tao, Wen A Novel Automatic Severity Vulnerability Assessment Framework / Wen Tao, Zhang Yuquing, Yang Gang. // Journal of Communications. — 2015. — Vol. 10. №5. — P. 320-329.
7. Доронин, А.К. Предсказательная модель машинного обучения для решения задачи классификации уязвимостей компьютерных систем / А.К. Доронин, В.А. Липницкий // Материалы Междунар. научн. конф. «Информационные технологии и системы» (ИТС 2018). — Минск: 2018. — С. 94-95.
8. Полетаева В.С. Информационно-аналитическая система прогнозирования угроз и уязвимостей информационной безопасности на основе анализа данных тематических интернет-ресурсов: автореферат на соискание ученой степени канд. техн. Наук. — Ульяновск: 2020. — 19 с.
9. Селифанов, В. В. Применение методов автоматизации при определении актуальных угроз безопасности информации в информационных система с применением банка данных угроз ФСТЭК России / В. В. Селифанов [и др.] // Интерэкспо Гео-Сибирь. — 2017. — Т. 8. — С.202-209.
10. Селифанов, В.В. Методика автоматизированного выявления взаимосвязей уязвимостей и угроз безопасности информации в информационных системах / В.В. Селифанов, Я.В. Юракова, И.Н. Картамов // Интерэкспо Гео-Сибирь. — 2018. — С. 271–276.

Лансере Н.Н.
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А.Бонч-Бруевича, ассистент кафедры защищенных систем связи
Управление ФСТЭК России по Северо-Западному федеральному округу, начальник отдела
nlansere@yandex.ru

МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ НА КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТАХ

Аннотация: В исследовании рассматриваются субъекты критической информационной инфраструктуры (КВО), использующие автоматизированные системы управления (АСУ) на критически важных объектах, которые функционируют в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. АСУ представляют собой комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и производственным оборудованием и производимыми ими процессами. Рассмотрена специфика АСУ ТП, в том числе потенциальный ущерб от непроизводительных потерь, заключающийся в уменьшении объема добываемой или производимой продукции в определенный отрезок времени.

Ключевые слова: автоматизированная система управления, критическая информационная инфраструктура, критически важные объекты, деструктивные воздействия, сетевые атаки, угрозы безопасности информации, информационная безопасность, базовая модель угроз.

Благодаря развитию общества и цифровых технологий, создаются новые антропогенные угрозы безопасности информации и увеличивается количество интерфейсов воздействия [1].

Постановление Правительства Российской Федерации [2] обязывает все субъекты критической информационной инфраструктуры, в отношении принадлежавших им на праве собственности, аренды или любых других законных основаниях (информационные системы (ИС), информационно-телекоммуникационные сети (ИТКС), автоматические системы управления (АСУ)), функционирующие в 12 основных направлениях деятельности, а также проводить категорирование объектов критической информационной инфраструктуры [3].

В исследовании будут рассматриваться субъекты критической информационной инфраструктуры, использующие АСУ на критически важных объектах (КВО), функционирующих в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. Серьезной угрозой для таких предприятий представляет собой возможность деструктивного воздействия на управление АСУ ТП КВО.

Количество сетевых атак на промышленные информационные системы продолжает возрастать, соответственно увеличивается заинтересованность предприятий в защите своей информационной инфраструктуры.

Важным фактором эффективной работы АСУ ТП КВО является ее состояние защищенности, которое будет оцениваться в устойчивом (бесперебойном) функционировании всех систем и сетей, в том числе при воздействии на неё таргетированных сетевых атак.

В области оборонно-промышленного комплекса защита АСУ ТП КВО особенно критична, здесь результатом успешно проведенной сетевой атаки может быть нанесение вреда не только в экономической сфере, но и в обеспечении обороны страны, безопасности государства и правопорядка.

Причины, по которым задачи по защите АСУ ТП КВО являются актуальными по мнению автора следующие:

− открытость и доступность универсальных технологий и протоколов, которые применяются в АСУ ТП;

− общая с АСУ ТП информационная инфраструктура предприятий;

− подавляющее большинство импортного оборудования и программного обеспечения, применяемого в АСУ ТП;

− совершенствование производственных процессов путем внедрения цифровых технологий и появление новых нормативных требований по защите АСУ ТП и обеспечению безопасности критической информационной инфраструктуры Российской Федерации.

В соответствии с темой диссертационной работы «Модели и методика оценки защищенности информации в автоматизированных системах управления производственными и технологическими

процессами на критически важных объектах (АСУ ТП КВО)» в рамках проводимого исследования проанализированы результаты мониторинга сведений о публикуемых критических уязвимостях программного обеспечения государственных информационных систем и объектов критической информационной инфраструктуры, а также связанных с ними сетевых атаках.

На основании сведений, полученных из общедоступных источников информации в период с 28 февраля 2022 г. по настоящее время оценено влияние целевых компьютерных атак на состояние защищенности критической информационной инфраструктуры Российской Федерации.

Проведенный анализ во взаимодействии с организациями, функционирующими в области разработки и внедрения средств защиты информации, и информации Национального координационного центра по компьютерным инцидентам [4], показал, что в указанный период:

повысилась интенсивность опроса внешних интерфейсов информационных систем и сетей;

основные компьютерные инциденты были вызваны использованием общедоступных инструментов, распространяемых в сети Интернет;

инциденты, повлекшие масштабные негативные последствия зачастую были реализованы за счет возможностей внутренних нарушителей или связаны со слабой парольной защитой.

При этом наблюдается существенное изменение критических инцидентов по сравнению с последним кварталом 2021 года. Ранее большинство инцидентов приходилось на сетевые атаки, в том числе рутинное сканирование внешних инрфейсов, а так же внедрение вредоносного программного обеспечения. Начиная с конца февраля 2022 года зафиксировано резкое увеличение сетевых атак на онлайн-ресурсы Российской федерации. Целью злоумышленников стала дестабилизация работы сайтов или компьютерные атаки, направленные на взламывание веб-сайтов для публикации страниц провокационного или дискредитирующего органы государственной власти содержания.

Цель научного исследования заключается в совершенствовании методов и средств технической защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах.

Задачами научного исследования являются:

анализ актуальных угроз безопасности информации, циркулирующей в АСУ ТП КВО;

совершенствование способов противодействия угрозам безопасности информации и обеспечения информационной безопасности АСУ ТП КВО;

разработка и совершенствование методов оценки эффективности системы технической защиты АСУ ТП КВО.

Исследования в области оценки рисков информационной безопасности отражены в работах С.А. Агеева [5], И.М. Ажмухамедова [6], И.В. Аникина [7], Е.К. Барановой [8], Т.И. Булдаковой [9], А.П. Глухова [10], А.А. Кононова [11] , А.Г. Кравец [12], Н.Г. Милославской [13].

Анализ отмеченных исследований показал, что при оценке рисков недостаточно учитывается специфика АСУ ТП КВО, к примеру, упускается наносимый потенциальный ущерб от непроизводительных потерь, заключающийся в уменьшении объема добываемой или производимой продукции в определенный отрезок времени, или увеличении общего времени выпуска продукции (простоя, ремонта, восстановления работоспособности АСУ ТП КВО).

В целях практического внедрения будут разработаны типовая формализованная модель инфраструктуры АСУ ТП КВО, с привязкой к базовой модели для конкретной отрасли субъектов критической информационной инфраструктуры, являющихся КВО. Данные модели будут учитывать реальные критические процессы организаций с учетом особенностей субъектов КИИ и включать критерии для проведения комплексной оценки защищенности АСУ ТП КВО.

Исследованиям в области анализа защищенности информационной инфраструктуры, а также применение различных методов выявления уязвимостей посвящены работы А.В. Барабанова [14], М.В. Буйневича [15,16], М.А. Еремеева [17], А.К. Новохрестова [18], В.В. Платонова [19]. Однако проблемы распознавания уязвимостей в современных АСУ ТП КВО остаются актуальными, из-за специфики коммуникации сетей АСУ ТП и информационной инфраструктурой предприятий.

Большой вклад в решение задач по обеспечению управления ИБ компьютерных, информационных и автоматизированных систем управления КИИ, в т.ч. АСУ ТП, внесли работы ученых: Д.П. Зегжда, П.Д. Зегжда, А.А. Кононов, И.В. Котенко, И.И. Лившиц, И.Б. Паращук, Д.С. Черешкин, В.Д. Чертовской. Актуальным остается совершенствование способов противодействия угрозам безопасности информации и обеспечения информационной безопасности АСУ ТП КВО

Начиная с 24 февраля 2022 г. по настоящее время в ходе рабочих поездок на предприятия оборонно-промышленного комплекса (ОПК) автором проведен контроль реализации мероприятий по повышению защищенности объектов информационной инфраструктуры Российской Федерации. В

ходе контроля проводится анализ информационной инфраструктуры нескольких десятков предприятий ОПК по результатам которого отмечаются разные подходы в организации функционирования информационной инфраструктуры, в том числе на уровне сетевого взаимодействия (физического и логического), а так же применяемых организационных и технических мер:

реализация меры по обеспечению контроля почтовых вложений разнится в зависимости от объема производства;

меры по защите веб-страниц предприятий также разнятся, некоторыми предприятиями страницы закрыты принудительно;

реализация временного ограничения сетевого доступа к объектам информационной инфраструктуры является актуальным проблемным вопросом, особенно в условиях организации удаленных рабочих мест в условиях пандемии.

В рамках исследования будут проведены:

анализ рисков нарушения безопасности информации и уязвимости процессов переработки информации, циркулирующей в АСУ ТП КВО (**определены и конкретизированы** применительно к особенностям деятельности АСУ ТП КВО типовые компьютерные инциденты и категории актуальных нарушителей);

разработка модели и способов противодействия угрозам нарушения безопасности информации в АСУ ТП КВО и оценки ее защищенности (**в отличие от известных методик** конкретизированы критерии оценки защищенности АСУ ТП КВО);

разработка методики оценки эффективности системы технической защиты информации АСУ ТП КВО (определить базовый набор мер по обеспечению безопасности АСУ ТП КВО и **повысить уровень их защищенности**).

Данные научные и научно-технические результаты должны способствовать противодействию киберугрозам и иным источникам опасности для общества, экономики и государства в соответствии с подпунктом Д пункта 20 Стратегии научно-технологического развития Российской Федерации.

В настоящий момент основные публикации по теме исследования:

Организация концептуальной модели критической информационной инфраструктуры / А. М. Гельфанд, Н. Н. Лансере, А. А. Ложкина, И. И. Фадеев // Методы и технические средства обеспечения безопасности информации. – 2020. – № 29. – С. 39-40. – EDN PYPOHZ;

Внедрение методологии быстрой оценки объектов критической инфраструктуры для учреждений образования // Управление образованием: теория и практика / Education Management Review Том 12 (2022). No2 / Volume 12 (2022). Issue 2. С. 10-16.

Таким образом, разработка Моделей и методики оценки защищенности информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах с целью выработки единых подходов их устойчивого функционирования в рамках научно-исследовательской работы соответствует пунктам 6-10, 13 паспорта специальности 05.13.19.

СПИСОК ЛИТЕРАТУРЫ

1 Азамов О. В. Информационная безопасность / Будылин К. Ю., Бунев Е. Г., Сакун С. А., Шакин Д. Н. // Наука XXI – 2009. – Том 9, № 3. – С. 35–44.

2 Постановление Правительства Российской Федерации от 08 февраля 2018 г. «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

3 Организация концептуальной модели критической информационной инфраструктуры / А. М. Гельфанд, Н. Н. Лансере, А. А. Ложкина, И. И. Фадеев // Методы и технические средства обеспечения безопасности информации. – 2020. – № 29. – С. 39-40. – EDN PYPOHZ.

4 Конференция АО "ОСК" 29 марта 2022 г., г. Санкт-Петербург [электронный ресурс]. – Режим доступа : https://fstec.ru/territorialnye-organy-szfo/severo-zapadnyj-federalnyj-okrug/deyatelnost-szfo/vzaimodejstvie-szfo/2364-konferentsiya-ao-osk-29-marta-2022-g-g-sankt-peterburg/

5 Агеев, С.А. Оценка рисков сетевой компьютерной безопасности на основе нечеткого логического вывода / С.А. Агеев, И.Б. Саенко // ИБРР-2017: X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России». – Санкт-Петербург: СПб.: СПОИСУ, 1-3 ноября, 2017. – Том 3. – С. 28–30.

