На правах рукописи

ВУЛЬФИН Алексей Михайлович

МОДЕЛИ И МЕТОДЫ КОМПЛЕКСНОЙ ОЦЕНКИ РИСКОВ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

Специальность 2.3.6 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени доктора технических наук

Уфа – 2022

Работа выполнена на кафедре вычислительной техники и защиты информации ФГБОУ ВО «Уфимский государственный авиационный технический университет»

Научный руководитель: доктор технических наук, профессор, **Васильев Владимир Иванович**

Официальные оппоненты:

Ажмухамедов Искандар Маратович, доктор технических наук, профессор, ФГБОУ ВО «Астраханский государственный университет», декан факультета цифровых технологий и кибербезопасности

Катасёв Алексей Сергеевич, доктор технических наук, доцент, ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ», профессор кафедры систем информационной безопасности

Шелупанов Александр Александрович, доктор технических наук, профессор, ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники», президент

Ведущая организация: ФГБОУ ВО «Оренбургский государственный университет», г. Оренбург

Защита диссертации состоится 01 июля 2022 г. в 10^{00} часов на заседании диссертационного совета 24.2.427.02 на базе ФГБОУ ВО «Уфимский государственный авиационный технический университет» по адресу: 450008, г. Уфа, ул. К. Маркса, 12.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Уфимский государственный авиационный технический университет» и на сайте *www.ugatu.su*.

Автореферат разослан «___» _____ 2022 года.

Ученый секретарь
диссертационного совета
доктор технически наук, доцент  Виноградова Ирина Леонидовна

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Одним из непременных условий построения эффективной цифровой экономики является обеспечение надежной и безопасной работы современных промышленных предприятий и информационно-телекоммуникационных систем. Непрерывно возрастает сложность киберфизических систем, информационно-управляющих систем промышленных объектов, цифровых АСУ ТП топливно-энергетического комплекса, информационных систем финансового сектора и др. В то же время, как показывает статистика последних лет, существенно возросло число случаев, связанных с попытками или успешной реализацией целенаправленных атак на подобные системы, в том числе объекты критической информационной инфраструктуры (КИИ). Согласно федеральному закону «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ, объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. Глубокое проникновение промышленного Интернета вещей в критическую инфраструктуру и производственный сектор привело к возрастанию тяжести последствий реализации подобных атак. Согласно мнению специалистов, ущерб от кибератак на топливно-энергетическую отрасль достигает в среднем 13,2 млн долларов ежегодно, ожидаемый мировой ущерб от киберпреступлений в 2022 г. составит 9 млрд долларов, также отмечается, что повышение рисков информационной безопасности (ИБ) вынуждает к выработке общих подходов к обеспечению ИБ. Совершенствующаяся нормативно-правовая база в сфере ИБ объектов КИИ и действия регуляторов обуславливают необходимость разработки адекватных новым условиям научно обоснованных моделей, методов и инструментальных средств поддержки принятия решений при управлении рисками ИБ. На сегодняшний день масштабируемой и переносимой методологии не предложено. Согласно Государственной программе «Цифровая экономика Российской Федерации» от 28.07.2017 г. в условиях роста угроз ИБ актуальной является разработка и совершенствование моделей, методов и средств оценки рисков ИБ на основе анализа структурированных и слабоструктурированных данных для обеспечения устойчивости объектов КИИ на всех уровнях информационного пространства.

Степень разработанности темы исследований. Исследованиям в области управления рисками ИБ посвящены работы таких российских и зарубежных ученых, как: Аралбаев Т.З., Ажмухамедов И.М., Аникин И.В., Боровский А.С., Булдакова Т.И., Васильев В.И., Гузаиров М.Б., Катасёв А.С., Котенко И.В., Макаревич О.Б., Машкина И.В., Мещеряков Р.В., Милославская Н.Г., Остапенко А.Г., Чопоров О.Н., Шелупанов А.А., Ajith A., Jaquith A., Massacci F., Noel S., Salmeron J.L. и др. Рассмотрены общие вопросы реализации риск-ориентированного подхода к обеспечению ИБ сложных и

критических информационных систем, проанализированы лучшие практики управления ИБ промышленных предприятий и корпоративных систем. В то же время, сегодня нет общепринятых методик и подходов к оценке качественных и количественных показателей защищенности (уровня ИБ) объектов КИИ, обладающих многоуровневой иерархической архитектурой и многообразием применяемых ИТ, средств автоматизации управления и контроля технологических процессов (ТП), разветвленными системами телекоммуникаций и т.п. Существующие подходы направлены, как правило, на решение частных задач защиты информации, отдельных слабо связанных между собой направлений и технических решений, что затрудняет их применение для современных высокотехнологичных объектов КИИ.

Анализ существующих подходов показал, что решение этой проблемы возможно на основе комплексирования и адаптации методов интеллектуального анализа данных (ИАД) и технологий когнитивного моделирования. Разработка в рамках данного подхода научно обоснованной методологии (т.е. совокупности образующих ее элементов – концепции, моделей, методов, алгоритмов и методик) оценки рисков ИБ в составе процесса управления рисками ИБ объектов КИИ позволит получить объективную оценку уровня защищенности этих объектов в условиях воздействия возможных внешних и внутренних угроз, оценить последствия (ущерб) от воздействия этих угроз и предложить адекватные защитные меры по снижению существующих (или потенциально возможных) рисков ИБ с учетом требований существующих нормативных документов. Применение методов ИАД должно обеспечить повышение оперативности и достоверности результатов комплексной оценки уровня защищенности объектов КИИ (рисков ИБ) с учетом имеющейся неопределенности, т.е. неполноты и нечеткости исходной информации об угрозах, уязвимостях и последствиях возможных атак, наличия субъективных факторов при принятии решений об оценке рисков ИБ и выборе эффективных контрмер по защите объектов КИИ от воздействия злоумышленников и других деструктивных факторов. Известные публикации, связанные с оценкой рисков ИБ с помощью технологий ИАД и методов машинного обучения, касаются лишь отдельных аспектов, прежде всего, качественной оценки уровня защищенности и не допускают возможности их прямого распространения на задачи комплексной оценки рисков ИБ объектов КИИ.

Объект исследования – многоуровневая распределенная информационно-управляющая система (объект КИИ), включая входящие в его состав средства защиты информации с инструментами координации, стратегического целеполагания, распределения ресурсов и принятия решений.

Предмет исследования – модели и методы комплексной оценки рисков ИБ в составе процесса управления рисками ИБ объектов КИИ на основе методов интеллектуального анализа данных и технологий когнитивного моделирования.

Цель работы – повышение достоверности и оперативности технологий и процедур комплексной оценки рисков ИБ объектов КИИ на основе методологии когнитивного моделирования и методов машинного обучения.

Для достижения этой цели в диссертации поставлены и решены следующие **задачи**:

1. Системный анализ проблемы комплексной оценки рисков ИБ объектов КИИ, выработка концепции ее решения.
2. Разработка проблемно-ориентированных моделей параметризации угроз и уязвимостей объектов КИИ.
3. Разработка и исследование метода и алгоритмов качественной оценки рисков ИБ объектов КИИ на основе технологий семантического анализа текстовых описаний угроз и уязвимостей.
4. Разработка и исследование метода и алгоритмов количественной оценки рисков ИБ объектов КИИ на основе когнитивного моделирования.
5. Разработка и исследование метода и алгоритмов оценки рисков ИБ объектов КИИ на основе выявления аномалий их состояния с помощью интеллектуального анализа временных рядов.
6. Разработка архитектуры исследовательского прототипа интеллектуальной системы поддержки принятия решений (ИСППР) по оценке рисков ИБ объектов КИИ и анализ результатов применения ИСППР при решении ряда прикладных задач по оценке уровня защищенности конкретных промышленных объектов и организаций.

Основные научные результаты, выносимые на защиту

1. Концепция комплексной оценки рисков ИБ объектов КИИ с применением технологий нечеткого когнитивного моделирования и методов машинного обучения.
2. Комплекс проблемно-ориентированных моделей параметризации угроз и уязвимостей, приводящих к нарушению ИБ объектов КИИ и их подсистем.
3. Метод, алгоритмы и методика качественной оценки рисков ИБ объектов КИИ с использованием технологий семантического анализа текстовых описаний угроз и уязвимостей.
4. Метод, алгоритмы и методика количественной оценки рисков ИБ объектов КИИ с использованием технологий нечеткого когнитивного моделирования.
5. Метод и алгоритмы оценки рисков ИБ объектов КИИ на основе выявления аномалий их состояния с помощью интеллектуального анализа временных рядов.
6. Комплекс алгоритмического и программного обеспечения исследовательского прототипа интеллектуальной системы поддержки принятия решений по оценке рисков ИБ объектов КИИ и результаты ее применения при решении прикладных задач.