6 Ажмухамедов, И.М. Анализ рисков информационной безопасности / И.М. Ажмухамедов, О.Н. Выборнова, О.М. Князева: Учебное пособие. – Астрахань: Федеральное государственное

бюджетное образовательное учреждение высшего профессионального образования «Астраханский государственный технический университет», 2015. – 104 с.
7 Аникин, И.В. Метод управления рисками информационной безопасности в корпоративных информационных сетях / И.В. Аникин // Инфокоммуникационные технологии. – 2015. – Том 13, № 2. – С. 215–221.
8 Баранова, Е.К. Методики анализа и оценки рисков информационной безопасности / Е.К. Баранова // Образовательные ресурсы и технологии. – 2015. – № 1(9). – С. 73–79.
9 Булдакова, Т.И. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечёткой модели / Т.И. Булдакова, Д.А. Миков // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. – 2013. – № 11. – С. 295–310.
10 Глухов, А.П. Оценка чувствительности ресурсов и рисков применения систем критических приложений к влияющим факторам / А.П. Глухов, Н.Н. Котяшев, А.В. Купцов // Стратегическая стабильность. – 2007. – № 1(38). – С. 39–44.
11 Черныш, К.В. Индикативная оценка рисков на критериальных моделях критически важных объектов и критических инфраструктур / К.В. Черныш, А.А. Кононов // XI Всероссийской конференции «Методологические проблемы управления макросистемами». – Апатиты: КНЦ РАН, 26 марта-3 апреля, 2016. – С. 86–89.
12 Козунова, С.С. Формализованное описание процедуры управления рисками информационной системы / С.С. Козунова, А.Г. Кравец // Вестник Астраханского государственного технического университета. Серия: управление, вычислительная техника и информатика. – 2018. – № 2. – С. 61–70.
13 Милославская, Н.Г. Управление рисками информационной безопасности / Н.Г. Милославская, М.Ю Сенаторов, А.И. Толстой: Учебное пособие для вузов. 2-е изд., испр. – М.: Горячая линия-Телеком, 2014. – 130 с.
14 Барабанов, А.В. Актуальные вопросы выявления уязвимостей и недекларированных возможностей в программном обеспечении / А.В. Барабанов, А.С. Марков, В.Л. Цирлов // Системы высокой доступности. – 2018. – Том 14, № 3. – С. 12–17.
15 Буйневич, М.В. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации / М.В. Буйневич, В.В. Покусов, К.Е. Израилов // Информатизация и связь. – 2021. – № 4. – С. 66–73.
16 Буйневич, М.В. Аналитическое моделирование работы программного кода с уязвимостями / М.В. Буйневич, К.Е. Израилов // Вопросы кибербезопасности. – 2020. – № 3(37). – С. 2–12.
17 Еремеев, М.А. Продукционное представление знаний для моделирования источников атак в сети / М.А. Еремеев, А.Г. Ломако, В.М. Моргунов, Н.В. Свергун // CDE'17: The 2017 Symposium on Cybersecurity of the Digital Economy. – Иннополис: Издательский Дом "Афина" (Санкт-Петербург), 19-20 сентября, 2017. – С. 167–180.
18 Новохрестов, А.К. Модель угроз безопасности автоматизированной системы коммерческого учета энергоресурсов / А.К. Новохрестов, Д.С. Никифоров, А.А. Конев, А.А. Шелупанов // Доклады ТУСУРа. – 2016. – Том 19, № 3. – С. 111–114.
19 Платонов, В.В. Методы выбора свойств для систем обнаружения сетевых атак / В.В. Платонов // Методы и технические средства обеспечения безопасности информации. – 2016. – № 25. – С. 24–25

Исмагилова А.С.
ФГБОУ ВО «Башкирский государственный университет», зав. кафедрой управления информационной безопасностью, д. ф. – м. н., профессор,
ismagilovaas@yandex.ru

Лушников Н.Д.
ФГБОУ ВО «Башкирский государственный университет», ассистент кафедры управления информационной безопасностью
luschnikovnikita@yandex.ru

ПРОГРАММНЫЙ КОМПЛЕКС МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ С ПРИМЕНЕНИЕМ ОБУЧАЮЩЕЙ НЕЙРОННОЙ СЕТИ.

Аннотация: На основе собранного датасета был разработан и предложен метод синтеза параметров математической модели сверточной нейронной сети. Представлена уникальная структура созданной математической модели многофакторной биометрической аутентификации с использованием обучающей нейронной сети, инициализации весов нейронной сети, сравнения Евклидова расстояния вещественных чисел массивов, сравнение частотного диапазона по 12 параметрам голоса. Сверточная нейронная сеть реализована совместно с обученной тренировочной моделью категориальной кросс-энтропии. Также изучены и применены геометрическая прогрессия, экспоненциальная функция для шифрования и дешифрования биометрических элементов базы данных. Результатом исследования является разработанная математическая модель, доступная для пользователя персонального компьютера любой операционной системы. Главными достоинствами программного обеспечения являются комплексная реализация всех программных модулей созданной математической модели, высокая точность обработки входных данных (99.4%). Синтез обучающей нейронной сети и сохраненного файла весов нейронной сети не позволит обмануть приложение при помощи фото или видео. Представленный программный продукт работает в режиме многопоточности.

Ключевые слова: биометрия, пользователь, нейронная сеть, математические методы, программное обеспечение.

В настоящее время наиболее актуальным вопросом является проблема защищенности устройства от несанкционированного доступа. Каждый из нас, используя персональное устройство, надеется на минимальные риски и угрозы извне. Любой пользователь имеет полное право быть защищенным в той информационной среде, которая его окружает. После изучения статистических данных в области кибербезопасности, включая актуальность угроз, типы нарушителей, частную модель угроз, меры по обеспечению безопасности, было принято решение создать программное обеспечение, которое позволит пользователю защитить его информационное пространство в полной мере [1].

По данным БКС Экспресс, мировой рынок кибербезопасности оценивается в 2021 г. на 187 млрд $, а к 2026 г. прогнозируется рост до 270 млрд $. За этот период рост индустрии составит 56%, расходы на кибербезопасность будут увеличиваться в среднем на 9,3% в год [3].

Финансовые затраты корпораций на безопасность информационных технологий и информационных ресурсов не всегда оправданы. Такие инвестиции не гарантируют абсолютную защиту от несанкционированного доступа. Для замены сложных и длинных паролей предлагается программный продукт, в котором при входе в систему не будет возможности подделать или украсть основные биометрические элементы [4].

Целью исследования является построение математической модели многофакторной аутентификации с применением нейронной сети, разработка алгоритма многофакторной аутентификации с использованием основных биометрических элементов.

Уникальность разработанной математической модели заключается в создании собственного математического алгоритма, в котором синтезированы все программные модули идентификации по фото, голосу, видеоидентификации, голосового помощника, обучающей нейронной сети, шифрования и дешифрования биометрических элементов. Данные программные модули функционируют комплексно, в режиме многопоточности. Дешифрование и шифрование биометрических элементов не позволит реализовать несанкционированный доступ на персональном устройстве пользователя. Количество обрабатываемых точек лица: 128 (больше, чем в аналогичных программных модулях). В области информационной безопасности представленная математическая модель впервые распознает голос по 12 характеристикам. Точность обработки биометрических данных: 99.4 % [2].

Программные модули фотоидентификации и аудиоидентификации реализованы с помощью Евклидова расстояния. В данном случае Евклидово расстояние вычисляется по исходным, а не по стандартизованным данным. В библиотеке dlib рекомендуется использовать граничное значение Евклидова расстояния между дескрипторами лиц, равное 0,6. Евклидово расстояние — геометрическое расстояние в многомерном пространстве, вычисляемое по следующей формуле (1.1) [5]:

$$p(x, y) = \| x - y \| = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + ... + (x_n - y_n)^2} = \sqrt{\sum_{k=1}^{n} (x_k - y_k)^2} \quad (1.1)$$

где $x = (x_1, x_2, ..., x_n), y = (y_1, y_2, ..., y_n)$ - значения в многомерном пространстве.

Для повышения уровня точности обработки данных при реализации программных модулей математической модели создана нейронная сеть для обучения и сохранения результата нейронной сети в виде файла весов (формат .h5).

После подготовки к обучению нейронной сети, создана ее модель с применением искусственного интеллекта.

Так как количество классов в папках базы данных более 2, компилирование модели обучающей нейронной сети реализуется с помощью категориальной кросс-энтропии по следующей формуле (1.2) [6]:

$$D(\hat{y}, y) = -\sum_{J} y_j \ln \hat{y}_j \quad (1.2)$$

С помощью утилиты HDFView есть возможность наиболее подробно изучить поведение нейронов после пройденных итераций обработки данных. Структура файла весов выглядит следующим образом (Рис. 1).

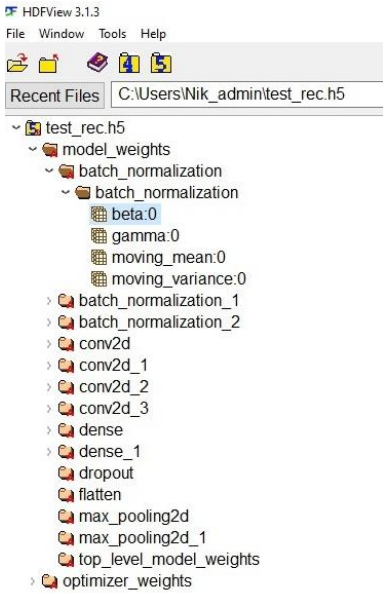


Рис. 1. Структура весов обучающей сверточной нейронной сети

Ранее использовались отдельные математические алгоритмы, которые на выходе показывали наименьшую точность распознавания образцов базы данных. Такая база данных обладает наименьшим количеством образцов [7].

В процессе создания программного обеспечения возникла потребность в разработке обученной нейронной сети и сохранении файла весов нейронной сети. В основе софта заложено обучение нейронной сети для автоматизации и реализации многопоточных процессов [8].

Недостатком математической модели является время обработки данных программного модуля распознавания пользователя по голосу. Это обусловлено качеством и корректностью работы программы во время представления голосового образца в виде массива вещественных чисел. Конфигурацию данного параметра пользователь может задавать самостоятельно [9].

Математическая модель реализована в комплексе и состоит из следующих компонентов:

— Разработка программного модуля идентификации по фото.
— Разработка программного модуля видеоидентификации.
— Разработка программного модуля идентификации по голосу.

— Создание голосового помощника.
— Создание обучающей нейронной сети.
— Разработка программного модуля шифрования и дешифрования биометрических элементов.
— Синтез всех программных модулей и представление математической модели многофакторной аутентификации.

Разработанная математическая модель реализована с использованием математических методов и собственного математического алгоритма (Рис. 2).

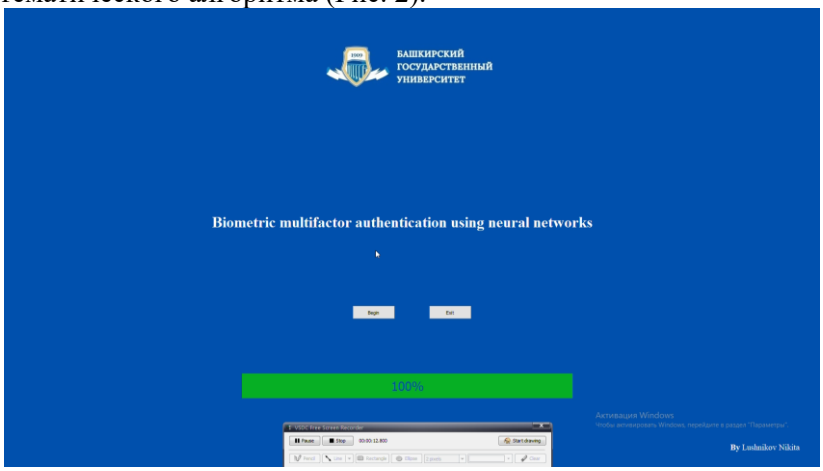


Рис. 2. Интерфейс программного комплекса многофакторной аутентификации

Предлагаемое программное решение предназначено для повышения уровня безопасности пользователей устройств [10]. Рассматриваемый софт является удобным помощником для пользователя любой системы. Представляемое программное решение является универсальным продуктом при наличии собственного устройства, использовании сайтов, образовательных модулей и СКУД [11]. Данный программный код в дальнейшем будет также интерпретирован в виде решения для мобильных приложений. Помимо этого, стоит отметить, что интегрированный в программный код голосовой помощник является хорошим гидом абсолютно для всех пользователей, включая людей с ограниченными возможностями (например, слабовидящих). В совокупности использование программного обеспечения и обученной нейронной сети позволяет автоматизировать процессы во многих областях применения [12].

СПИСОК ЛИТЕРАТУРЫ

1. Акилин Г.А., Грицкевич Е.В. Особенности имитационного моделирования информационных систем, использующих биометрическую идентификацию по лицу // Сборник статей по материалам международного научного конгресса «Интерэкспо Гео-Сибирь». — 2019. — С. 61-65.
2. Гринчук О.В., Цурков В.И. Обучение мультимодальной нейронной сети для определения подлинности изображений // Известия Российской академии наук. Теория и системы управления. — 2020. — № 4. — С. 103-109.
3. Девицына С.Н., Елецкая Т.А., Балабанова Т.Н., Гахова Н.Н. Разработка интеллектуальной системы биометрической идентификации пользователя // Научные ведомости. Серия: Экономика. Информатика. — 2019. — Т. 46. — №1. — С. 148-160.
4. Исмагилова А.С. Многофункциональное ПО для защиты учетных записей пользователей с использованием биометрических технологий / А. С. Исмагилова, Н. Д. Лушников // Защита информации. Инсайд. — 2021. — № 2 (98). — С. 28-31.
5. Караваев Д.А. Вейвлет-подобная архитектура комплекснозначной сверточной нейронной сети для синтеза комплексных сигналов // Вестник кибернетики. — 2020. — № 2. — С. 20-31.
6. Крылова И.Ю., Рудакова О.С. Биометрические технологии как механизм обеспечения информационной безопасности в цифровой экономике // Молодой ученый. — 2018. — № 45 (231). — С. 74-79.
7. Лушников Н.Д., Лебедев А.А. Внедрение биометрических технологий для защиты информационных ресурсов // Наука и бизнес: пути развития. — 2020. — № 6 (108). — С. 124-126.

8. Лушников Н.Д., Редников Д.В. Искусственный интеллект как вектор развития информационных технологий в будущем // Наука и бизнес: пути развития. — 2019. — № 1 (91). — С. 84-86.
9. Осовский С. Нейронные сети для обработки информации: учебное пособие / С. Осовский. М., Телеком. — 2017. — 448 с.
10. Пчеловодова Н. Российский биометрический рынок в 2019-2022 годах. Результаты масштабного исследования J’son \& Partners Consulting // Системы безопасности. — 2019. — №2. — С. 88-91.
11. Четырбок П.В., Шостак М.А. Обучение модульной нейронной сети для многозадачного искусственного интеллекта // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. — 2021. — № 4. — С. 70-74.
12. Чупакова А.О., Гудин С.В. Разработка и обучение модели искусственной нейронной сети для создания систем поддержки принятия решений // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. — 2020. — № 3. — С. 61-73.

Маслова М.А.
ФГАОУВО СевГУ, старший преподаватель
кафедры «Информационная безопасность»,
ФГАОУВО Ростовский государственный
экономический университет (РИНХ), МНС
MAMaslova@sevsu.ru

Разработка метода и инструментария анализа рисков нарушения информационной безопасности

Аннотация: Анализ рисков информационной безопасности имеет большое значение, так как неотъемлемой частью этого процесса является оценка рисков информационной безопасности, которую необходимо периодически проводить в целях эффективного внедрения мероприятий по управлению информационной безопасностью, идентификации новых угроз и уязвимостей, постоянного изменения в требованиях и приоритетах деятельности организации. Все эти этапы необходимы для обеспечения высокого уровня эффективности функционирования комплексной системы защиты информации. Исходя из анализа последних исследований и публикаций, по существующим методам в области анализа рисков нарушения информационной безопасности можно сделать вывод, что все они сводятся к стандартным методам оценки рисков с помощью качественного, количественного или комбинированного методов. Существуют так же перспективные интеллектуальные методы для анализа больших объемов данных, которые пока применятся в недостаточной мере. Научное исследование, заявляемое в рамках Гранта, будет направленно на развитие существующих и разработке новой методики и инструментария анализа и оценки рисков нарушения информационной безопасности основанных, в том числе, на интеллектуальных методах анализа данных.

Ключевые слова: информационная безопасность, интеллектуальные методы, оценка рисков, анализ рисков, методики анализа и оценки рисков, недостатки существующих методик, интеллектуальный анализ данных, угрозы.

Разрабатываемый метод анализа и оценки рисков информационной безопасности будет основываться на рассмотрении и анализе существующих методик оценки и анализа рисков информационной безопасности, выделении положительных и отрицательных сторон методик и сходящихся, и расходящихся DataSet с последующей их оценкой, произведен расчет параметров методом Дельфи и составлены рекомендации к действию по устранению рисков информационной безопасности.

Цель исследования — анализ существующих и разработка новой методики и инструментария анализа, и оценки рисков информационной безопасности на основе интеллектуальных методов анализа данных.

Задачи исследования:

1) Анализ существующих методов оценки и анализа рисков информационной безопасности;
2) Разработка функциональной модели анализа рисков информационной безопасности с учетом недостатков существующих методов;
3) Разработка программного модуля, реализующего функциональную модель анализа и оценку рисков информационной безопасности;
4) Экспериментальные тестовые исследования разработанного программного модуля с целью определения параметров его функционирования и сравнение с другими системами.

Анализ современного состояния исследований в данной области. Значительный вклад в изучении понятия и сущности «риск» внесли такие зарубежные и отечественные ученые, как: Блез Паскаль и Пьер де Ферма, Бернстайн П.Л., Герц Р.Ч., Дипиаза С.А., Луман Н., Найт Ф.Х., Л.Дж. Хоффман, Пигу А., Хьюса С., Эрроу К., Алексеенко В.Б., Аливанова С.В., Ануфриев С.И., Балдин К.В., Воробьев С.В., Гунько Ю.А., Кутлыева Г.М., Куренная В.В., Кусакина О.Н., Мочалова Ю.И., Рыбасова Ю.В., Чередниченко О.А., Хабибулин М.С. Г.С. Вечканов, И.А. Бланк, Г. Марковиц, Гончаренко, С.Э. Саркисов, В.М. Вяткин и т.д.

Современными проблемами риск-менеджмента посвящены работы: В.В. Асаул, А.О. Михайлова, П. Берстайна, И.Т. Балабанова, А.А. Иванова, С.Я. Олейникова, С.А. Бочарова, В.В. Шахова, А.С. Миллермана, В.Г.Медведева, А.Л. Лельчука, Д.В. Шамина и т.д.

Особенности управления рисками инновационной деятельности и инновационными проектами занимаются такие ученые-экономисты, как: Е.Е. Куликова, А.Т. Коржаев, В.Л. Попова, Е.С.

Симоненко, С.В. Валдайцева, С.А. Самоволева, Р. Таплина, А. А. Белозёрова, С. Ю. Микова, М.А. Нестеренко, С.А. Агеев, Т.И. Булдакова, Д.А. Миков, А. Андрейчиков, К. Маслова, С.Лелянова, М. Гончаров, В.Ф. Шаньгин, А.В. Соколов, И.В. Сибикина и др.

Методам интеллектуального анализа данных для оценки рисков посвящены работы: Н.А. Маслова, В.М. Лотох, С.М. Ващенко, В.А. Дюк, А.П. Самойленко, С.В. Бегутова, В.В. Корнеев, С. Лелянова, К. Маслова, А. Андрейчиков, Т.И. Буклдакова, Д.М. Фатхи.

Предлагаемые методы и подходы к решению поставленных задач.

Существует множество методов анализа и оценки рисков информационной безопасности - они различны и практически не реализуют общие формализованные подходы, что значительно затрудняет их выбор и использование. При этом существующие факторы риска, такие как угрозы, ущерб и уязвимость, анализируют в основном с помощью эвристических методов, включающих в себя экспертный анализ. Поэтому решение данной проблемы видится в разработке нового строго формализованного метода, основанного на интеллектуальном анализе данных и генерирующего, в том числе, количественные оценочные значения.

Научная новизна работы заключается в разработке нового метода и инструментария анализа и оценки рисков информационной безопасности с учетом всех отрицательных сторон существующих подходов, на основе алгоритмов интеллектуального анализа данных.

Ожидаемые по окончании проекта научные результаты:

1) Данные исследования существующих методов анализа и оценки рисков информационной безопасности;
2) Функциональная модель анализа рисков информационной безопасности с учетом недостатков существующих методов;
3) Программный модуль, реализующий функциональную модель анализа и оценку рисков информационной безопасности;
4) Результаты экспериментальных тестовых исследований разработанного программного модуля с целью определения параметров его функционирования и сравнение с другими системами.

СПИСОК ЛИТЕРАТУРЫ

1. Агеев С.А. Методы интеллектуального анализа данных для управления рисками информационной безопасности в защищенных мультисервисных сетях специального назначения / С.А. Агеев // Информационные системы. Автоматизация процессов управления — 2015. — № 2 (40). — С. 42-49.
2. Асаул В.В. Обеспечение информационной безопасности в условиях формирования цифровой экономики / В.В. Асаул, А.О. Михайлова // Теория и практика сервиса: экономика, социальная сфера, технологии. — 2018. — № 4 (38). — С 5-9.
3. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности/ Е.К. Баранова // Новые технологии. — 2015 — №1(9) — С. 73-79.
4. Белозёрова А. А. Оценка риска информационной безопасности при использовании ERP-систем / А.А. Белозёрова, С.Ю. Микова, М.А. Нестеренко // Молодой ученый. — 2016. — №15. — С. 152-155.
5. Кузнецов А.А. Управление рисками информационной безопасности на примере современных методик / А.А. Кузнецов, М.А. Маслова // Городская научно–практическая конференция с международным участием «Молодежная инициатива – 2019». Сборник материалов конференции Ростов н /Д. — С.189-190.
6. Реализация ESG- принципов в стратегии устойчивого развития экономики России // Издательско-полиграфический комплекс РГЭУ (РИНХ). — Ростов н /Д. — 2022. — С.484-491.
7. Фатхи Д.М. Применение методов интеллектуального анализа данных для тестирования баз данных систем информационной безопасности / Д.М. Фатхи // Информационная безопасность регионов. — 2014. — № 1 (14). — С 48-50.
8. Средство оценки безопасности Microsoft Security Assessment Tool (MSAT): понимание рисков, процесс MSAT, загрузка и установка | Microsoft Docs [Электронный ресурс] : — Режим доступа: https://www.microsoft.com/ru–ru/download/details.aspx?id=12273.
9. Обзор методик и анализ рисков информационной безопасности, информационных систем предприятия [Электронный ресурс] : — Режим доступа: https://cyberleninka.ru/article/v/obzor–metodik–analiza–riskov–informatsionnoy–bezopasnosti–informatsionnoy–sistemy–predpriyatiya.
10. Microsoft Security Assessment Tool 4.0 [Электронный ресурс] . — Режим доступа: anti–malware.ru.

Палютина Г.Н.
Институт развития технологий цифровой экономики
РГЭУ (РИНХ), младший научный сотрудник,
hello616@yandex.ru

РАЗРАБОТКА АЛГОРИТМОВ АДАПТИВНОЙ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ТЕХНОЛОГИИ КОГНИТИВНОГО МОДЕЛИРОВАНИЯ

Аннотация: Тема автоматизации оценки информационных рисков поднимается многими исследователями, но при этом она все еще содержит в себе различные противоречия. В том числе эти противоречия связаны с адаптивной оценкой рисков информационной безопасности, с формированием и выбором из большого множества факторов именно тех, которые влияют на оценку рисков. В связи с этим подтверждается актуальность и востребованность темы научной работы.

Основная идея научного исследования заключается в создании алгоритма адаптивной оценки рисков информационной безопасности на основе технологии когнитивного моделирования: нейронная сеть, основываясь на базе знаний, заложенной в ее обучение, будет выбирать те факторы, которые оказывают прямое воздействие на риски информационной безопасности, адаптируясь под конкретные условия работы информационной системы.

Научная новизна исследования заключается в совершенствовании методов и алгоритмов адаптивной оценки рисков информационной безопасности, учитывающих возможность построения ансамблей нечетких когнитивных карт на основе нескольких вариантов формализации знаний и опыта эксперта.

Результат научного исследования – алгоритм адаптивной оценки рисков информационной безопасности на основе технологии когнитивного моделирования. Данный алгоритм может быть применен в рамках создания системы защиты информации компаниями различного направления, а также в рамках обучения студентов направления «Информационная безопасность» с целью формирования у них практических навыков управления рисками информационной безопасности.

Ключевые слова: управление информационной безопасностью, адаптивная оценка рисков, модели и методы адаптивной оценки, нечеткие когнитивные карты, ансамбли нечетких когнитивных карт.

Целью проекта «Разработка алгоритмов адаптивной оценки рисков информационной безопасности на основе технологии когнитивного моделирования» является повышение эффективности управления рисками информационной безопасности путем разработки моделей, методик и алгоритмов адаптивной оценки рисков на основе когнитивного моделирования с использованием нечетких когнитивных карт (НКК) [1], [2].

Тематика научного проекта коррелирует с тематикой диссертационного исследования «Методы и алгоритмы адаптивной оценки рисков информационной безопасности», результаты данного научного проекта будут отражены в диссертационной работе.

Для достижения цели, поставленной в рамках данной научной работы, необходимо решить следующие задачи:

1. Анализ современных методов оценки рисков информационной безопасности, в том числе адаптивной оценки рисков.
2. Анализ особенностей применения технологии когнитивного моделирования, в частности НКК, для оценки информационных рисков.
3. Анализ принципов построения математических моделей проблемных ситуаций и исследование математических методов анализа задач принятия решений на основе нечеткой логики.
4. Предложение алгоритмического метода, применимого для оценки рисков информационной безопасности на основе когнитивного моделирования с использованием когнитивных карт.
5. Теоретическое обоснование эффективности применения результатов исследований.
6. Апробация и внедрение результатов в практику работы организаций различного профиля.

Вопрос автоматизации оценки рисков информационной безопасности [3] поднимается различными исследователями и организациями [4], [5]. В методике оценки угроз ФСТЭК [6] отмечается необходимость организациями реализовывать не дискретный процесс моделирования угроз, а непрерывный с возможностью автоматической загрузки новых данных об угрозах с сайта регулятора. Также в документе отражены изменения в области оценки рисков.

Все это говорит о том, что тема автоматизации оценки информационных рисков не является до конца разрешенной и все еще содержит в себе различные противоречия. В связи с чем подтверждается ее актуальность и востребованность исследования.

На сегодняшний день создан ряд стандартов и подходов к управлению рисками. Наибольшую востребованность на практике приобрели следующие международные спецификации и стандарты: ISO 17799-2002 (BS 7799), ISO/IEC 27002, GAO и FISCAM, SCIP, COBIT, NIST 800-30, SAC, COSO, SAS 55/78 и некоторые другие аналогичные им. В России разработан свой стандарт СТО БР ИББС-1.0-2004.

Анализ существующих методик (Octave, Fair, NIST RMF, CRAMM, COBIT for Risk) позволил сформировать относительно единый процесс управления рисками информационной безопасности и выявить этапы, на которых уместна автоматизация, а также острые вопросы, которые требуют проработки. Эти этапы: определение риск-аппетита; идентификация риска, анализ риска, оценка риска; ранжирование риска; разработка плана реагирования на риски; принятие решения по рискам; реализация мероприятий по реагированию на риски; оценка эффективности реализованных мер.

На этапе 2 входящие данные, необходимые для оценки рисков (модель злоумышленника, информация о бизнес-процессах и т.д.) не определены четко и могут варьироваться. Основываясь на экспертном подходе, нельзя исключить возможность того, что какие-то весомые факторы не будут учтены. В связи с этим возникает вопрос корректного выбора этих факторов.

Одним из способов решения данного вопроса является применение когнитивного моделирования. Так, в [7-9] рассматривается применение технологии когнитивного моделирования, в частности нечетких когнитивных карт для оценки информационных рисков. Но исследования [10-11] показывают, что данный метод также имеет свои трудности в реализации. Наибольшая точность работы карт достигается при наиболее сложных методах ее создания, что, однако не решает проблему верификации и последующей корректировки когнитивной карты. Наличие большого количества входных данных выявляют сложности при построении когнитивной карты. Поэтому этот метод требует более углубленного исследования, в частности в области оптимизации входных данных когнитивной карты.

Среди участников отечественного рынка, которые предоставляют решения в управления информационной безопасностью и в том числе в области оценки рисков (Positive Technologies, Max Patrol), пополнение базы входными данными происходит из следующих источников:

1) Сканирование методами DAST, SAST.
2) Импорт данных из внешних каталогов (Active Directory, SCCM, гипервизоры).
3) Импорт данных из SIEM- и NTA-систем по результатам анализа событий и трафика.

Каждый из этих методов наряду с преимуществами имеет определенные недостатки, среди которых можно выделить: относительную сложность реализации, невысокую скорость проверки, снижение эффективности при усложнении программного обеспечения; сложность построения SIEM-систем, связанная с необходимостью сбора и анализа событий от различных неоднородных агентов.