Научная новизна результатов

1. Концепция комплексной оценки рисков ИБ объектов КИИ, основанная на интеграции технологий нечеткого когнитивного

моделирования и методов машинного обучения. Отличается применением комплекса проблемно-ориентированных моделей, методов и алгоритмов к проблеме комплексной оценки рисков ИБ объектов КИИ, что позволяет повысить оперативность и снизить эффект неопределенности от влияния субъективных факторов.

2. Комплекс проблемно-ориентированных моделей параметризации угроз и уязвимостей объектов КИИ основан на использовании технологий интеллектуального анализа угроз, уязвимостей и обнаружения аномалий в накапливаемых данных мониторинга состояния объектов, и отличается:

- технологией анализа текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения, на основе эффективного использования дополнительной информации из открытых баз знаний, что позволяет сократить трудозатраты на анализ баз знаний угроз и уязвимостей и повысить оперативность выполнения основных этапов комплексной оценки рисков ИБ;
- составом и структурной организацией (адаптивный выбор и динамическое конфигурирование моделей с учетом имеющихся ограничений, требований точности и достоверности оценок) ансамбля гетерогенных моделей машинного обучения при оценке степени опасности уязвимостей и построении детекторов аномалий, что позволяет повысить достоверность и оперативность обнаружения скрытых зависимостей в накапливаемых данных.

3. Метод, алгоритмы и методика качественной оценки рисков ИБ объектов КИИ, основанные на использовании технологий семантического анализа текстовых описаний угроз и уязвимостей, отличаются способом формализации слабоструктурированных текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения, с помощью гетерогенных нейросетевых моделей вложений в виде графовой семантической модели, что позволяет обеспечить выявление потенциальных угроз, уязвимостей и сценариев реализации атак с возможностью их ранжирования по приоритетам, а также автоматизировать и повысить оперативность основных этапов процесса оценки рисков ИБ.

4. Метод, алгоритмы и методика количественной оценки рисков ИБ объектов КИИ, основанные на построении иерархии вложенных нечетких когнитивных карт, отличаются:

- построением укрупненной когнитивной карты с последующей ее декомпозицией с учетом структурно-функциональной организации объекта КИИ на ряд вложенных НКК соответствующих уровней детализации, что позволяет последовательно раскрывать внутреннюю структуру (топологию) базовых концептов исходной НКК с учетом совокупности объективных и субъективных факторов неопределенности;
- сценарным моделированием сложных многошаговых целенаправленных кибератак с использованием базы меташаблонов атак с дальнейшей формализацией в виде иерархической НКК для

возможности анализа с требуемым уровнем детализации (инкапсуляция структурно-функциональной организации выделенной зоны в виде укрупненного концепта НКК) и количественной оценкой рисков ИБ;

- возможностью комплексной оценки различных аспектов функционирования объектов КИИ с применением технологий интеллектуального анализа данных, что позволяет повысить достоверность итоговых количественных оценок риска ИБ с учетом разброса исходных экспертных оценок.

5. Метод и алгоритмы оценки рисков ИБ объектов КИИ на основе обнаружения аномалий временных рядов накапливаемых параметров, характеризующих состояние сложных технических объектов, сетевого трафика промышленных сетей и поведения пользователей конечных систем, отличающиеся применением комплекса адаптивных нейросетевых моделей для представления паттернов состояний, алгоритмов адаптивной сегментации временных рядов накапливаемых параметров и ассемблированием гетерогенных детекторов аномалий, применение которых позволяет повысить достоверность и оперативность поиска скрытых зависимостей в накапливаемых данных и повысить достоверность результатов оценивания рисков ИБ путем уточнения априорных экспертных вероятностей реализации угроз и эксплуатации уязвимостей.

Теоретическая значимость. Значение результатов для теории комплексной оценки рисков информационной безопасности объектов КИИ заключается в том, что предложены: концепция комплексной оценки рисков ИБ объектов КИИ, основанная на интеграции технологий нечеткого когнитивного моделирования и методов машинного обучения; комплекс проблемно-ориентированных моделей параметризации угроз и уязвимостей объектов КИИ; метод, алгоритмы и методика качественной оценки уровня рисков ИБ объектов КИИ на основе использования технологий семантического анализа текстовых описаний угроз и уязвимостей; метод, алгоритмы и методика количественной оценки рисков ИБ объектов КИИ на основе построения иерархии вложенных когнитивных карт; метод и алгоритмы оценки рисков ИБ объектов КИИ на основе обнаружения аномалий временных рядов накапливаемых параметров, характеризующих состояние этих объектов, сетевого трафика промышленных сетей и поведения пользователей конечных систем.

Практическая значимость. Разработано алгоритмическое, программное и методическое обеспечение исследовательского прототипа ИСППР по оценке рисков ИБ объектов КИИ, в составе которой реализован набор предложенных подсистем и модулей. В частности, модель параметризации и оценки семантической близости текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения объектов КИИ, позволяет сократить в 7-10 раз объемы просматриваемых экспертом данных и уменьшить время анализа в 10-12 раз с помощью префильтрации этих данных. Применение модели оценки степени опасности новых уязвимостей на основе прогнозирования набора метрик

позволяет получить оценку степени их опасности (и набора ее метрик). Семантическая модель текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения зоны безопасности объекта КИИ, предназначена для автоматизации низкоуровневого моделирования сценариев эксплуатации уязвимостей и реализации угроз на основе описания шаблонов компьютерных атак, и позволяет снизить трудоемкость формирования перечня актуальных угроз. Применение способа мониторинга целостности данных, получаемых с бортовых систем мобильного объекта, позволило снизить оценку риска ИБ для рассматриваемой системы на 45 % и обеспечить оценку вероятности успешного распознавания атаки с помощью системы мониторинга целостности данных на уровне 0,85-0,98. Предложенные решения по цифровому профилированию и анализу совокупности отпечатков (fingerprints) пользовательских окружений и динамических пользовательских профилей обеспечивают точность определения удаленного управления на уровне 93 % и точность классификации мошеннических операций на уровне 81 %. Предложенные решения в задачах обнаружения аномалий сетевого трафика в гетерогенных промышленных сетях позволяют добиться оценки F_1-меры на уровне 96 %, алгоритмы обнаружения аномалий в данных мониторинга состояния АСУ ТП нефтедобычи позволяют корректно классифицировать до 78-95 % состояний, в том числе вызванных воздействием злоумышленника.

Методы исследования. При решении поставленных в диссертационной работе задач использовались методы системного анализа, математического и когнитивного моделирования; методы семантического анализа, нейронных сетей и машинного обучения; методы оценки рисков ИБ, обнаружения аномалий временных рядов.

Достоверность полученных результатов. Предложенные в диссертационной работе решения подтверждаются результатами сравнительного анализа эмпирической информации и данных, полученных в результате математического и когнитивного моделирования, непротиворечивостью полученных результатов, а также экспертной оценкой и степенью повторяемости полученных результатов.

Социально-экономический эффект от внедрения результатов работы заключается в снижении трудоемкости процессов обработки и анализа больших объемов слабоструктурированных данных в базах знаний угроз и уязвимостей, а также повышении обоснованности выбора средств и мер защиты объектов КИИ.

Реализация и внедрение результатов работы. Работа выполнена в рамках реализации гранта Минобрнауки России (грант ИБ) (проект № 1/2020), грантов РФФИ (№№ 14-08-01182, 16-07-00243, 17-07-00351, 17-08-01569, 17-48-020095, 19-07-00972, 20-08-00668) и договоров с ООО «Фродекс», с АО УНПП «Молния» и с ОАО «Уфимский НТЦ».

Результаты диссертационной работы внедрены и активно используются в ряде организаций и учреждений различного профиля: ООО «Фродекс», ООО «Инженерный центр систем безопасности», ООО Научно-производственное

предприятие «Полигон», ЗАО «Республиканский центр защиты информации», ООО «Уфимский НТЦ», ФГБОУ ВО «УГАТУ».

Апробация работы. Основные теоретические положения и практические результаты работы докладывались и обсуждались на научно-технических конференциях, в том числе на: Всероссийской научно-технической конференции «Нейроинформатика», Москва, РФ, (2010, 2013, 2015 гг.); Международной научной конференции «Computer Science and Information Technologies» (2010, Moscow-Saint-Petersburg, Russia; 2014 Sheffield, UK; 2017, Baden-Baden, Germany); Международной конференции «Информационные технологии интеллектуальной поддержки принятия решений», Уфа, РФ, (2014, 2017, 2018, 2019, 2020); Международной научно-технической конференции «International Conference on Industrial Engineering, Applications and Manufacturing», (2017, Saint-Petersburg, Russia, 2018, Moscow, Russia); IEEE International Symposium on Signal Processing and Information Technology (2017, Bilbao, Spain); Международной конференции и молодежной школе «Информационные технологии и нанотехнологии» (2018, 2019, 2020, 2021, Самара, РФ); Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства» (2018, Ставрополь, РФ); Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (2019, Ставрополь, РФ); International Conference on Electrotechnical Complexes and Systems (2019, 2020, 2021, Ufa, Russia); Всероссийской научной конференции с международным участием «Информационные технологии и системы» (2019, Ханты-Мансийск, РФ); Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (с приглашением зарубежных ученых) (2019, 2020, Ставрополь, РФ); International Conference on Applied Innovations in IT (2020, Koethen, Germany); Information Technologies and Intelligent Decision Making Systems (2021, Moscow, Russia); Международной научно-практической конференции «Приоритетные направления развития науки и технологий» (2021, Тула, Россия); IFAC Conference on Technology, Culture and International Stability (2021, Moscow, Russia).

По проблеме диссертационного исследования опубликовано 74 работы, в том числе: 24 статьи в ведущих рецензируемых научных журналах, входящих в перечень изданий, рекомендованных ВАК, 19 публикаций в отечественных и зарубежных изданиях, индексируемых международными системами Scopus и Web of Science (из них, 2 – Q2); 2 коллективные монографии, изданные в России и за рубежом, 1 патент на изобретение; 17 свидетельств о государственной регистрации программы для ЭВМ, 11 трудах конференций и других работах.

Сведения о личном вкладе автора. Решение задач, сформулированных в диссертационной работе, выполнено автором лично. В работах, выполненных в соавторстве, диссертант внес основной вклад в разработку методов, моделей, алгоритмов, методик и программного обеспечения.

Структура и объем работы. Диссертационная работа состоит из введения, шести глав, заключения, списка использованных источников, приложений. Основной текст диссертации изложен на 287 страницах, содержит 112 рисунков и 72 таблицы. В приложениях на 98 страницах содержатся поясняющие таблицы и материалы внедрения. Библиографический список включает в себя 330 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность проблемы исследования, приведены основные научные положения и результаты.

В первой главе проведен анализ современного состояния в области комплексной оценки рисков ИБ объектов КИИ.

Выполнен анализ нормативно-правого обеспечения проблемы обеспечения ИБ объектов КИИ. Выполнен анализ методов качественной и количественной оценки рисков ИБ объектов КИИ с использованием технологий интеллектуального анализа данных. Отмечается, что существующие подходы направлены, как правило, на решение частных задач, отдельных поддающихся анализу направлений и решений, что затрудняет их применение для современных высокотехнологичных объектов КИИ. Предложена концепция комплексной оценки рисков ИБ объектов КИИ с применением технологий нечеткого когнитивного моделирования и методов машинного обучения, заключающаяся в:

–проведении системного анализа проблемы безопасности киберфизических объектов в пределах единой информационной среды (киберпространства) и оценке потенциального ущерба (последствий) для физического мира и человека;

–автоматизации сбора и анализа индикаторов угроз из множества каналов (источников) и выявлении потенциальных угроз, уязвимостей и векторов атак на основе оценки семантической близости их текстовых описаний с возможностью ранжирования (присвоения уровня критичности) и приоритезации для последующего структурирования, консолидации и обогащения накопленной информации об уязвимостях информационной инфраструктуры и ее компонент, выявлении наиболее успешных сценариев реализации атак и оценки их последствий для объектов КИИ на основе взаимодействия с внешними базами знаний;

–автоматизации сбора и анализа статистических данных о событиях информационной безопасности с построением прямых связей между выявленными уязвимостями и угрозами безопасности информации для анализируемой информационной системы (объекта КИИ) на основе методов анализа слабоструктурированных текстовых описаний и интеграцией с существующими банками данных об угрозах и уязвимостях программного и аппаратного обеспечения;

–когнитивном моделировании как средстве реализации системного риск-ориентированного подхода к количественной оценке рисков ИБ объекта

КИИ путем построения иерархии вложенных когнитивных моделей в базисе интервальных чисел, с возможностью анализа различных сценариев воздействия внутренних и внешних злоумышленников и с учетом накопленных данных о состоянии объекта;

–получении оценок рисков ИБ объекта КИИ на основе обнаружения аномалий временных рядов накапливаемых параметров, характеризующих состояние объектов, сетевого трафика промышленных сетей и поведения пользователей конечных систем, основанных на построении нейросетевых моделей объекта и последующей оценке согласованности модельных данных и поведения объекта.

Во второй главе осуществляется разработка и исследование моделей параметризации множеств угроз и уязвимостей, приводящих к нарушению ИБ объектов КИИ и их подсистем.

В соответствии с рекомендациями ГОСТ 62443, реализация системного риск-ориентированного подхода к обеспечению ИБ осуществляется на основе декомпозиции (сегментации) инфраструктуры объектов КИИ на относительно независимые выделенные локальные зоны безопасности и связывающие их тракты с учетом требований к уровню их безопасности.

Качественная и количественная оценка рисков ИБ объекта КИИ, согласно ГОСТ 27005 и 62443, базируется на трехфакторной формуле оценки рисков ИБ, и определяется как произведение $C_{\text{ущ}_i}$ потенциального ущерба (последствия), наносимого *i*-ому информационному ресурсу выделенной зоны безопасности (в относительных единицах к ценности актива) на вероятность $P_{\text{угр}_j}$ возникновения *j*-й угрозы и вероятность $P_{\text{уязв}_k}$ использования *k*-й уязвимости: $R_i = P_{\text{угр}_j} \cdot P_{\text{уязв}_k} \cdot C_{\text{ущ}_i}$.

При оценке рисков ИБ необходимо определить целевые и достигнутые уровни безопасности, определяемые для каждой зоны безопасности, на основе анализа архитектуры объекта КИИ, идентификации и классификации активов, подлежащих защите, и параметризации угроз и уязвимостей. Следовательно, необходим иерархический комплекс моделей, позволяющих учитывать не только вероятность нарушения безопасности и ее проявления, но и оценивать эффективность контрмер, учитывать выявление новых уязвимостей, эволюцию угроз и методов атак – т.е. эволюцию объекта защиты и необходимость уточнения оценок вероятностей реализации угроз и эксплуатации уязвимостей, а также реализацию опережающей стратегии защиты (проактивная защита), основанной на предсказании угроз (предиктивный анализ) и раннем обнаружении атак с целью адаптации системы к предполагаемому деструктивному воздействию. Предлагаемые модели должны обеспечивать агрегацию оценок рисков ИБ в пределах выделенных зон и возможность перехода к интегральным оценкам рисков ИБ для укрупненных зон анализа с возможностью выбора оптимального (рационального) способа защиты информации с учетом ограничений на величину рисков и выделяемых ресурсов на реализацию контрмер.

Для комплексной оценки риска ИБ объекта КИИ необходимо решение задач оценки состава потенциальных угроз ИБ, уязвимостей и сценариев реализации атак с возможностью их ранжирования по приоритетам (присвоения уровня критичности) и выбором рационального состава защитных мер. Для решения этих задач в работе рекомендовано использовать существующие открытые базы знаний угроз (Threat Intelligence) и уязвимостей (Vulnerability Intelligence), которые содержат полученные из различных источников систематизированные текстовые описания аспектов безопасности программного и аппаратного обеспечения информационной инфраструктуры, консолидированные в виде слабосвязанных групп иерархических гипертекстовых документов в отдельных базах данных (БДУ ФСТЭК России, CAPEC, ATT&CK, OWASP, STIX, WASC и др.).

Для автоматизации поиска и анализа баз знаний предложена **модель параметризации и оценки семантической близости текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения объектов КИИ (рис. 1)**. После предобработки текстовых описаний (D) и построения словаря W (множество уникальных термов) формируется разреженная матрица B (1) вхождений термов (w_i) в текстовое представление ($d_j \in D$). С помощью предобученных нейросетевых моделей NN_1 и NN_2 (2) строятся векторные вложения на уровне термов (Word2Vec) и на уровне текстовых описаний (Doc2Vec), которые позволяют сформировать гетерогенный вектор признаков (4) мультиязычного текстового описания с учетом (3) статистической меры оценки важности термов (T_F, I_{DF}). Выходом модели (5) является разреженная матрица S семантической близости текстовых описаний.

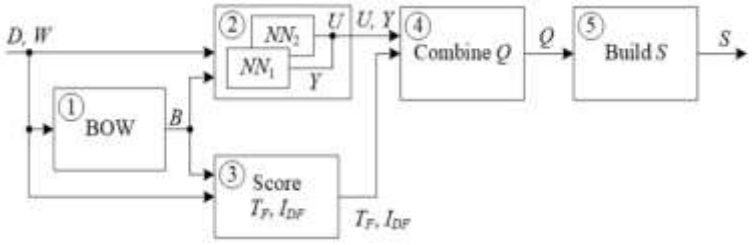


Рисунок 1 – Модель параметризации и оценки семантической близости текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения объектов КИИ

D – множество текстовых описаний; W – множество уникальных термов; B – разреженная матрица вхождений термов; NN_1, NN_2 – Word2Vec и Doc2Vec модели; U, Y – формализованные векторы вложений; Q – гетерогенный вектор признаков; S – разреженная матрица семантической близости; T_F-I_{DF} – статистическая мера оценки важности термов; BOW – словарь вхождений термов

Применение модели позволяет сократить в 7-10 раз объемы просматриваемых экспертом данных и уменьшить в 10-12 раз время анализа при оценке опасности выявленных уязвимостей и релевантных им угроз нарушения ИБ с помощью префильтрации на основе технологий интеллектуального анализа текстов, тем самым повышая продуктивность работы специалиста.