Таким образом, в процессе анализа современного состояния исследований в области оценки рисков информационной безопасности были обнаружены неопределенности в подходе к выбору факторов оценки рисков, их источников. Одним из подходов является подход, основанный на технологиях нечеткого моделирования, основной трудностью которого является процесс построения когнитивных карт с большим объемом входных данных.

Проводимые исследования будут способствовать совершенствованию методов и алгоритмов адаптивной оценки рисков информационной безопасности. Научная новизна исследования заключается в изучении возможности построения ансамблей нечетких когнитивных карт на основе нескольких вариантов формализации знаний и опыта эксперта.

Результатом научного исследования являются полученные в ходе исследования теоретические данные и алгоритм адаптивной оценки рисков информационной безопасности.

Данный алгоритм может быть применен в рамках создания системы защиты информации компаниями различного направления, а также в рамках обучения студентов по направлению «Информационная безопасность» с целью формирования у них навыков управления рисками информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Chen-Tung Chen. Study of dynamic fuzzy cognitive map model with group consensus based on linguistic variables / Chen-Tung Chen Yen-Ting Chiu // Technological Forecasting and Social Change. —2021. — № 171. [Электронный ресурс]. — Режим доступа: https://www.sciencedirect.com/science/article/pii/S0040162521003802

2. Tahani Albalawi. Security Mental Model: Cognitive Map Approach / Tahani Albalawi. Kambiz Ghazinour, Austin Melton // International Conference on Computational Science and Computational Intelligence (CSCI) — 2017. [Электронный ресурс]. — Режим доступа: https://www.researchgate.net/publication/329473497_Security_Mental_Model_Cognitive_Map_Approach
3. Топ-10 проектов Gartner в области безопасности на 2020-2021 годы. [Электронный ресурс]. — Режим доступа: https://www.gartner.com/smarterwithgartner/gartner-top-security-projects-for-2020-2021/
4. Исследовательская и консультативная компания Gartner, Inc [Электронный ресурс]. — Режим доступа: https://www.gartner.com/en
5. Какаев, Д. В. Автоматизация расчетов рисков информационной безопасности методом экспертных оценок на Python / Д.В. Какаев, М.А Маслова // Научный результат. Информационные технологии. — 2019. — № 4. [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/avtomatizatsiya-raschetov-riskov-informatsionnoy-bezopasnosti-metodom-ekspertnyh-otsenok-na-python
6. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г. [Электронный ресурс]. — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g
7. Васильев, В. И. Автоматизация процесса оценки информационных рисков с использованием нечетких когнитивных карт / В.И. Васильев, Р.Т. Кудрявцева, В.А. Юдинцев // Вестник Уфимского государственного авиационного технического университета. — 2014. — № 3. [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/avtomatizatsiya-protsessa-otsenki-informatsionnyh-riskov-s-ispolzovaniem-nechetkih-kognitivnyh-kart
8. Васильев, В. И. Анализ и управление рисками информационной безопасности с использованием технологии когнитивного моделирования / В.И. Васильев, А.М. Вульфин, Р.Т. Кудрявцева // Доклады Томского государственного университета систем управления и радиоэлектроники. — 2017. — № 4. [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/analiz-i-upravlenie-riskami-informatsionnoy-bezopasnosti-s-ispolzovaniem-tehnologii-kognitivnogo-modelirovaniya
9. Васильев, В. И. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт // В.И. Васильев, А.М Вульфин, И.Б. Герасимова, В.М. Картак // Вопросы кибербезопасности. — 2020. — № 2. [Электронный ресурс]. — Режим доступа: https://cyberrus.com/wp-content/uploads/2020/06/11-21-236-20_2.-Vasilyev.pdf
10. Гамазов, И. Н. Анализ задач, возникающих при создании нечетких когнитивных карт / И.Г. Гамазов, В.И. Терехов // Проблемы науки. — 2016. — № 6. [Электронный ресурс]. — Режим доступа: https://scienceproblems.ru/images/PDF/2016/6/analiz-zadach-voznikajushchih-pri-sozdanii.pdf
11. Жилов, Р.А. Оптимизация когнитивной карты для задач прогнозирования // Кибернетика и программирование. – 2015. – № 5. – С. 128 - 135. [Электронный ресурс]. — Режим доступа: https://nbpublish.com/library_read_article.php?id=16592

Поликанин А.Н.
г. Новосибирск, СГУГиТ,
кафедра информационной безопасности,
старший преподаватель
polikanin.an@yandex.ru

МЕТОДИКА ПРОТИВОДЕЙСТВИЯ ОПТИЧЕСКОМУ КАНАЛУ УТЕЧКИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ МИНИ-БПЛА

Аннотация: применение мини-БПЛА в качестве платформы базирования средств разведки и технических средств каналов утечки информации открывает новые возможности злоумышленникам в преодолении существующих традиционных рубежей охраны и контроля доступа и попаданию внутрь контролируемых зон с целью организации технических каналов утечки, в частности в оптическом диапазоне.

Ключевые слова: мини-БПЛА, тепловизор, квадрокоптер, дальность обнаружения, распознавания, идентификации.

Цель работы: совершенствование защиты информации от утечки по оптическому каналу при использовании злоумышленниками квадрокоптеров, оснащенных средствами оптической разведки.

Объект исследования: оптический канал утечки информации

Предмет исследования: средства оптической и тепловизионной разведки с использованием малых беспилотных летательных аппаратов, методика противодействия организации канала утечки, использующего подобные средства разведки.

Актуальность: ноябрь 2021 года Сочи состоялось совещание Президента РФ и представителей Минобороны по вопросам эффективности использования БПЛА в качестве средств разведки в военной сфере. В той же мере тема является актуальной и для гражданской сферы.

В ходе работы определены 5 основных положений на защиту.

Положение 1.

Применение мини-БПЛА, как носителя средств оптического канала утечки информации создаёт возможность частичного игнорирования контролируемых зон защиты объектов и носителей информации и представляет чрезвычайную угрозу конфиденциальности визуальной информации

Соответствует области исследований в специальности 2.3.6.:

«3. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.»

Квадрокоптеры доступны всем и оснащены высокоразрешающими средствами оптической разведки, включая тепловизоры. В то же время собственники информации и даже специалисты по информационной безопасности не вполне четко осознают угрозы, пока нет понимания, что высокие этажи и заборы, а также большие контролируемые территории не являются серьезным препятствием для ведения оптической разведки.

В качестве примера, можно привести возможности квадрокоптера ***DJI Air 2S***, имеющего поперечные размеры не больше 250 мм, таким образом, заметить его в воздухе сложно, при весе 600 гр. способен нести высокоразрешающую камеру 20 мега пикселей, находится в воздухе до 30 мин, преодолевает расстояния до 18 км, высота до 5000 м, дальность управления по радиоканалу 8 км [1]. Следовательно, злоумышленник может находиться в безопасности, находясь на большом расстоянии от места проведения разведки. При этом шумовые характеристики под нагрузкой соответствуют примерно 70-75 дБ, услышать квадракоптер на шумной улице практически невозможно (Рис. 1).

Положение 2

Средства оптической (визуальной и тепловизионной) разведки позволяют получать устойчивый канал утечки на дальностях и в условиях, существенно затрудняющих борьбу с утечкой оптической информации, либо в условиях ограниченной видимости и контроля обстановки

Соответствует области исследований в специальности 2.3.6.:

«8. Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения.»

Рис. 1. Квадрокоптер ***DJI Air 2S.*** Уровень шума.

При этом возникают следующие угрозы: перехват текстовой информации, отображенной на экране компьютера, экранах проектора или на бумажных носителях при просмотре через окна; идентификация и слежение за ключевыми лицами; фиксация действий и процессов.

Все это соответствует банку данных угроз, в частности УБИ.067 – Угроза неправомерного ознакомления с защищаемой информацией; УБИ.088 – Угроза несанкционированного копирования защищаемой информации.

Для подтверждения данного положения был проведен анализ дальности распознавания текста на экране монитора или на бумажном носителе. Ключевое условие – трансляция изображения символа текста должна приходиться на массив элементов матрицы 4x4 (Рис. 2).

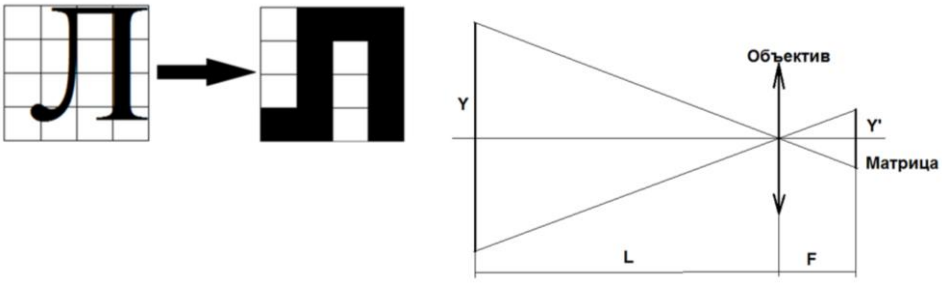


Рис. 2. Анализ дальности распознавания текста

В этом случае будет происходить успешное распознавание символа. Размер четырех элементов можно установить по паспортным данным камеры. Тогда, согласно оптической эквивалентной схеме дальность распознавания определится по формуле 1.1.

$$L = \frac{Y \times F}{Y'}, \tag{1.1}$$

где Y – размер символа; Y' - размер четырех пикселей; F - фокусное расстояние объектива камеры; L - дальность распознавания.

14 шрифт Word имеет размер в распечатке примерно 2,5 мм. Эти размеры связаны с фокусным расстоянием объектива и предельной дальностью разрешения. Здесь наибольшую роль играет фокусное расстояние, т.к. параметры матриц, в основном, подошли к своему пределу и примерно одинаковы. В то же время фокусные расстояния могут меняться в больших пределах с разницей в два порядка. Как пример высокоразрешающего средства разведки можно привести **DJI Inspire 2** с камерой 24 мега пикселя и фокусным расстоянием 50 мм [2] (Рис. 3).

Рис. 3. **DJI Inspire 2** с камерой Zenmuse X7

Камера достаточно тяжелая, и квадрокоптер значительно тяжелее предыдущего. При таких параметрах камеры дальность распознавания текста 14 шрифта составляет 28 м, что в городских условиях в большинстве случае позволяет вести наблюдение за пределами контролируемых зон зданий. Данное исследование было опубликовано в журнале Scopus [3].

Что касается тепловизионной разведки, здесь мы имеем дело с тепловыми следами на информационных носителях, например, клавиатура банкомата или компьютера, при нажатии на клавиши тепловой след сохраняется больше минуты, интенсивность излучения зависит от материала клавиатуры, его коэффициента излучения, длительности нажатия (Рис. 4, 5).

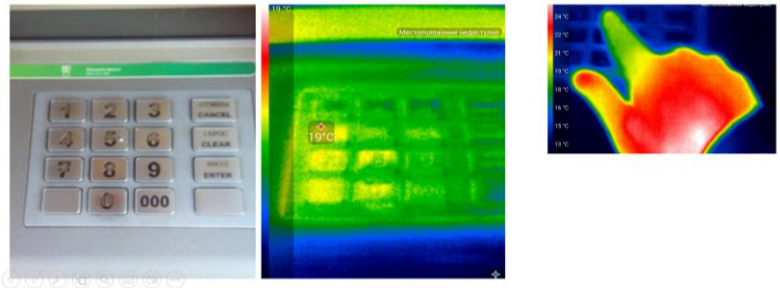


Рис. 4. Тепловые следы на информационных носителях

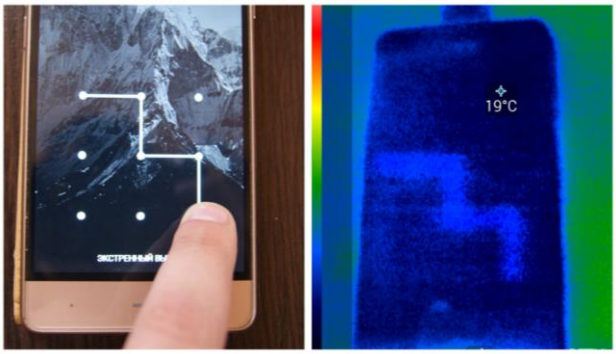


Рис. 5. Тепловые следы на информационных носителях

На пластике, стекле, металле тепловой след сохраняется достаточно долго для его считывания.

В качестве средства тепловизионной разведки можно привести пример инфракрасной камеры, базирующейся на квадрокоптере с матрицей 640x480 и фокусным расстоянием 50 мм (Рис. 6).

Рис. 6. Тепловизионная камера на квадрокоптере.

Это одна из высокоразрешающих тепловизионных матриц. Также может идти речь о тепловизионном наблюдении в ограниченной видимости, ночью или в тумане.

Что касается дальности обнаружения распознавания и идентификации, то для тепловизионного спектра она более сложна и должна учитывать множество факторов, включая параметры среды, объекта, оптики и даже экрана наблюдателя.

Положение 3.

Разработана математическая модель расчета дальности обнаружения распознавания и идентификации с помощью тепловизора.

Соответствует области исследований в специальности 2.3.6.:

«10. Модели и методы оценки защищенности информации и информационной безопасности объекта.*»*

В основе расчета лежат работы исследователей Мирошникова М. М. [5] и Дж. Ллойда [6], которые рассчитывали пороговую разность температур $\Delta T_{пор}$, а также $\Delta T_{раз}$ (разрешения), которая учитывает еще и размер объекта, формулы 1.2 и 1.3.

$$\Delta T_{\text{пор}} = \frac{\pi\sqrt{ab\Delta f_R}K_э T^2}{\alpha\beta A_0 C_2 D^* \int_{\lambda_1}^{\lambda_2} S(\lambda) W_\lambda \tau_0(\lambda)\frac{d\lambda}{\lambda}} \quad (1.2)$$

$$\Delta T_{раз} = \frac{3\Delta T_{пор}\nu\sqrt{\alpha\beta}}{r_\Sigma(\nu)\sqrt{\tau\Delta f_R T_e f_k}}, \quad (1.3)$$

где D^* и $S(\lambda)$ – удельная обнаружительная способность и относительная спектральная чувствительность приемника излучения;

$a, b, \Delta f_R$ – линейные размеры и шумовая полоса частот электрической схемы включения приемника;

λ_1, λ_2 – границы спектральной чувствительности приемника;

$K_э$ – коэффициент использования приемником излучения эталонного источника;

A, α, β - площадь входного зрачка и линейные углы мгновенного поля зрения объектива тепловизора по строке и по кадру;

W_λ – спектральная светимость абсолютно-черного тела (АЧТ) с температурой Т;

$\tau_o(\lambda), C_2$ – спектральный коэффициент пропускания оптической системы и постоянная в формуле Планка;

T_e, f_k – постоянная времени глаза и частота кадров тепловизора;

ν – пространственная частота в пространстве предметов, рад$^{-1}$;

$r_\Sigma(\nu)$ – результирующий модуль передаточной функции (МПФ) всех звеньев тепловизора.