Разработана **модель количественной оценки степени опасности новых уязвимостей (рис. 2)**, для которых экспертная оценка метрики CVSS (Common Vulnerability Scoring System 2 и 3 версии) еще не определена, на основе прогнозирования набора метрик с помощью анализа текстового описания. Предложено два подхода для количественной оценки базовой

метрики CVSS опасности уязвимостей по формализованному текстовому описанию: построение ансамбля предикторов для оценки отдельных значений набора метрик с последующим расчетом результирующего значения и построение ансамбля регрессоров для непосредственной количественной оценки результирующего значения метрики CVSS. Ансамбль моделей позволяет получить оценку метрик опасности уязвимости CVSS на уровне F_1 = 0,80-0,85 и оценку MSE =0,865 для ансамбля регрессоров.

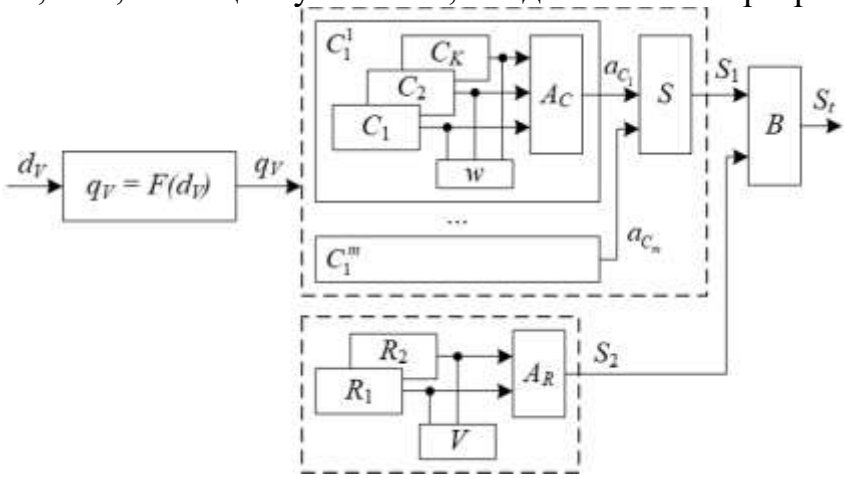


Рисунок 2 – Ансамбль моделей для прогнозирования базовой метрики оценки степени опасности уязвимости на основе формализованного текстового описания

d_V – текстовое описание уязвимости, q_V – формальный вектор признаков текстового описания; C – ансамбль моделей-классификаторов набора метрик; R – модели-регрессоры количественной оценки степени опасности уязвимости; A – модули согласования моделей ансамбля; w, v – весовые коэффициенты моделей в составе ансамбля; S – оценки степени опасности уязвимости; B – блок итоговой количественной оценки степени опасности уязвимости.

Для автоматизации низкоуровневого моделирования сценариев эксплуатации уязвимостей и реализации угроз на основе описания шаблонов компьютерных атак, содержащихся в базах знаний (БДУ ФСТЭК России, CAPEC, MITRE и ATT&CK), характеризующих различные аспекты безопасности программного и аппаратного обеспечения, предложена **семантическая модель текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения (рис. 3)** зоны объекта КИИ, в виде графа

$$G = \{V, E, D\},$$

где V – множество вершин графа – текстовые описания;

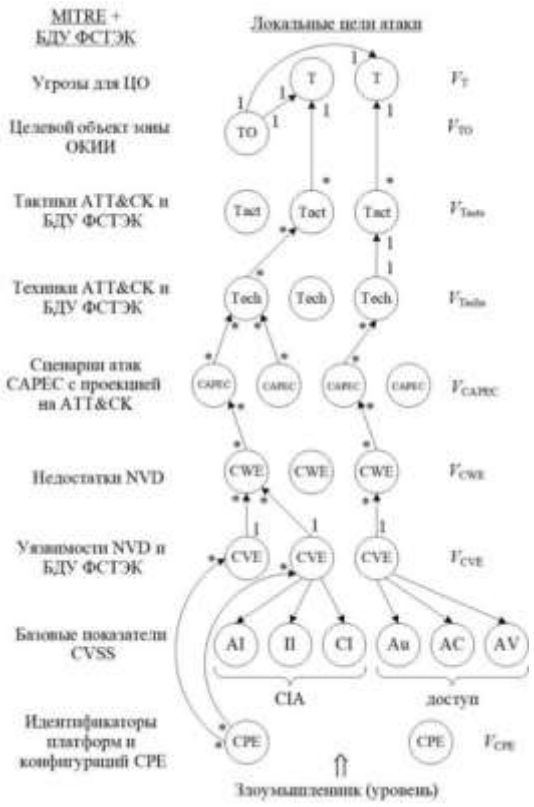
$$V = V_{CPE} \cup V_{CVE} \cup V_{CWE} \cup V_{CAPEC} \cup V_{Techs} \cup V_{Tackts} \cup V_{TO} \cup V_T,$$

E – множество взвешенных ориентированных ребер, устанавливающих отношения между текстовыми описаниями:

$$E \subseteq V \times V, \quad e(v_i, v_j), \quad v_i, v_j \in V,$$

$D(e)$ – функция, определяющая степень семантической близости для концептов $v_i, v_j \in V$.

Модель позволяет формализовать логическую цепочку: «множество выявленных уязвимостей программного обеспечения → множество релевантных угроз → множество наиболее вероятных сценариев реализации угроз → возможные киберфизические последствия» с учетом требований нормативных документов ФСТЭК России. Использование модели позволяет снизить трудоемкость формирования перечня актуальных угроз и уязвимостей за счет префильтрации несвязанных или недостижимых вершин (угроз).



V_{CPE} – идентификаторы платформ и конфигураций для программно-аппаратного обеспечения;
V_{CVE} – идентификаторы выявленных уязвимостей для каждого компонента;
V_{CWE} – текстовые описания CWE, представляющие недостатки (слабые места) программного и аппаратного обеспечения;
V_{CAPEC} – металшаблоны CAPEC, описывающим известные типовые атаки;
V_{Techs} – техники реализации атаки, которые описывают инструменты, технологии, утилиты и т.д., используемые нарушителями;
V_{Tackts} – тактики, т.е. действиям на разных этапах реализации атаки;
V_{TO} – объекты воздействия;
V_T – угрозы;

Рисунок 3 – Семантическая модель текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения объектов КИИ в задаче анализа актуальных угроз и уязвимостей

На этапе анализа сценариев реализации угроз с возможностью установки приоритетов мер по их устранению необходимо обеспечение видимости и контекста потенциальной атаки за счет агрегации и анализа данных из множества источников, характеризующих состояние подсистем объекта КИИ. Предложена **модель обнаружения аномалий состояния объектов и сущностей в зоне анализируемого объекта КИИ (рис. 4)**, основанная на применении методов машинного обучения и интеллектуального анализа собираемых данных мониторинга состояния объектов и сущностей в виде многомерных временных рядов.

Многомерные временные ряды (МВР) представляют собой последовательность измерений, собранных с датчиков в зоне безопасности объекта КИИ. Аномалии представляют собой отрезки временного ряда с соотнесенными событиями состояния объекта. Применение адаптивного оконного анализа позволяет выделять непрерывные подпоследовательности ВР, для которых выполняется процедура построения признакового описания на основе статистических функций, параметрических моделей, приближающих сегмент ВР, семейства регрессионных и нейросетевых авторегрессионных моделей. Гетерогенная модель ансамбля детекторов для обнаружения аномалий в МВР включает детекторы на основе нейросетевых автоенкодеров (NAE) с долгой-краткосрочной памятью (LSTM), модели оценки выбросов с автоподстройкой порога (LOF-детектор), модели обнаружения аномалий на основе изолирующего леса (IFO-детектор). Для создания модели обнаружения аномалий используются данные о штатном функционировании объекта или подсистемы для построения модели нормального функционирования, либо имеющаяся модель (математическая,

полунатурная). Модель может быть использована для обнаружения аномалий состояния объекта КИИ, пользователя конечной системы и пользовательского окружения объекта КИИ.

Рисунок 4 – Модель обнаружения аномалий состояния подсистем в зоне объекта КИИ

С целью параметризации и оценки угрозы нарушения конфиденциальности и целостности информации и оценки соблюдения требований политики ИБ объекта КИИ разработан **комплекс моделей анализа поведения пользователей конечной системы (рис. 5)**, включающий:

– построение цифрового отпечатка (ЦО) пользователя (модель пользовательского окружения конечной системы и модель динамического профиля взаимодействия пользователя с конечной системой);

– профилирование состояния пользователя.

Рисунок 5 – Комплекс моделей обнаружения аномалий поведения пользователя и пользовательского окружения

A – ЦО пользовательского окружения при работе с Web-системой, B – ЦО динамических биометрических признаков пользовательского сеанса; D – ЦО динамического профиля пользователя (характер действий в удаленной системе), V – образ автоматического профилирования пользователя (видеоаналитика); M – модели обнаружения аномалий;

После параметризации и формирования перечня актуальных угроз и уязвимостей с помощью предложенных моделей для каждой из выделенных зон безопасности объекта КИИ осуществляется переход к построению и последующему анализу иерархии нечетких когнитивных карт с целью формирования обоснованной качественной и количественной оценки показателей рисков ИБ объекта КИИ.

В работе используются когнитивные модели на основе: традиционных нечетких когнитивных карт (НКК), нечетких продукционных когнитивных карт (НПКК), обобщенных интервально-значных НКК (серые и интуиционистские НКК).

НКК – это ориентированный граф, заданный с помощью кортежа множеств: НКК $=< C, F, W >$, где $C = \{C_i\}$ – множество концептов; $F = \{F_k\}$ – множество направленных дуг графа; $W = \{W_{ij}\}$ – множество весов связей НКК, $X_i(t)$ – значение переменной состояния *i*-го концепта C_i в момент времени *t*, определяемое в общем случае уравнением

$$\tilde{X}_i(t+1) = f\left(\tilde{X}_i(t) \oplus \left(\sum_{\substack{j=1 \\ (j\neq i)}}^{n} \oplus \tilde{W}_{ji} \otimes \tilde{X}_j(t)\right)\right),\ (i = 1,2,\dots,n), \quad (2)$$

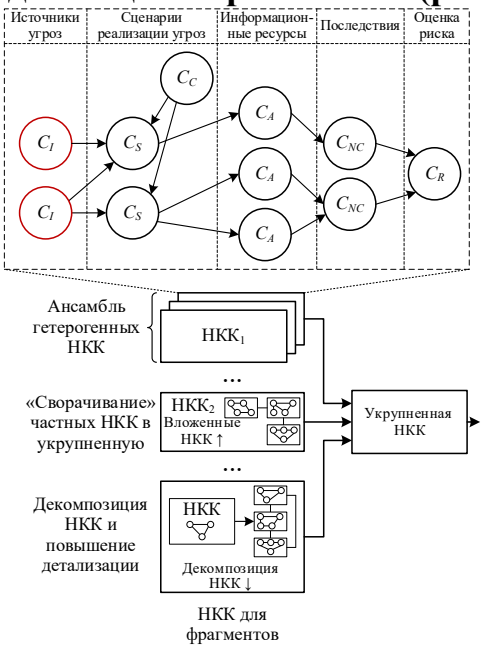
где веса связей $\tilde{W}_i$ и переменные состояния $\tilde{X}_i(t)$ представляют собой интервальные числа, определяемые как элементы нечетких интервальных множеств; $\oplus$ и $\otimes$ – операции сложения и умножения интервальных чисел, заданные на нечетких интервальных множествах; f – нелинейная функция активации концепта.

В качестве основы для построения НКК использованы способы задания интервальных нечетких множеств: серые числа, интуиционистские числа. Под серым множеством $A \subseteq X$ понимается множество

$$A = \{< x, [\underline{x}, \overline{x}] > | x \in X\}, \quad (3)$$

элементами которого являются серые числа $x \in [\underline{x}, \overline{x}] \leq A$, $[\underline{x}, \overline{x}] \in [0,1]$, где $\underline{x}$ и $\overline{x}$ – нижняя и верхняя граница серого числа x; X – универсальное множество. Веса связей между концептами серой НКК задаются в виде серых чисел $[\underline{W_{ij}}, \overline{W_{ij}}]$; переменные состояния концептов – серые числа $[\underline{X_i}, \overline{X_i}]$.

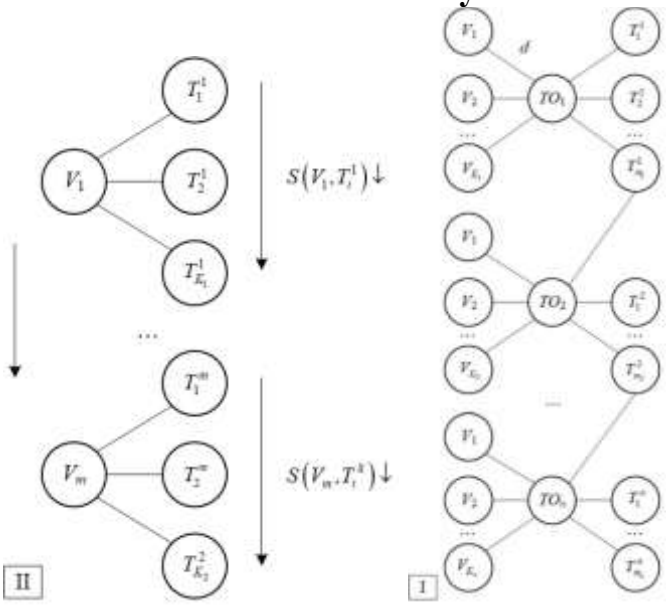
Рассмотрены особенности применения НПКК для решения задачи оценки рисков ИБ. Используется описание взаимодействия между концептами с помощью системы нечетких правил, отражающих знания и опыт экспертов предметной области. Предполагается, что переменная состояния X_i каждого концепта C_i рассматривается как лингвистическая переменная, принимающая значения из нечеткого терм-множества $\{T_{i1}, T_{i2}, \dots, T_{im}\}$, подмножества (термы) которого $T_{ik}, (k = 1,2,\dots,m)$, в свою очередь, задаются функциями принадлежности: $T_{ik} = (\mu_{ik}(X_i), X_i), \mu_{ik}: X_i \to [0,1]$, где $X_i \in [0,1]$ или $X_i \in [-1,1]$. Предложена **общая схема построения нечеткой когнитивной модели оценки рисков ИБ (рис. 6)**:



1. Определение множества концептов, характеризующих:
1.1. C_{NC} – негативные последствия реализации угроз ИБ для объекта КИИ;
1.2. C_A – информационные ресурсы объекта КИИ;
1.3. C_I – источники угроз;
1.4. C_S – угрозы нарушения ИБ и сценарии их реализации (тактики и техники);
1.5. C_R – оценка риска ИБ;
1.6. C_C – выбор рационального способа защиты с учетом ограничений;
2. Оценка связей между концептами (F) и взаимовлияния концептов с помощью нечеткой лингвистической шкалы с возможностью учета разброса мнений экспертов (W);
3. Декомпозиция НКК и вложение частных НКК, построение ансамблей НКК для достижения требуемого уровня детализации представления;
4. Моделирование и количественная оценка рисков ИБ;
5. Выбор рационального способа и средств защиты объекта КИИ с учетом требований нормативной базы и имеющихся ограничений.

Рисунок 6 – Обобщенная схема построения нечеткой когнитивной модели оценки рисков ИБ объекта КИИ

В третьей главе осуществляется разработка метода и алгоритмов комплексной оценки рисков ИБ объекта КИИ на основе семантического анализа текстовых описаний угроз и уязвимостей. На основе предложенной в работе модели оценки семантической близости текстовых описаний разработан **метод ранжирования по приоритетам угроз с учетом зависимостей между угрозами и выявленными для каждой зоны безопасности объекта КИИ уязвимостями (рис. 7)**.



а) б)

Рисунок 7 – а) Список актуальных уязвимостей, ранжированных по степени критичности, и сопоставленные с ними угрозы (в порядке убывания метрики семантической близости), б) соотнесения множества угроз T и уязвимостей V через промежуточные узлы – объекты воздействия TO (TO_j – объект воздействия, $j = \overline{1,n}$; T_j^i – угроза, связанная с TO_j; $i = \overline{1,m_j}$; V_{K_j} – уязвимость, связанная с TO_j)

Для реализации дивизимного (угроза и приводящие к ее реализации уязвимости) и агломеративного (от выявленных уязвимостей к релевантным угрозам) сопоставления устанавливается соответствие $F \subset T \times V$ между элементами множества угроз $T = \{T_1, T_2, \dots, T_l\}$ и множества уязвимостей $V = \{V_1, V_2, \dots, V_t\}$ на основе анализа матрицы S оценок семантической близости текстовых описаний.

Пороговая фильтрация и экспертная корректировка разреженной матрицы позволяет для каждой зоны объекта КИИ построить группу актуальных уязвимостей, ранжированных по степени критичности, и сопоставленных с ними угроз (в порядке убывания метрики семантической близости), а также выполнить соотнесение множества угроз T и уязвимостей V через промежуточные узлы – объекты воздействия TO.

Разработана **архитектура конвейера по обработке текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения объекта КИИ** (рис. 8).

С целью автоматизации сбора индикаторов угроз из множества каналов (источников) и выявления потенциальных угроз, уязвимостей и векторов атак с возможностью их ранжирования (присвоения уровня критичности) для последующего структурирования, выявления наиболее опасных сценариев реализации атак и оценки их последствий на основе предложенных моделей и метода разработана **автоматизированная система анализа угроз и уязвимостей объекта КИИ на основе технологий семантического анализа их текстовых описаний**.