Эти формулы использовались исследователями для расчетов конструкций тепловизоров, при условии минимизации значений $\Delta T_{пор}$ и $\Delta T_{раз}$. Однако вопросы расчета дальности обнаружения, распознавания и идентификации в этих работах не рассматривались. Также и в других работах, посвящённых конструированию тепловизионных приборов, дальности действия уделяется очень мало внимания. В формулах Мирошникова М. М. и Дж. Ллойда нет даже самого понятия дальности действия, поэтому при разработке методики в используемые формулы была введена дальность через применение критерия Джонсона – формула (1.4), которая позволяет принимать решения о дальности обнаружения распознавания и идентификации.

$$\nu = N \Big/ \left(\frac{2h}{l}\right), \quad (1.4)$$

где N – критерий Джонсона; h – критический размер объекта; l – расстояние между объектом и прибором

В результате совместного использования формул 1.2, 1.3, 1.4 выведена формула 1.5 дальности тепловизионного средства разведки с учетом параметров тепловизора, объекта и слоя атмосферы между объектом и прибором.

$$l = \frac{h \cdot r_\Sigma(\nu)\Delta T_{раз}(T_e \cdot f_k)^{1/2} C_2 D^*(d/f')^2 f' \cdot \int_{\lambda_1}^{\lambda_2} S(\lambda)\tau_o(\lambda)\varepsilon(\lambda)W(\lambda,T)\lambda^{-1}d\lambda}{6\sqrt{2}K_э T^2\sqrt{\Delta f_R}N \cdot m}, \quad (1.5)$$

где m – отношение «сигнал/шум»;

Последняя публикация результатов исследования в журнале ВАК Труды учебных заведений связи [7].

Эксперимент.

В ходе эксперимента в качестве лабораторного оборудования использовался тепловизор FLIR TermoCAM с параметрами матрицы 120x120 болометрических элементов, температурная чувствительность дельта Тпор. 0,2 градуса С (Рис. 7).

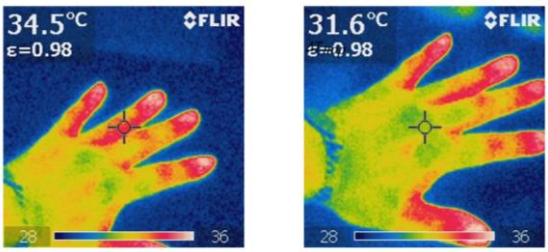


Рис. 7. Тестовый замер температуры руки

Проведен эксперимент по наблюдению тепловых отпечатков с использованием материалов металл, пластик и бумага (Рис. 8).

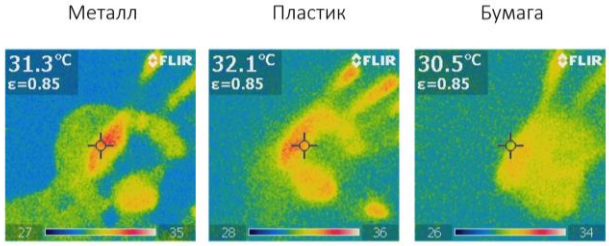


Рис. 8. Замеры тепловых отпечатков.

Эксперимент показала, что температурные отпечатки держатся на указанных материалах более 1 мин. При температуре отпечатка до 30-32 градусов дальность распознавания превышает 4 м, отпечаток виден отчетливо, что подтверждается теоретическими расчетами согласно математической модели (Рис. 9).

Рис. 9. Термоснимок теплового отпечатка пальца на листе металла, дистанция 4 м.

Положение 4

Разработанная методика противодействия организации оптического канала утечки информации, использующего малые беспилотные летательные аппараты позволяет существенно повысить эффективность борьбы с возникновением оптического канала утечки.

Соответствует области исследований в специальности 2.3.6.:

«15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.»

Согласно Федеральному закону РФ от 02.12.2019 №404-ФЗ [8], право как либо воздействовать, включая физические и другие способы, на разведывательные мини-БПЛА имеют только силовые органы государственной власти, такие как ФСБ, МВД, СВР, ФСО и Росгвардия. Таким образом, обычные физические и юридические лица, в качестве средства борьбы могут применять только пассивные методы защиты и не имеют права наносить какой-либо урон чужой собственности. Пассивные методы могут включать организационные и технические меры. К техническим мерам можно отнести средства обнаружения мини-БПЛА. Например, средства, использующие в том числе тепловизионный канал обнаружения (Рис. 10).

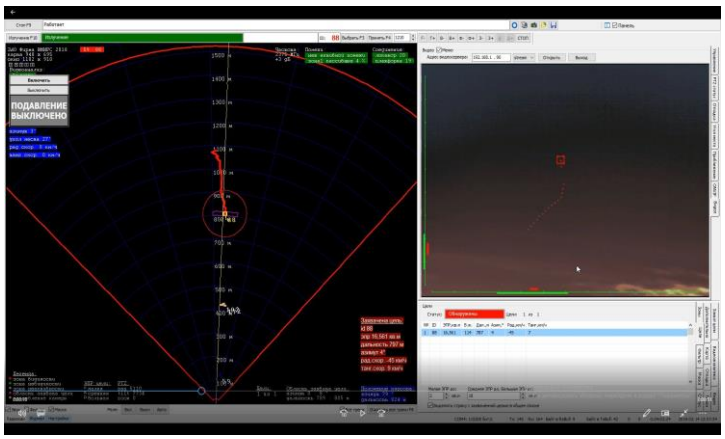


Рис. 10. Комплекс обнаружения и траекторного сопровождения Юмирс БПЛА «РАДЕСКАН-Антидрон»

Данное средство также может использовать вышеуказанную модель обнаружения, распознавания и идентификации, но уже с целью защиты, а не анализа канала утечки [9].

Положение 5

Разработанная программа автоматизированного расчета дальности действия тепловизионных средств разведки позволяет делать точные расчеты контролируемых зон и оперативно реагировать на возникающие опасности перехвата информации по оптическому (тепловизионному) каналу.

Соответствует области исследований в специальности 2.3.6.:

«15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.»

Разработана программа автоматизированного расчета дальности действия тепловизионного средства разведки, получено Свидетельство о регистрации на программное средство [10]. При проведении расчетов в интерфейс программы заносятся параметры тепловизора, предполагаемого объекта и среды и выводится результат расчета дальность обнаружения, распознавания и идентификации (Рис. 11).

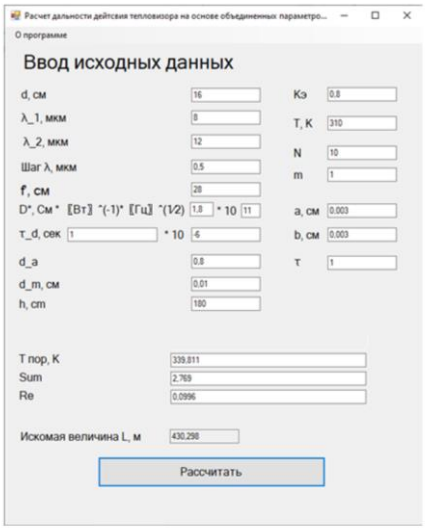


Рис. 11. Интерфейс программы расчета дальности обнаружения, распознавания и идентификации в тепловизионном спектре.

Данную программу можно использовать для более точного определения границ контролируемой зоны и возможных направлений несанкционированного съема информации с использованием тепловизионного диапазона.

СПИСОК ЛИТЕРАТУРЫ

1. Характеристики квадрокоптера DJI Air 2s. [Электронный ресурс]. — Режим доступа: https://www.dji.com/ru/air-2s/specs/16328.html
2. Характеристики квадрокоптера DJI Inspire [Электронный ресурс]. — Режим доступа: https://brlab.ru/scopes/professionalnaya-videosyemka/dji-inspire-2-x7/
3. Ignatenko N. V., Polikanin A. N. Investigation of using quadcopter as a means of acoustic and optic surveillance / N. V. Ignatenko, A. N. Polikanin // Journal of Physics: Conference Series, Tomsk, 20–22 ноября 2019 года. – 2020. – С. 57-61
4. Инфракрасная тепловизионная камера на базе DJI Matrice 200. [Электронный ресурс]. — Режим доступа: https://aeromotus.ru/product/infrakrasnaya-teplovizionnaya-kamera-na-baze-dji-matrice-100-s-radiometriej/
5. Мирошников, М. М. Теоретические основы оптико-электронных приборов: учебное пособие / М. М. Мирошников. — 3-е изд., испр. — Санкт-Петербург: Лань, 2010. — 704 с.
6. Дж. Ллойд. Системы тепловидения/ Перевод с английского канд. техн. наук Н.В.Васильченко. – М. Мир, 1978. – 416 с.
7. Новиков С. Н., Поликанин А. Н. Методика расчета дальности действия тепловизора на основе объединенных параметров температурной чувствительности и разрешения / С. Н. Новиков, А. Н. Поликанин // Труды учебных заведений связи. – 2019. – Т. 5. – № 4. – С. 6 –14.
8. Федеральный закон "О внесении изменений в статью 70 Федерального закона "О государственной регистрации недвижимости" и статью 16 Федерального закона "О внесении изменений в Градостроительный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" от 08.12.2020 N 404-ФЗ (последняя редакция). – [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_370072/
9. Комплекс обнаружения и траекторного сопровождения Юмирс БПЛА «РАДЕСКАН-Антидрон» [Электронный ресурс]. — Режим доступа: https://deviceden.ru/mobilnye-kompleksy-ohrany/yumirs-bpla-radeskan-antidron.html
10. Свидетельство о государственной регистрации программы для ЭВМ № 2021680539 Российская Федерация. Расчет дальности действия тепловизора: № 2021680223: заявл. 13.12.2021: опубл. 13.12.2021 / А. С. Грехов, А. Н. Поликанин [Электронный ресурс]. — Режим доступа: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://elibrary.ru/download/elibrary_47436047_38071114.PDF

Русаков А.М.
РТУ МИРЭА, старший преподаватель
rusakov_a@mirea.ru

КОНЦЕПЦИЯ ПРОЕКТА «РАЗРАБОТКА МОДЕЛИ ДИНАМИКИ РИСКОВ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ ИНФРАСТРУКТУРНОГО ГЕНЕЗА»

Аннотация: Во время перехода к цифровой экономике особенно актуальны вопросы информационной безопасности субъектов критической информационной инфраструктуры (КИИ). С ростом информационных технологий наряду с быстрым моральным «старением» средств защиты информации остаются нерешенные вопросы оценки рисков инфраструктурного характера субъектов КИИ. В данном проекте предлагаются модели и алгоритмы оценки рисков субъектов КИИ с учетом возникающих межобъектных и межсубъетных системных связей инфраструктурного характера и механики рисков ИБ обоснованных тем, что сама система при определенных условиях может генерировать деструктивизм инфраструктурного характера, приводящий к катастрофическим последствиям.

Ключевые слова: критическая информационная инфраструктура, инфраструктурный деструктивизм, модель динамики рисков, деструктивные воздействия.

При переходе к цифровой экономике особенно актуальны вопросы информационной безопасности (ИБ) субъектов критической информационной инфраструктуры (КИИ). Обеспечение безопасности КИИ определено на регулятивном уровне. Однако, в нормативно-правовых и методических регламентах регуляторов, определяющих решение вопросов, связанных с обеспечением безопасности КИИ, не учитывается синергетический эффект от возникающих на инфраструктурном уровне эффектов. В это же время, реализуемые от них деструктивные воздействия, способны привести к инфраструктурному деструктивизму, то есть к саморазрушению системы [1-4].

Специфичные для КИИ признаки и свойства определяют динамизм рисков деструктивного воздействия инфраструктурного генеза, порождаемых самой инфраструктурой [3, 4], что требует их исследования в контексте ИБ.

В проекте предлагается моделирование динамики рисков деструктивного воздействия инфраструктурного генеза (т.е. происхождения), что позволит определить время возникновения точки бифуркации в КИИ-системе и спрогнозировать развитие событий ИБ на инфраструктурном уровне.

Тема проекта связана с разработкой модели динамики рисков деструктивного воздействия инфраструктурного генеза. Диссертационное исследование планируется выполнить на тему: «Методы и алгоритмы оценки рисков деструктивных воздействий инфраструктурного генеза».

Цель исследования: повышение уровня информационной безопасности объектов критической информационной инфраструктуры за счет оценки рисков деструктивных воздействий инфраструктурного генеза.

Для достижения данной цели потребуется решить следующие задачи:

- Анализ видов рисков деструктивных воздействий инфраструктурного генеза.
- Синтез методов и подходов к оценке рисков информационной безопасности в контексте инфраструктурного деструктивизма.
- Оценка меры опасности инфраструктурного деструктивизма.

Результаты диссертационного исследования будут востребованы на всех этапах жизненного цикла субъектов КИИ в условиях цифровой экономики России, а также на уровне образовательных организаций ВО – в рамках курсов дисциплин «Организационно-правовые основы информационной безопасности», «Управление информационной безопасностью», «Информационная безопасность распределенных систем», «Сети и системы передачи данных», «Защищенные распределенные информационные системы».