Загрузка данных из локальной БД (1) – преобразование текстовых полей в единое текстовое описание.

Нормализация (2) текстовых описаний угроз и уязвимостей: символьная фильтрация, токенизация и фильтрация с использованием общего и специализированного (формируемого экспертами) «стоп-словарей» и лемматизация.

Экспертная структурно-семантическая разметка (3) текста для выделения семантических особенностей текстовых описаний (ключевые слова, ключевые словосочетания, именованные сущности) и уточнение специализированного «стоп-словаря».

Построение формализованного вектора признаков текстовых описаний (4). Применяемые схемы частотного представления (Bag of Word, BoW), прямого кодирования, скоринга для частотного представления (BoW + TF-IDF) и распределенного представления (с помощью нейросетевых моделей векторных вложений Word2Vec, Doc2Vec) позволяют сформировать гетерогенный вектор признаков текстового описания

На следующем **этапе (5) выполняется отбор наиболее значимых признаков** с помощью экспертной оценки структуры двухмерной визуализации стохастического вложения соседей с t-распределением (TSNE), редуцированного пространства признаков с помощью метода главных компонент (PCA) или приближения и проекции однородного многообразия (UMAP).

Заключительным является **этап (6)** оценки семантической близости текстовых описаний и формирование матрицы попарных расстояний на основе оценки косинус-меры сходства гетерогенный вектор признаков текстового описания.

Рисунок 8 – Архитектура конвейера по обработке текстовых описаний

Система позволяет автоматизировать сбор и обработку накапливаемых с помощью сканеров безопасности данных об обнаруженных уязвимостях. Основной модуль системы реализует метод интеллектуального анализа текстовых описаний аспектов безопасности программного и аппаратного обеспечения информационной инфраструктуры. Применение данной **системы** позволяет осуществить ранжирование по приоритетам угроз с учетом зависимостей между угрозами и выявленными уязвимостями.

Структура системы анализа угроз и уязвимостей объекта КИИ включает в себя следующие основные подсистемы (рис. 9):

- подсистему локального хранения актуальной копии БДУ ФСТЭК России (I);
- подсистему сопоставления угроз и уязвимостей на основе их текстового описания (II);
- подсистему оценки актуальных угроз и уязвимостей для сегмента информационной инфраструктуры (III).

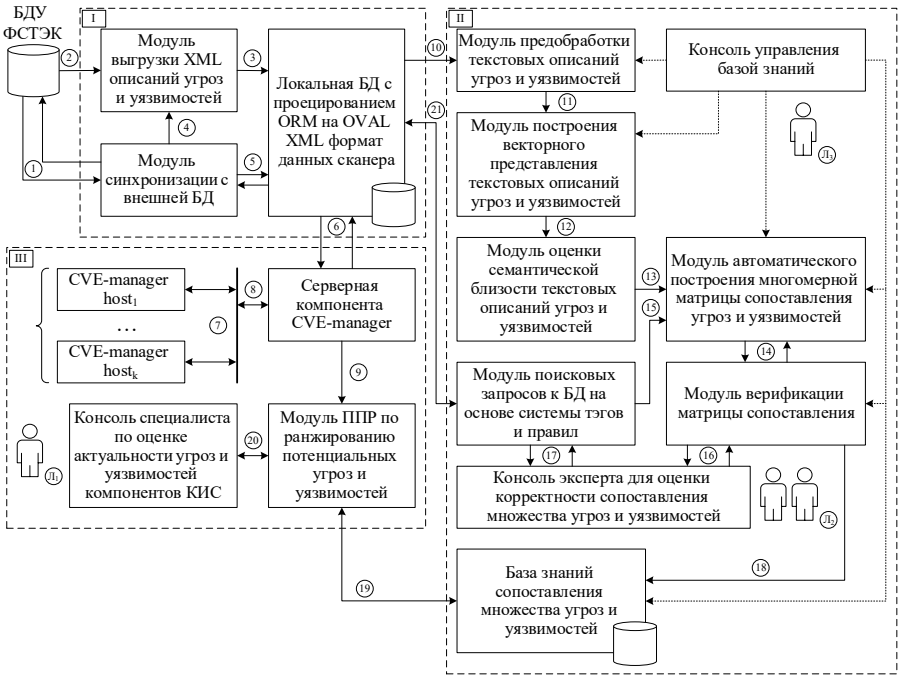


Рисунок 9 – Структурно-функциональная организация системы анализа актуальных угроз и уязвимостей на основе оценки семантической близости их текстовых описаний

Применение системы позволяет:

– автоматизировать процесс сопоставления и ранжирования угроз ИБ для каждой выявленной уязвимости на рабочих станциях и серверах информационной инфраструктуры;

– снизить когнитивную нагрузку на эксперта и повысить достоверность оценки степени опасности уязвимостей ПО за счет использования дополнительной информации о существующих зависимостях между выявленными уязвимостями и потенциальными угрозами;

– масштабировать решение за счет интеграции с существующими БД уязвимостей и формализации знаний экспертов о прецедентах сопоставления угроз и уязвимостей в пополняемой базе.

Разработана **структура системы оценки степени опасности уязвимостей** на основе прогнозирования набора метрик CVSS с помощью анализа текстового описания для повышения точности и оперативности оценки (рис. 10). Первый этап работы системы связан со сбором и агрегацией специализированных новостных рассылок и тематических ресурсов в виде слабоструктурированных текстовых данных для построения документо-ориентированной БД.

Практическая значимость системы обусловлена повышением точности и оперативности оценки метрик опасности уязвимостей с возможностью интеграции в систему аудита и инвентаризации для оперативного принятия мер защиты от новых уязвимостей. Предложена **методика оценки актуальных угроз и уязвимостей программного обеспечения объекта КИИ с использованием методов семантического анализа текстовых описаний.** Завершающий этап предлагаемой методики позволяет перейти к построению когнитивной модели оценки рисков ИБ для объектов КИИ.

Автоматизированное моделирование и оценка актуальности угроз и сценариев их реализации на основе перечня выявленных уязвимостей для всех компонентов КИИ позволяет выявить наиболее вероятные сценарии реализации угроз и оценить последствия от их реализации.

Рисунок 10 – Структура системы оценки степени опасности уязвимостей на основе интеллектуального анализа данных

Для реализации предложенной методики разработана **система построения и анализа семантической модели текстовых описаний объектов зоны безопасности объекта КИИ** (рис. 11)**.**

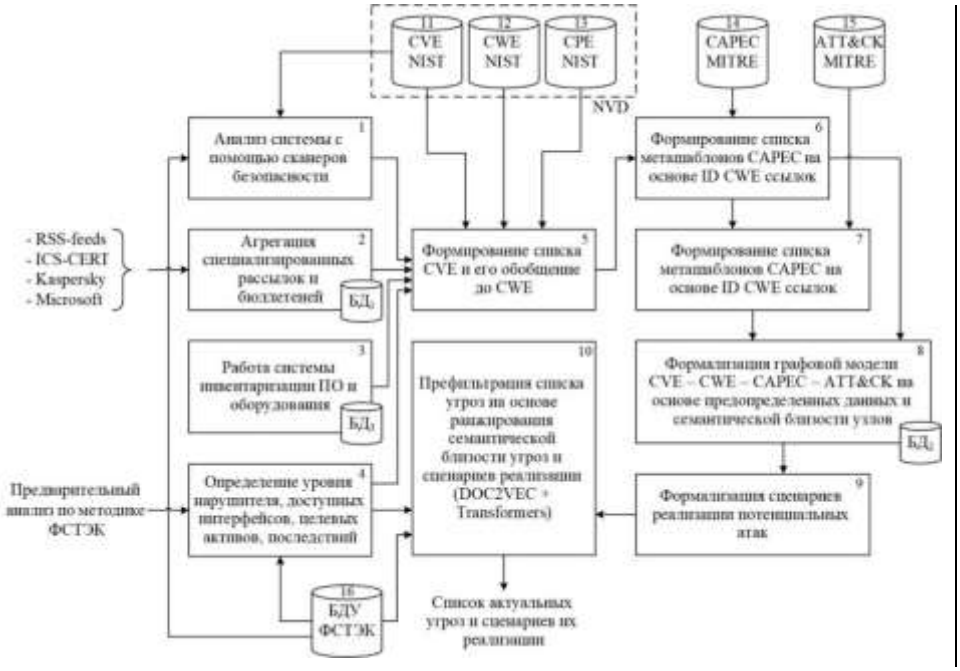


Рисунок 11 – Структура системы построения и анализа семантической модели текстовых описаний объектов зоны безопасности объекта КИИ

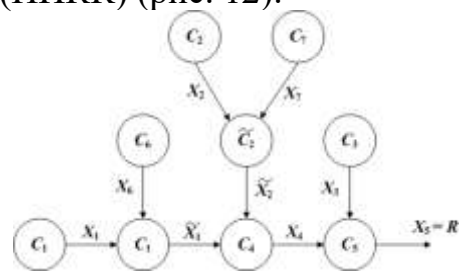
Результирующая НСКК позволяет оценить риски ИБ при реализации воздействия нарушителя на инфраструктуру. Наиболее детализированный уровень НСКК отражает ряд действий нарушителя на каждом этапе реализации угрозы, что позволяет получить детализированную оценку риска ИБ для целевых объектов информационной инфраструктуры.