Научная новизна проекта заключается в том, что, во-первых, впервые будет определена и обоснована динамика рисков инфраструктурного генеза; во-вторых, по-новому выполнено моделирование жизненного цикла субъекта КИИ с акцентом на инциденты инфраструктурного генеза на разных этапах его жизненного цикла; в –третьих, предложена оригинальная многофакторная схема динамики рисков деструктивных воздействий инфраструктурного генеза на субъекте КИИ.

Одной из важных задач по реализации проекта является оценка рисков ИБ субъектов КИИ с учетом возникающих межобъектных и межсубъетных системных связей инфраструктурного характера. Для решения этой задачи предлагается использовать дихотомию рисков информационной

безопасности в условиях инфраструктурного деструктивизма на базе методов их оценки. В данном случае, одним из классов оценок будут несистемные оценки рисков ИБ, полученные традиционным способом без учета синергетического эффекта инфраструктурного деструктивизма.

Отдельно выделим класс систематических оценок рисков субъектов КИИ, к которым отнесем методы на основе анализа межобъектных и межсубъетных системных связей инфраструктурного характера. Работы в данном направлении уже ведутся и имеют положительные результаты [1-4]. В проекте продолжим развитие данного подхода, используя понятие синергизма. Применим термин синергизма к проблеме оценки рисков деструктивных воздействий субъектов КИИ получим, что взаимодействия одного или нескольких воздействий может усиливать или нейтрализовать как положительный, так и отрицательный эффект. Выделяют следующие вида синергизма:

- потенцирование эффекта.
- сенситизирующее действие деструктивных воздействий;
- суммация эффекта;
- аддитивное действие деструктивных воздействий.

Таким образом, учет синергизма при оценке рисков информационной безопасности позволит более точно прогнозировать деструктивные воздействия на КИИ.

Среди работ в области защиты КИИ от деструктивных воздействий следует выделить работы М.В. Буйневича, К.Е. Израилова, М.А. Еремеева, А.К. Новохрестова, С.И. Макаренко, Г.В. Бабенко, Н.А. Гайдамакина, П.Н. Девянина, Д.П. Зегжды, П.Д. Зегжды, Е.А. Максимовой и других ученых. Перспективными являются работы Г. А. Остапенко, А. Н. Шершень[5, 6]; С. И. Макаренко [7]; П. Д. Зегжда, В. Г. Анисимов, А. Ф. Супрун [8]; Е. А. Басыни [9]; Д. В. Афанасьевой [10].

Для реализации проекта потребуется рассмотреть статистический анализ взаимосвязи и взаимозависимости признаков, теоретико-множественные модели и методы анализа и прогнозирования рисков деструктивных воздействий, современные модели и методы поддержки принятия решений по обеспечению информационной безопасности КИИ, событийный и сценарный подход для оценки информационной безопасности, а также различные методы интеллектуального анализа данных и искусственного интеллекта в сфере информационной безопасности.

Решение вопросов повышение уровня информационной безопасности КИИ за счёт разработки методов и алгоритмов оценки рисков деструктивных воздействий инфраструктурного генеза требует дальнейшего исследования.

СПИСОК ЛИТЕРАТУРЫ

1. Максимова, Е. А. Модель состояний субъектов критической информационной инфраструктуры при деструктивных воздействиях в статичном режиме / Е. А. Максимова // Труды учебных заведений связи. – 2021. – Т. 7. – № 3. – С. 65-72. – DOI 10.31854/1813-324X-2021-7-3-65-72.
2. Максимова, Е. А. Оценка информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях / Е. А. Максимова; Волгоградский государственный университет. – Волгоград: Волгоградский государственный университет, 2020. – 95 с. – ISBN 978-5-9669-1975-7.
3. Anthropomorphic Model of States of Subjects of Critical Information Infrastructure Under Destructive Influences / E. A. Maksimova, A. M. Rusakov, M. A. Lapina, V. G. Lapin // Lecture Notes in Networks and Systems. – 2022. – Vol. 424. – P. 569-580. – DOI 10.1007/978-3-030-97020-8_51.
4. Максимова, Е. А. Метод оценки инфраструктурной устойчивости субъектов критической информационной инфраструктуры / Е. А. Максимова, М. В. Буйневич // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 1(43). – С. 50-63. – DOI 10.14529/secur220107.
5. Предупреждение и минимизация последствий компьютерных атак на элементы критической информационной инфраструктуры и автоматизированные информационные системы критически важных объектов: риск-анализ и оценка эффективности защиты / А. Г. Остапенко, Е. В. Ермилов, А. Н. Шершень [и др.] // Информация и безопасность. – 2013. – Т. 16. – № 2. – С. 167-178.
6. Остапенко, Г. А. Концептуальный подход к расчету и регулированию рисков нарушения актуальности информации в элементах критической информационной инфраструктуры / Г. А. Остапенко, А. Н. Шершень, А. О. Калашников // Информация и безопасность. – 2013. – Т. 16. – № 2. – С. 239-242.
7. Макаренко, С. И. Динамическая модель двунаправленного информационного конфликта с учетом возможностей сторон по наблюдению, захвату и блокировке ресурса / С. И. Макаренко

// Системы управления, связи и безопасности. – 2017. – № 1. – С. 60-97. – DOI 10.24411/2410-9916-2017-10106.
8. Зегжда П. Д., Анисимов В. Г., Супрун А. Ф. и др. Модели и метод поддержки принятия решений по обеспечению информационной безопасности информационно-управляющих систем //Проблемы информационной безопасности. Компьютерные системы. – 2018. – №. 1. – С. 43-47.
9. Басыня, Е. А. Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия / Е. А. Басыня // Безопасность информационных технологий. – 2018. – Т. 25. – № 4. – С. 42-51.
10. Афанасьева, Д. В. Применение искусственного интеллекта в обеспечении безопасности данных / Д. В. Афанасьева // Известия Тульского государственного университета. Технические науки. – 2020. – № 2. – С. 151-154.

Стручков И.В.
Северо-Кавказский федеральный университет,
инженер-исследователь,
selentar@bk.ru

РАЗРАБОТКА МЕТОДА ВЫЯВЛЕНИЯ ВРЕДОНОСНЫХ ВОЗДЕЙСТВИЙ НАРУШИТЕЛЕЙ ПРИ РЕАЛИЗАЦИИ ДОВЕРЕННОГО ВЗАИМОДЕЙСТВИЯ АГЕНТОВ В ДЕЦЕНТРАЛИЗОВАННОЙ КИБЕРФИЗИЧЕСКОЙ СРЕДЕ

Аннотация: Высокий темп роста интеграции вычислений с физическими процессами определяет популярность киберфизических систем и актуализирует вопросы обеспечения их информационной безопасности при реализации доверенного взаимодействия. В большинстве работ по взаимодействию агентов в киберфизической системе, предлагаемые методы апробируются в лабораторных условиях и не учитывают наличие неблагоприятной внешней среды. При этом, наряду с традиционными угрозами информационной безопасности, киберфизические системы подвержены угрозам реализации специфических атак за счет системных свойств. Целью работы является повышение эффективности выполнения функциональных задач агентами в децентрализованной киберфизической системы путем обеспечения доверенного взаимодействия между ними на основе технологии распределенного реестра. Научная новизна исследования заключается в применении для реализации доверенного взаимодействия технологии распределенного реестра для объединения показаний отдельных цепочек блоков взаимодействия устройств киберфизической системы с последующим анализом полученных данных с целью обнаружения аномальных значений их поведения и выявления вредоносных воздействий нарушителей.

Ключевые слова: слова: доверенное взаимодействие, информационная безопасность, технологии распределённого реестра, киберфизические системы.

Цели и задачи научного проекта

Цель исследования состоит в повышении эффективности выполнения функциональной задачи агентами в доверенной кибер-физической среде (ДКФС) путем обеспечения доверенного взаимодействия (ДВ) между ними на основе технологии распределенного реестра (ТРР).

Для достижения поставленной цели необходимо решить следующие частные научные задачи:

1. Разработать математическую модель ДВ агентов в ДКФС при выполнении функциональных задач.
2. Разработать модель угроз ИБ процесса ДВ агентов в ДКФС, формализующих сценарии атак на ИБ ДВ (п.8 паспорта научной специальности 05.13.19 (2.3.6)).
3. Разработать метод ДВ агентов в ДКФС на основе ТРР (п.13 паспорта научной специальности 05.13.19 (2.3.6)).
4. Разработать метод и алгоритм оценки доверия к агентам при их взаимодействии в ДКФС (п.3 паспорта научной специальности 05.13.19 (2.3.6)).
5. Выполнить имитационное моделирование и оценить эффективность разработанных моделей, методов и решений с учетом ограничений вычислительных и информационных ресурсов агентов в ДКФС.

Анализ современного состояния исследований в данной области

Киберфизические системы (КФС) являются активно развивающейся областью техники. Популярность применения КФС связана с ростом автоматизации, которая приводит к интеграции вычислений с физическими процессами. КФС используют связь между разнородными физическими объектами при различных технологиях, таких как радиочастотная идентификация (RFID), беспроводные сенсорные сети (WSN) [1]. Агенты подобных систем взаимодействуют в киберфизической среде и находят приложения в таких областях как медицина, управление дорожным движением и безопасностью, групповая робототехника, системы вооружения и связи и т. д.

Проведен анализ литературы по теме исследования с помощью базы Scopus. Использовался набор ключевых слов для первоначального отбора документов: trust management AND information security. Представлена динамика исследовательской активности, полученная на основе сопоставления количества научных работ в данной области по годам, относительно ДВ и работ, посвященным ИБ ДВ (рис. 1). Количество исследований в данной области демонстрирует неуклонный интерес к ИБ ДВ. Этот обусловлено важностью обеспечения ИБ в следствии развития технологий и увеличения числа киберпреступлений.

Рис. 1. Динамика исследовательской активности

Наиболее часто в приведенной выборке, встречается упоминание таких областей как: сетевая безопасность, блокчейн, безопасность данных и интернет вещей. Распределение наиболее встречаемых тем в статьях, посвященных ИБ ДВ (рис. 2).

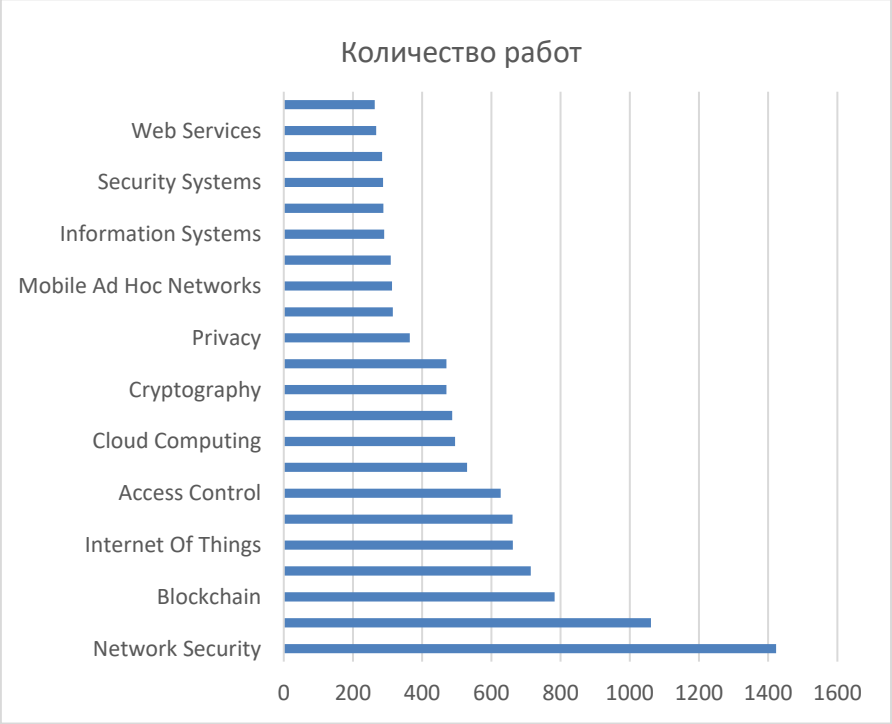


Рис. 2. Распределение по направлениям исследований

Из представленных работ к области ДВ агентов в ДКФС наибольший интерес представляют примерно треть от общего числа отобранных работ: принятие решений, беспроводные сенсорные сети, интернет вещей, TPP и распределенные компьютерные системы.

Российских разработок, в международной базе практически не представлено. Это связано с закрытостью ограничениями в области разработок ИБ. С большим отрывом лидирует Китай, затем США и Индия. Российские работы по количеству располагаются на 29 месте (рис. 3).

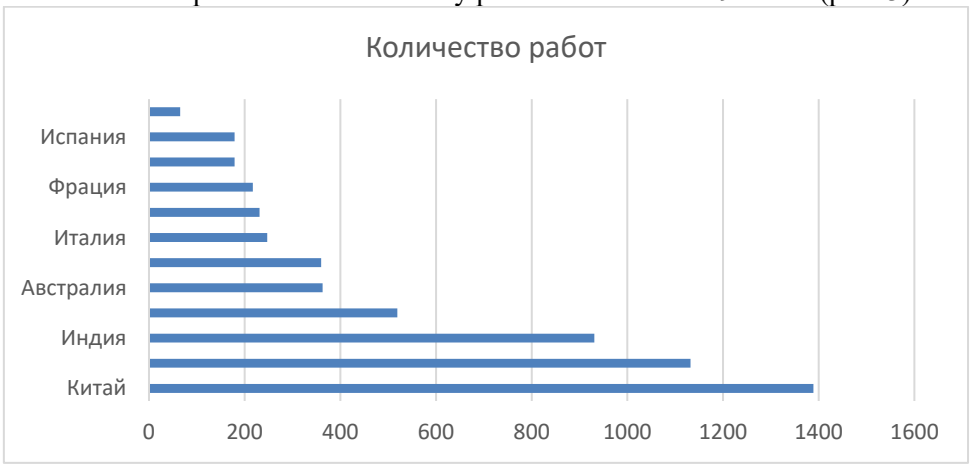


Рис. 3. Распределение по странам исследований

Проанализированы ведущие организации-разработчики решений, исследования которых содержат технические решения в области ИБ ДВ (рис. 4).

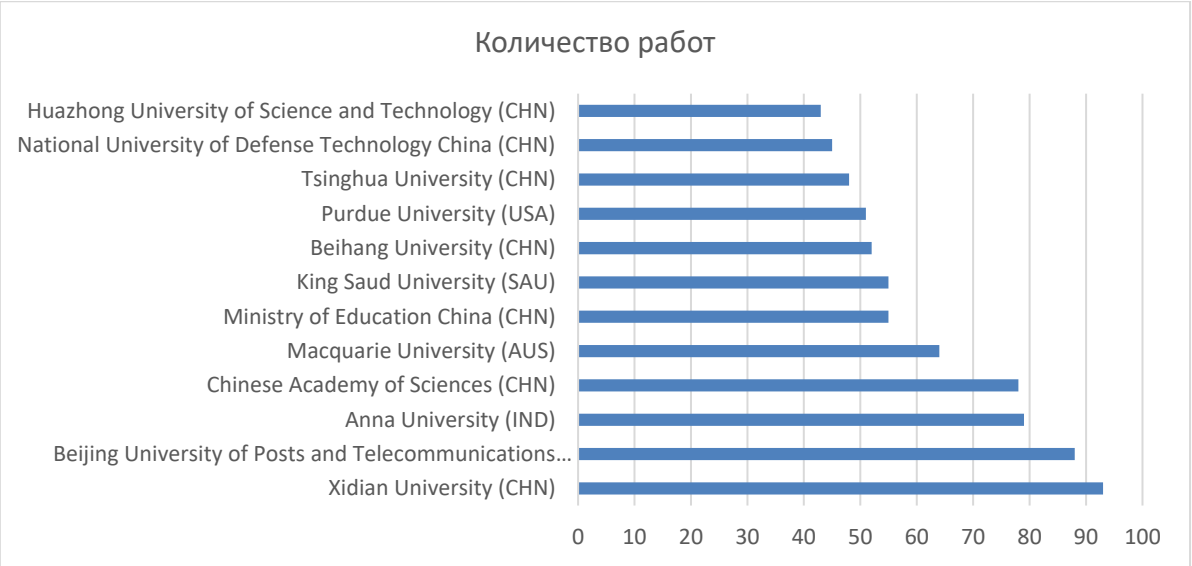


Рис. 4. Распределение по организациям исследований

Можно сделать вывод о том, что КФС совместно с системами связи осуществляют контроль за физическими процессами, обычно путем передачи данных через узлы системы централизованно, где процессы влияют на вычисления и наоборот. На практике при решении ряде задач, требующих покрытия больших пространств, эффективным является децентрализованное взаимодействие между отдельными устройствами КФС. В большинстве работ, предлагаемые методы не учитывают наличие угроз ИБ. При этом, наряду с традиционными угрозами ИБ, КФС подвержены угрозам реализации специфических атак за счет системных свойств КФС, например, вредоносных воздействий нарушителей при реализации ДВ. Под вредоносным воздействием понимаются действия узлов децентрализованной системы, которые демонстрируют непоследовательное поведение, независимо от основной причины. Наличие таких при реализации ДВ может привести к невозможности выполнить целевую функцию КФС.

Таким образом, ИБ это одна из проблем, влияющих на эффективность работы агентов в КФС [2]. Часто для решения проблемы ИБ используются такие механизмы «Hard Security» [3]. Однако подобные механизмы не обеспечивают надежность КФС при наличии злонамеренных действий со стороны инсайдера из-за изменения его поведения. Методы управления доверием [4,5] решают эту проблему, измеряя степень уверенности в поведении, ожидаемом другими. Концепция доверия относится к категории «Soft Security» [3]. Эти решения связаны с поддержанием репутации, которая определяет общее представление о поведении объекта. Доверие исследовалось для различных областей, таких как социальные сети [6], WSN [7], P2P [8], MANET [9]. В работе [10] представлен обзор проблем ДВ в КФС. Однако, данная работа не охватывает важные аспекты доверительного управления, такие как тип используемой математической модели и принятая архитектура. Вопросы обеспечения ИБ ДВ в КФС являются актуальным направлением исследований, а выявление вредоносных воздействий нарушителей при реализации ДВ агентов в ДКФС среде становится одним из главных барьеров для применения КФС на практике.

Предлагаемые методы и подходы к решению поставленных задач

Предлагаемые методы и подходы к решению поставленных задач базируются на использовании положений теории ИБ, методов машинного обучения, методов оптимизации, искусственного интеллекта и TPP.

Новизна исследования, заявленного в проекте

В рамках данного проекта предлагается научная идея разработки метода выявления вредоносных воздействий нарушителей при реализации ДВ агентов в ДКФС.

Новизна исследования заключается в применении для реализации ДВ TPP для объединения показаний отдельных цепочек блоков взаимодействия агентов КФС с последующим анализом полученных данных с целью обнаружения аномальных значений. Предлагаемые решения позволят выполнить: хранение, агрегирование данных о действиях агентов и выявление вредоносных воздействий нарушителей при реализации ДВ.

Практическая значимость предлагаемых решений обусловлена факторами достижения за счет предлагаемых технических решений высоких показателей ИБ ДВ агентов в ДКФС, что позволит

повысить отказоустойчивость. Предлагаемые модели, методы и алгоритмы позволят повысить эффективность КФС при реализации ДВ агентов.

Ожидаемые по окончании проекта научные результаты.

Ожидаемыми научными результатами реализации проекта являются:

1. Математическая модель ДВ агентов в ДКФС.
2. Модель угроз ИБ процесса ДВ агентов в ДКФС.
3. Метод ДВ агентов в ДКФС на основе ТРР.
4. Метод и алгоритм оценки доверия к агентам при взаимодействии агентов в ДКФС.

СПИСОК ЛИТЕРАТУРЫ

1. Grgurevic I. et al. Application of the Internet of Things Concept in Carsharing System. 2015. P. 401–414.
2. Sicari S. et al. Security, privacy and trust in Internet of Things: The road ahead // Comput. Networks. Elsevier, 2015. Vol. 76. P. 146–164.
3. Jøsang A., Keser C., Dimitrakos T. Can We Manage Trust? // Lect. Notes Comput. Sci. Springer, Berlin, Heidelberg, 2005. Vol. 3477. P. 93-107.
4. Бахтин А. А., Брагин Д. С., Конев А. А., Шарамок А. В. Оценка соответствия модели угроз и требований доверия систем Интернета вещей массового применения // Наноиндустрия. – 2020. – Т. 13. – № S4(99). – С. 137-138. – DOI 10.22184/1993-8578.2020.13.4s.137.138. – EDN DQPZLH.
5. Степенкин, А. А. Доверительная модель информационной безопасности среды многоагентных робототехнических систем // Вопросы кибербезопасности. – 2020. – № 6(40). – С. 23-31. – DOI 10.21681/2311-3456-2020-06-23-31. – EDN ROPRAF.
6. Sherchan W., Nepal S., Paris C. A survey of trust in social networks // ACM Comput. Surv. ACM PUB27 New York, NY, USA , 2013. Vol. 45, № 4.
7. Lopez J. et al. Trust management systems for wireless sensor networks: Best practices // Comput. Commun. 2010. Vol. 33, № 9. P. 1086–1093.
8. Josang A., Ismail R., Boyd C. A survey of trust and reputation systems for online service provision // Decis. Support Syst. North-Holland, 2007. Vol. 43, № 2. P. 618–644.
9. Ahmed A. et al. A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks // Front. Comput. Sci. Higher Education Press, 2015. Vol. 9, № 2. P. 280–296.
10. Yehia L., Khedr A., Darwish A. Hybrid Security Techniques for Internet of Things Healthcare Applications // Adv. Internet Things. Scientific Research Publishing, Inc, 2015. Vol. 05, № 03. P. 21–25.

Сушкин Н. А.
ИКТИБ ЮФУ, аспирант, техник,
sushkin@sfedu.ru

ТЕХНОЛОГИЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ВОЗДЕЙСТВИЯ НА СИСТЕМУ НАВИГАЦИИ И СВЯЗИ БПЛА

Аннотация: Глобальная навигационная спутниковая система (GNSS) широко используется для определения местоположения БПЛА и на сегодняшний день является самым популярным навигационным решением. Это связано с простотой и относительно невысокой стоимостью данной технологии, а также точностью передаваемых координат. Тем не менее, существует множество угроз безопасности для систем навигации и связи навигации. Это в первую очередь связано с природой навигационного сигнала, т. к. сигнал передается в открытом виде, поэтому злоумышленник может заблокировать или подделать его. В данном исследовании проведен анализ существующих методов защиты систем навигации и связи. В рамках исследования был разработан экспериментальный стенд и сценарии атак на систему навигации GPS для БПЛА. Далее были собраны данные из журнала полетов БПЛА и проведен анализ кибер-физических параметров, чтобы зафиксировать влияние атаки на показания бортовых датчиков. Исходя из этого, был предложен новый метод обнаружения аномалий БПЛА, основанный на анализе изменений внутренних параметров БПЛА. Этот метод самодиагностики позволяет БПЛА оценивать наличие изменений в его подсистемах, и выявлять признаки кибератаки. Проведение реальных атак на БПЛА позволило проанализировать природу изменений поведения БПЛА под воздействием атаки, а также изменений его кибер-физических параметров.

Ключевые слова: безопасность, атака, навигационная система, беспилотный летательный аппарат, угроза, вероятность, глобальная навигационная спутниковая система, технология защиты.

Научная новизна исследования:

1. Разработка нового метода автономного обнаружения вредоносного воздействия, основанного на анализе изменений кибер-физических параметров БПЛА.
2. Технология обнаружения вредоносного воздействия на систему навигации и связи БПЛА, обеспечивающая определение типа вредоносного воздействия в автономном режиме.
3. Построение модели вредоносного воздействия на систему навигации и связи БПЛА.

Научная задача

1. Разработка технологии обнаружения вредоносного воздействия на систему навигации и связи БПЛА.
2. Реализация программного обеспечения для полетного контроллера или платы управления БПЛА, которое позволит в автономном режиме обнаруживать атаку и уведомлять об этом оператора, либо соседние БПЛА.
3. Разработка метода автономного обнаружения вредоносного воздействия для БПЛА, основанного на анализе изменений кибер-физических параметров БПЛА.
4. Разработка методики категорирования и оценки типов вредоносного воздействия на БПЛА.

Ожидаемые результаты:

1. Технология обнаружения вредоносного воздействия на систему навигации и связи БПЛА, реализованная в виде программного обеспечения для полетного контроллера или платы управления БПЛА.
2. Метод автономного обнаружения вредоносного воздействия для БПЛА, основанный на анализе изменений кибер-физических параметров БПЛА, который будет внедрен в технологию обнаружения вредоносного воздействия на систему навигации и связи БПЛА.
3. Методика категорирования и оценки типов вредоносного воздействия на БПЛА.

Анализ аналогов разрабатываемой технологии:

Вопросы реализации методов обнаружения атак подделки данных глобальной системы позиционирования и связи для беспилотных летательных аппаратов рассматриваются, как зарубежными, так и Российскими исследователями и являются достаточно актуальными. Для обмена информацией, как между БПЛА, так и между БПЛА и оператором используются беспроводные каналы связи. Беспроводной канал не защищен физически, поэтому нарушитель может оказать на него воздействие. Воздействие на канал передачи данных также может быть оказано со стороны окружающей среды. На сегодняшний день атака на глобальную навигационную систему при правильном ее исполнении может привести к серьезным последствиям для БПЛА или группы БПЛА

[1]. Помимо естественной ошибки, присутствующей в показаниях датчиков, на полетный контроллер также влияют естественные уязвимости навигационной системы, такие как возможность блокировки или глушение сигнала, которые ставят под угрозу доступность сигнала. Уязвимости навигационной системы выходят за рамки естественных свойств передаваемого сигнала. Атаки подделки навигационного сигнала — это атаки, в которых спутники, передающие сигнал подделываются с целью манипулирования навигационной системой БПЛА посредством передачи поддельных координат, созданных злоумышленником [2],[3].

Атака подделки GPS влечет за собой последствия, связанные с падением БПЛА, либо его перехватом и перенаправлению по другой траектории полета. В обоих случаях данные проблемы связаны с кибербезопасностью. Целенаправленная атака, которая берет под контроль БПЛА или просто уничтожает его, может легко причинить вред всем, кто находится в зоне полета БПЛА, или повредить другие транспортные средства [4].

Для повышения безопасности любой информационной системы важно обнаружить уязвимости до того, как это делают злоумышленники. Это достигается за счет постоянного анализа и оценки рисков. Уязвимости для БПЛА можно разделить на 4 группы:

1. Уязвимости базовой системы
2. Уязвимости каналов связи
3. Уязвимости датчиков
4. Уязвимости авионики [5].

При обнаружении аномалий в группах БПЛА, к примеру, основное внимание уделяется методам, на основе анализа физических параметров технологического процесса, таких как: показания датчиков, состояние исполнительных механизмов, и математические отношения между ними, контролируемые соответствующими программируемыми логическими контроллерами для выявления аномалий.

В области обнаружения аномалий был предложен ряд современных методов, которые в основном можно разделить на следующие три категории: методы, основанные на знаниях, методы на основе моделей и методы, основанные на данных. Метод, основанный на знаниях, позволяет получить шаблоны аномалий путем обобщения опыта экспертов в конкретной области, реализовать систему обнаружения аномалий и обнаружение тех же шаблонов аномалий [6]. Метод, основанный на модели, обычно строится наблюдателем путем создания точной физической модели системы, а затем сравнивает оценочное значение наблюдателя или фильтра с фактическим измеренным значением. По сгенерированной остаточной ошибке выполняется обнаружение аномалии [7]. Метод, на основе данных, автоматически изучает поведенческую модель системы на основе собранных данных системного процесса [8]. Для реализации первых двух методов необходимо обладать знаниями предметной области или системы БПЛА, чтобы получить хороший результат обнаружения аномалий. Однако, как правило, трудно создать точную физическую модель для каждой подсистемы БПЛА. Поскольку в реальных полетных данных БПЛА имеется немного аномальных образцов, и только известные аномальные образцы могут быть обнаружены. Адаптивность и возможности защиты от помех этих двух методов ограничены.