С учетом трехуровневой архитектуры АСУ ТП нефтедобывающего предприятия построены референсная и зональная модели архитектуры,

выделены зоны безопасности и тракты, построена графовая модель сценариев эксплуатации уязвимостей и реализации угроз для выделенной зоны безопасности АСУ ТП нефтедобывающего предприятия в виде иерархии вложенных НСКК.

В четвертой главе разрабатываются метод и алгоритмы комплексной оценки рисков ИБ объектов КИИ с использованием методов нечеткого когнитивного моделирования и машинного обучения.

Рассмотрен пример решения задачи оценки риска ИБ от реализации вирусной атаки с помощью нечетких продукционных когнитивных карт (НПКК) (рис. 12).



C_1, C_2, C_3 – угроза, уязвимость и информационный ресурс; C_4 и C_5 – реализация угрозы и риск (потенциальный ущерб); C_6 и C_7 – ресурсы, выделяемые на парирование (блокирование) угрозы и устранение уязвимости; $\widetilde{C_1}$ и $\widetilde{C_2}$ – модифицированные (скомпенсированные за счет принятия контрмер) угроза и уязвимость.

Рисунок 12 – Схема НПКК для оценки риска ИБ с учетом контрмер

Рассмотрены особенности применения НСКК для оценки рисков ИБ от нарушения конфиденциальности и целостности информации, вызванных воздействием на информационные активы угроз типа «Несанкционированный доступ» и «Вредоносное программное воздействие/вирусы» (рис. 13).

Для оценки рисков ИБ в зоне безопасности объекта КИИ путем проведения сценарного моделирования предложено построение укрупненной НСКК, с последующей ее декомпозицией на ряд вложенных НКК следующих уровней детализации. При построении вложенных НКК реализовано последовательное раскрытие неопределенностей – каждый последующий слой содержит более детальную (локальную) информацию о внутренней структуре базовых концептов исходной НКК (рис. 13).

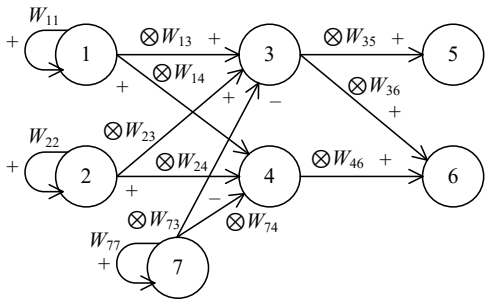
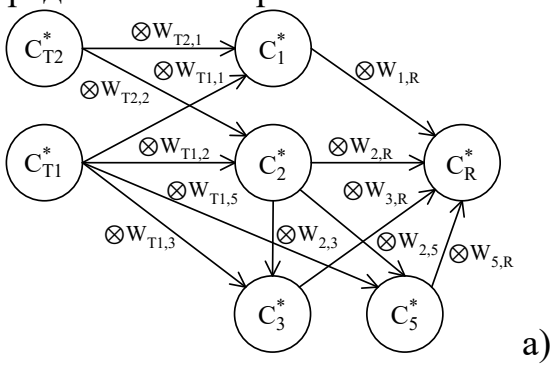


Рисунок 13 – Нечеткая серая когнитивная карта

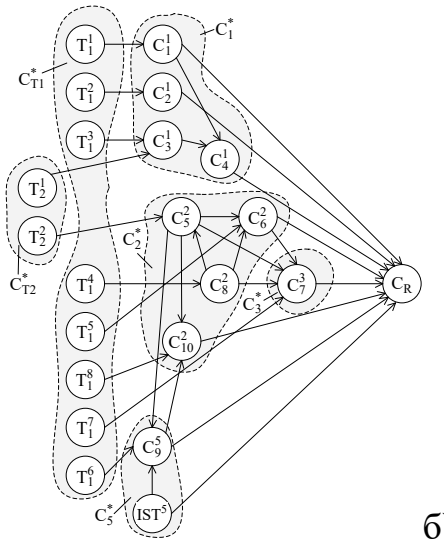
1 – концепт C_1, представляющий собой угрозу, связанную с попыткой несанкционированного доступа (НСД) к информации; 2 – концепт C_2, представляющий угрозу, связанную с вредоносным программным воздействием (вирусными атаками); 3 – концепт C_3, характеризующий целевой объект угрозы – базу данных (БД), размещенную на сервере; 4 – концепт C_4, характеризующий электронный документооборот (ЭДО) организации; 5 – концепт C_5, характеризующий потенциальный ущерб, вызванный нарушением конфиденциальности информации; 6 – концепт C_6, характеризующий потенциальный ущерб вследствие нарушения целостности информации при воздействии заданной угрозы.

Рассмотрена **методика анализа рисков ИБ с использованием построения вложенных нечетких когнитивных карт** на примере задачи обеспечения целостности телеметрической информации (ТМИ) в промышленной автоматизированной информационной системе (АИС) сбора, хранения и обработки информации о состоянии авиационных бортовых систем. В составе АИС выделены зоны безопасности, объединяемые по принципу единства выполняемых функций и требований к безопасности их

реализации, связанные каналами телекоммуникаций (трактами). Рассмотрена задача анализа рисков ИБ, связанных с обеспечением целостности ТМИ АИС, с учетом воздействия на систему внешних и внутренних угроз, с помощью НСКК. Укрупненная НСКК для оценки рисков ИБ АИС, выступающая в данном случае как когнитивная модель АИС начального приближения, представлена на рис. 14.



а)



б)

верхний индекс (маркер «*») обозначает принадлежность концепта C_p^* к укрупненной НСКК, нижний индекс (p) обозначает номер концепта текущего уровня.

Рисунок 14 – Укрупненная (исходная) НСКК для оценки рисков ИБ (а) и первый уровень декомпозиции НСКК для оценки рисков ИБ АИС (б)

Предложен **сценарный подход к моделированию сложных многошаговых целенаправленных кибератак с использованием базы меташаблонов атак CAPEC и БДУ ФСТЭК России** с формализацией в виде иерархической НКК для возможности анализа с требуемым уровнем детализации и количественной оценки рисков ИБ (рис. 15 и 16).

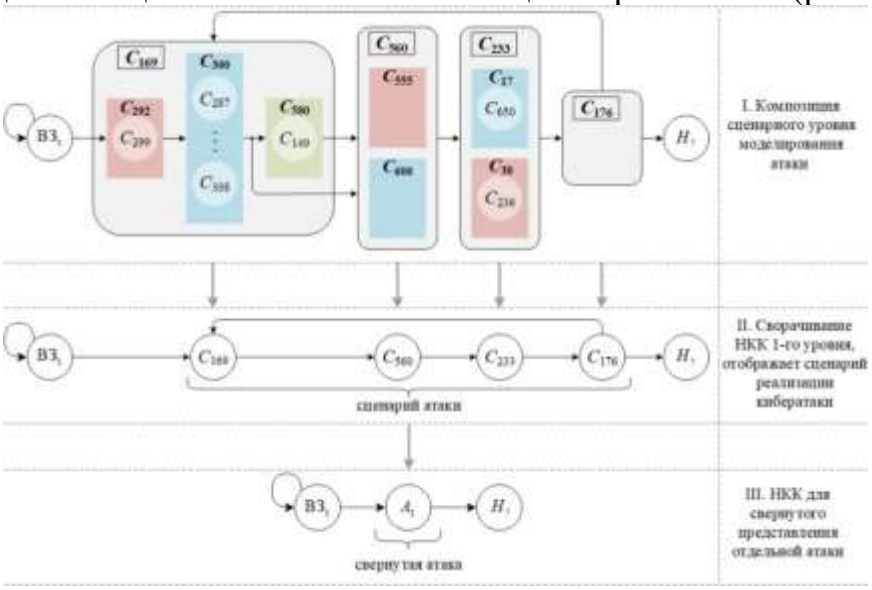


Рисунок 15 – Этапы построения укрупненной НКК для формирования графа атак

Исходными данными для конструирования вектора атаки на основе меташаблонов являются результаты работы сканеров уязвимостей и базы данных угроз и уязвимостей, а также потенциальных слабостей программного и аппаратного обеспечения. Набор показателей системы оценки уязвимостей CVSS и базы CVE и CWE позволяют формально описать уязвимость и

сценарий ее эксплуатации, а также автоматизировать процесс построения цепочки возможных переходов внутри меташаблона. Рассмотрен алгоритм построения укрупненной НКК для сформированного вектора атаки.