В основном методы строятся на анализе изменения состояния по сравнению с эталонным или на корреляции данных, полученных от нескольких датчиков GPS [9]. В некоторых методах помимо GPS используются другие сенсорные механизмы типа магнитометра акселерометра и другие, для улучшения качества полета [10]. При это корреляция может проходить как между устройствами одного БПЛА, так и между устройствами БПЛА группы.

Представленный в этом исследовании метод основан анализе изменения состояния БПЛА. При этом, как подтверждено экспериментально, метод позволяет достаточно точно детектировать наличие аномального поведения и определять атаку. Новизна и достоинство предложенного метода заключается в следующем: метод является универсальным и может быть применен к различным набором данным, получаемых от сенсорной системы БПЛА. Метод определяет лишь то, что в системе произошло изменение и делает это достаточно точно, далее уже дело системы принятия решений определить является ли изменение атакой. Метод не требует информации о том, какие значения являются эталонными и нормальными. Он основан на том, что БПЛА самостоятельно анализирует изменения показателей и сравнивает свое состояние в разные промежутки времени. Если состояние устойчивое или быстро переходит в устойчивое, то аномалий нет.

Ключевое предположение нового подхода к обнаружению неисправностей на основе данных состоит в том, что характеристики, которые измеряются для каждого компонента БПЛА, предположительно включают в себя различные шаблоны неисправных состояний, отличных от

безопасных состояний. Подход направлен на изучение характеристик безопасных состояний БПЛА по этим функциям на этапе кодирования и распознавание любых аномальных шаблонов как ошибок на этапе установления порога. Хотя необработанные журналы полетов включают образцы состояний БПЛА, некоторые метрики могут быть не учтены или пропущены. Чтобы извлечь важную информацию для обнаружения неисправностей, процесс выбора признаков имеет решающее значение при разработке входного вектора признаков.

Поскольку метод позволяет анализировать любые параметры и может работать с любыми доступными данными, то не имеет значения, какими датчиками оснащен БПЛА. С помощью разработанного метода можно не только обнаруживать аномалии, но и определять изменение закономерностей поведения БПЛА, изменение его состояний. Если значения определяемой энтропии не слишком высоки, и имеет место однократное увеличение, то это может указывать на изменение режима полета. Соотношение анализируемых параметров позволяет выявить атаку и определить ее тип. Каждая атака затрагивает определенный набор подсистем, поэтому тип атаки можно охарактеризовать по результирующим параметрам, на которые она влияет. Данные, собранные в виде временных рядов, могут быть использованы для обучения нейронных сетей принимать решения о проведении атаки. Метод может использоваться для анализа других наборов параметров и применяться не только к БПЛА, но и к любой кибер-физической системе.

СПИСОК ЛИТЕРАТУРЫ

1. Warner J. S., Johnston R. G. A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing //Journal of security administration. – 2002. – Т. 25. – №. 2. – С. 19-27.
2. Lester E. T. Military position source challenges for worldwide ADS-B out compliance //2013 Integrated Communications, Navigation and Surveillance Conference (ICNS). – IEEE, 2013. – С. 1-12.
3. Clifton A. Ericson, Software safety in a nutshell.
4. "Global positioning system directorate", In: Systems engineering and integration Interface Specification IS-GPS-200G Technical Report, 2012.
5. Blasch E. 1. J. Salerno, and G. Tadda," Measuring the Worthiness of Situation Assessment," //Proc. IEEE Nat. Aerospace Elect. Coif. – 2011. – Т. 20. – С 87-94
6. Zhang Y. M. Fault Detection and Diagnosis for NASA GTMUAV with Dual Unscented Kalman Filter //Handbook of Unmanned Aerial Vehicles. – 2015. – С. 1157-1181.
7. Birnbaum Z. et al. Unmanned aerial vehicle security using recursive parameter estimation //Journal of Intelligent & Robotic Systems. – 2016. – Т. 84. – №. 1. – С. 107-120.
8. Pang J. et al. Anomaly detection based on data stream monitoring and prediction with improved Gaussian process regression algorithm //2014 International Conference on Prognostics and Health Management. – IEEE, 2014. – С. 1-7.
9. Eldosouky A. R., Ferdowsi A., Saad W. Drones in distress: A game-theoretic countermeasure for protecting uavs against gps spoofing //IEEE Internet of Things Journal. – 2019. – Т. 7. – №. 4. – С. 2840-2854.
10. Qiao Y., Zhang Y., Du X. A vision-based GPS-spoofing detection method for small UAVs //2017 13th International Conference on Computational Intelligence and Security (CIS). – IEEE, 2017. – С. 312-316.

Фельдман Е.В.
Челябинский государственный университет, старший преподаватель кафедры Компьютерной безопасности и прикладной алгебры

РАЗРАБОТКА МОДЕЛИ ОБНАРУЖЕНИЯ АНОМАЛЬНЫХ БАНКОВСКИХ ТРАНЗАКЦИЙ ДЛЯ ПРОТИВОДЕЙСТВИЯ СОВЕРШЕНИЮ БЕСКОНТАКТНЫХ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ФИНАНСОВЫХ ОПЕРАЦИЙ

Аннотация: не более 200 слов. Цифровизация различных процессов создала площадку, позволяющую бесконтактно совершать общественно опасные деяния. Злоумышленники научились похищать информацию, обходить систему платежей налогов, создавать серые схемы расчетов, в том числе с использованием криптовалют. Отдельной проблемой специалисты выделяют тему узаконивания денег, добытых запрещенным путем, средства полученные при мошенничестве, наркоторговле, торговле людьми и так далее. Для восполнения экономической и информационной стабильности и безопасности в приоритете является разработка и внедрение новых информационных и финансовых технологий и специальные автоматизированные системы. Автоматизированная система контроля с (Anti-Money Laundering system, AML-системы) в настоящее время стала одним из главных подходов в борьбе с совершением бесконтактных преступлений с использованием цифровых технологий. Существующие методы искусственного интеллекта разработаны недостаточно для борьбы с бесконтактными преступлениями при использовании финансовых операций, также не существует универсальных систем анализа транзакций. Разработка методов борьбы с бесконтактными преступлениями при использовании финансовых операций в настоящее время актуальна. Цель работы – разработать организационные и технические способы противодействия, а также модели обнаружения аномальных банковских транзакций, применяемых при процессе отмывания денег и нелегальном обороте товаров и услуг.

Ключевые слова: компьютерная безопасность, машинное обучение, распознавание образов, нейронные сети, классификация, выявление аномальных транзакций, банковские транзакции.

(пустая строка)

Существующие методы искусственного интеллекта разработаны недостаточно, что не позволяет обрабатывать поток операций, проходящих онлайн. Отметим, что во время интеллектуального анализа существующих решений транзакции фильтруются в соответствии с разработанными правилами и заданными ограничениями. Все отфильтрованные транзакции считаются «законными» и не проходят процедуру анализа, который может быть использован в незаконных целях. Существующие решения учитывают только показатели, связанные непосредственно с операцией или ее участниками, и не учитывают косвенные показатели. В результате возникают ложные ошибки и срабатывания. Таким образом, важными проблемами в области автоматизации противодействия легализации (отмыванию) денег, полученных незаконным путем, и поддержке терроризма являются [1]: невозможность автоматизировать в режиме онлайн те факторы и признаки, которые уникальны для конкретных видов финансовой деятельности или финансовых агентств; отсутствие централизованного инструмента для анализа транзакций; обязательность в использовании сочетания программного обеспечения и ручного анализа; большое количество неверных срабатываний и ошибок; существенные затраты на содержание команды аналитиков для ручного анализа транзакций.

В настоящее время стоит вопрос о разработке и развитии системы, которая будет фиксировать подозрительные транзакции. С ее помощью можно облегчить и ускорить процесс обработки данных, снизить риски, хранить информацию и данные о злоумышленниках, рассчитать их скоринг, далее это помогает отслеживать пользователей, которые могут заниматься отмывкой денег. Но из-за высокой стоимости таких систем только позволить себе их могут только крупные финансовые организации [2].

Высокую надежность информации обусловлено решениями, поддерживающими искусственный интеллект. Они автоматизируют весомую часть операций и обеспечивают надежность информации за счет расширенных возможностей анализа структурированных и неструктурированных данных. Современные системы научились выполнять следующие операции [1]: исследование и анализ активности клиентов; мониторинг коммуникаций, анализ писем по ключевым словам; многоязычный мониторинг, по сравнению с существующими инструментами решения искусственного интеллекта предлагает лучший вариант для перевода или транслитерации имен клиентов, кодовых слов и других данных на языках и скриптах, отличных от тех, которые используются в языках с латинскими корнями; мониторинг списков наблюдения, длинные отраслевые списки, включающие имена на нелатинских языках. Это затрудняет постоянный анализ существующих инструментов.

Борьба с отмыванием денег важна для обеспечения безопасности финансовых систем, а также для обнаружения незаконного оборота услуг и товаров. Создание виртуальных денег (криптовалюты), казалось бы, вызвало в обществе противоречие: скрываться от правоохранительных органов и действия закона злоумышленникам помогает анонимность, но доступная операция базы криптовалют дает возможность вести криминалистическое исследование, либо аналитику денежных операций. Важная функция AML аналитики – это отслеживание и фиксация подозрительных транзакций. Анализ транзакции, проведенный вручную, может показывать ошибочные данные. В сравнении с ним прогресс в настоящее время стоит за автоматическим анализом криптографических транзакций [3,4,5,6,7,8].

Выявление противоправных действий с кредитными картами позволяет определить, является ли транзакция мошеннической на основе исторических данных. Изменения в расходах клиентов в разные дни, например, в обычные будни и праздничные выходные, создают трудности в исследованиях экспертов [9,10,11,12].

Техническое сопровождение оперативных мероприятий и следственных действий является важным вопросом. Техническое сопровождение состоит из следующих этапов: обыски, выемки, наведение справок, получение компьютерной информации; правильное написание запросов в организации; правильное назначение исследования, компьютерной экспертизы. При реализации по компьютерным преступлениям (и по тем преступлениям, которые совершаются с использованием компьютерных технологий) следователь и оперативные сотрудники должны не только обеспечивать соответствие мероприятия процессуальным нормам, но и обеспечивать соответствие электронных носителей или компьютерной информации на предмет наличия доказательной базы, а также целостности данной информации.

Задачи научного исследования: анализ состояния предметной области и инструментов для борьбы с бесконтактными преступлениями при использовании финансовых операций; оценка возможности использования доступных наборов данных для разработки модели обнаружения аномальных банковских транзакций; разработка модели обнаружения аномальных банковских транзакций; сравнительный анализ точности разработанных моделей обнаружения аномальных банковских транзакций.

Новизна научного исследования состоит в решении следующих перспективных задач: проведение комплексного анализа принципов и решений для борьбы с бесконтактным совершением преступлений при использовании цифровых технологий, и разработка научно-обоснованной модели обнаружения аномальных банковских транзакций с помощью методов машинного обучения.

СПИСОК ЛИТЕРАТУРЫ

1. Khrestina M.P. Development of Algorithms for Searching, Analyzing and Detecting Fraudulent Activities in the Financial Sphere / Khrestina M.P., Dorofeev D.I., Kachurina P.A., Usubaliev T.R., Dobrotvorskiy A.S. // European Research Studies Journal. — 2017. —4B. — 484-498.
2. Анженко Т.А. Применение финансовых технологий для противодействия отмыванию денежных средств [Электронный ресурс]: Официальный сайт газеты «Экспертный союз». – Режим доступа: https://confes.fb.tusur.ru/sites/default/files/webform/Anzhenko T. Fintech.docx (дата обращения 09.07.21);
3. Weber M. Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics / Weber M., Domeniconi G., Chen J., Weidele D., Bellei C., Robinson T., Leiserson C. // Arxiv. — 2019.
4. Bistarelli S. A Suite of Tools for the Forensic Analysis of Bitcoin Transactions: Preliminary Report / Bistarelli S., Mercanti I., Santini F. // Euro-Par Workshops. — 2018.
5. Kedharewsari K. Integration of Big Data & Cloud Computing To Detect Black Money Rotation with Range – Aggregate Queries / Kedharewsari K., Anu M., Rajalakshmi V. // International Journal of Engineering and Technology. — 2016. — 8. — 768-773.
6. Maksutov A. Detection of Blockchain Transactions Used in Blockchain Mixer of Coin Join Type / Maksutov A., Alexeev M., Fedorova N., Andreev D. // 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) . — 2019. — 274-277.
7. Oakley J. Unmasking Criminal Enterprises: An Analysis of Bitcoin Transactions / Oakley J., Worley C., Yu L., Brooks R., Skjellum A.// 13th International Conference on Malicious and Unwanted Software (MALWARE) . — 2018.— 161-166.
8. Plaksiy K. Applying Big Data Technologies to Detect Cases of Money Laundering and Counter Financing of Terrorism / Plaksiy K., Nikiforov A., Miloslavskaya N. // 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). — 2018. — 70-77.

9. Maniraj S.P. Credit Card Fraud Detection using Machine Learning and Data Science / Maniraj S.P., Aditya S., Shadab A., Swarna S. // International Journal of Engineering Research. — 2019.
10. Dornadula V.N. Credit Card Fraud Detection using Machine Learning Algorithms, / Dornadula V.N., Geetha S. // Procedia Computer Science. — 2019. —165. — 631-641.
11. Lebichot B. Deep-Learning Domain Adaptation Techniques for Credit Cards Fraud Detection / Lebichot B., Le Borgne YA., He-Guelton L., Oble F., Bontempi G. // Recent Advances in Big Data and Deep Learning. INNSBDDL 2019. Proceedings of the International Neural Networks Society. — 2020.
12. Carcillo F. Combining unsupervised and supervised learning in credit card fraud detection / Carcillo F., Borgne Y.L., Caelen O., Kessaci Y., Oble F., Bontempi G. // Information Sciences. — 2021. — 557. — 317-331.