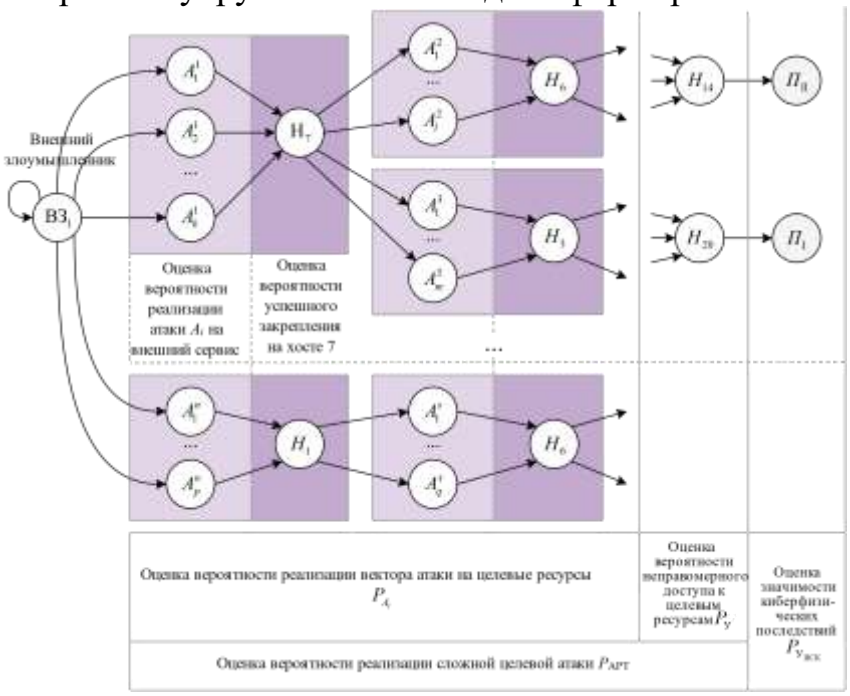


Рисунок 16 – НКК для моделирования набора возможных атак на выделенные целевые концепты

Предложены рекомендации по повышению интерпретируемости результатов моделирования рисков ИБ, полученных с НКК.

В пятой главе осуществляется разработка метода и алгоритмов оценки риска ИБ на основе обнаружения и анализа аномалий в накапливаемых данных мониторинга ИБ объекта КИИ с использованием технологий анализа временных рядов и методов машинного обучения. Переход от статической эталонной модели объекта КИИ и априорных оценок при анализе и оценке рисков ИБ к адаптивной модели объекта с уточнением вероятности реализации угроз, эксплуатации уязвимостей и итоговых оценок риска ИБ основан на применении методов мониторинга ИБ (наблюдение за объектом защиты, системой защиты и взаимодействием объекта с внешней средой).

Разработана структура системы мониторинга целостности ТМИ, основанная на обнаружении вызванных воздействием возможного злоумышленника аномалий в многомерных временных рядах, полученных с помощью модели сложного технического изделия, и принимаемых с бортовых систем летательного аппарата (ЛА). Выходом системы мониторинга является оценка условной вероятности событий нарушения целостности данных. База нечетких продукционных правил применяется для объяснения принимаемого решения о типе согласования при необходимости проведения процедуры расследования инцидентов нарушения целостности ТМИ. На рис.17: X_M – параметры состояния ГТД, полученные на основе модели; X_R – параметры состояния ГТД, полученные с борта ЛА; F_R^W – компактный вектор признаков состояния ГТД; R_K – результат мониторинга: «обрыв сигнала», «нормальная работа», «нарушение целостности»; U_R – вектор оценок вероятностей принадлежности текущего вектора параметров состояния одному из

состояний мониторинга; ВПС – вектор признаков согласованности; ННС – нейронечеткий классификатор; БПР – блок принятия решений.

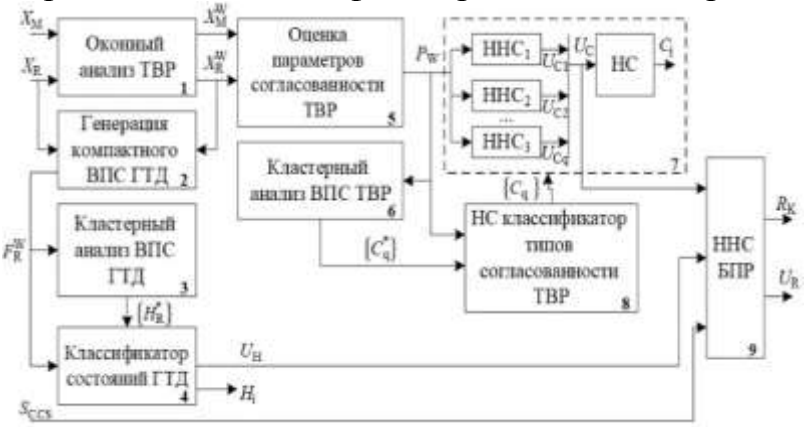


Рисунок 17 – Структурная схема системы анализа согласованности параметров ГТД, получаемых с модели и с борта ЛА

Предложен способ мониторинга целостности данных о состоянии мобильного объекта (МО), основанный на сравнении ТВР, полученных от эксплуатируемого МО, и модели МО, установленной на предприятии-изготовителе. Для сравнения вычисляются следующие метрики близости: коэффициент детерминации, средний процент отклонения и евклидово расстояние, кроме того, принимается сигнал системы контроля исправности МО и идентифицируется режим работы МО (установившийся и переходный). Далее, в соответствии с выработанными правилами нечеткой логики, принимается решение о наличии или отсутствии атаки злоумышленника на принятые данные, их целостности. На рис. 18 представлена структурная схема системы мониторинга целостности данных. По результатам экспериментов, оценка вероятности успешного распознавания атаки с помощью системы мониторинга целостности данных, основанного на правилах нечеткой логики, составила 0,85, а на основе нейронечеткого модуля – 0,98.

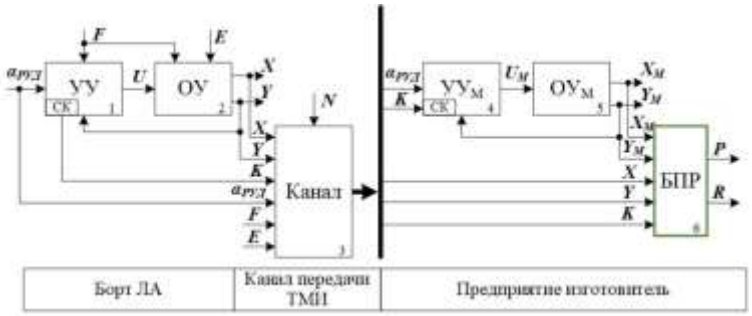


Рисунок 18 – Схема реализации системы мониторинга целостности данных, получаемых с бортовых систем мобильного объекта

Алгоритм мониторинга целостности данных:

1. Выделяется набор параметров МО для анализа рассогласований данных, полученных с модели, и данных, полученных с МО;
2. Выделяется скользящее окно для анализа многомерных векторов X, Y, Y_M, X_M X_M^W, X_R^W – наборы ТВР, сгенерированные моделью и полученные с МО, в одном временном окне;
3. Строится многомерный временной ряд (ВР) P^W – параметры согласованности ТВР для каждого из окон анализа W_S;
4. Определяется режим работы МО U_H в выделенном временном окне;
5. Выполняется расчет параметров согласованности ТВР, полученных с борта МО, и ТВР, генерируемых моделью;
6. По параметрам рассогласования на основе типа динамики МО и сигнала системы контроля принимается решение о целостности данных, полученных с МО.

Разработаны **система обнаружения сетевых атак в гетерогенной сети промышленного объекта** и **алгоритм** интеллектуального анализа сетевого трафика. С целью оценки их количественных и качественных характеристик использовались общедоступные размеченные по типам атак и режимам работы базы данных сетевого трафика (NSL-KDD, CICIDS-2017, UNSW-NB15, сети промышленного Интернета вещей – WUSTL-IIOT-2018; беспроводные промышленные сенсорные сети – WSN-DS-2016) и полусинтетические наборы, собранные с использованием полунатурного стенда, моделирующего взаимодействие промышленной сети и корпоративного сегмента. Особенностью указанных наборов данных является акцент на использование промышленных протоколов, таких как Modbus.

Структурная схема системы обнаружения сетевых атак в гетерогенной сети промышленного объекта на основе интеллектуального анализа данных и **обобщенный алгоритм интеллектуального анализа параметров сетевого трафика в задаче обнаружения аномалий и вредоносной сетевой активности** представлены на рисунке 19.

В составе подсистемы автоматического профилирования (рис.20) предложена обобщенная схема модуля видеоаналитики, позволяющего:

1. анализировать оценить степень уверенности композиции классификаторов в типе распознаваемого образа (аутентификация на основе изображения лица), динамике движений субъекта (распознавание типа движений, жестов), типе психоэмоционального состояния оператора (корректность классификации паттернов составила 97 %);

2. выполнять функции нейросетевой системы идентификации и аутентификации пользователя.

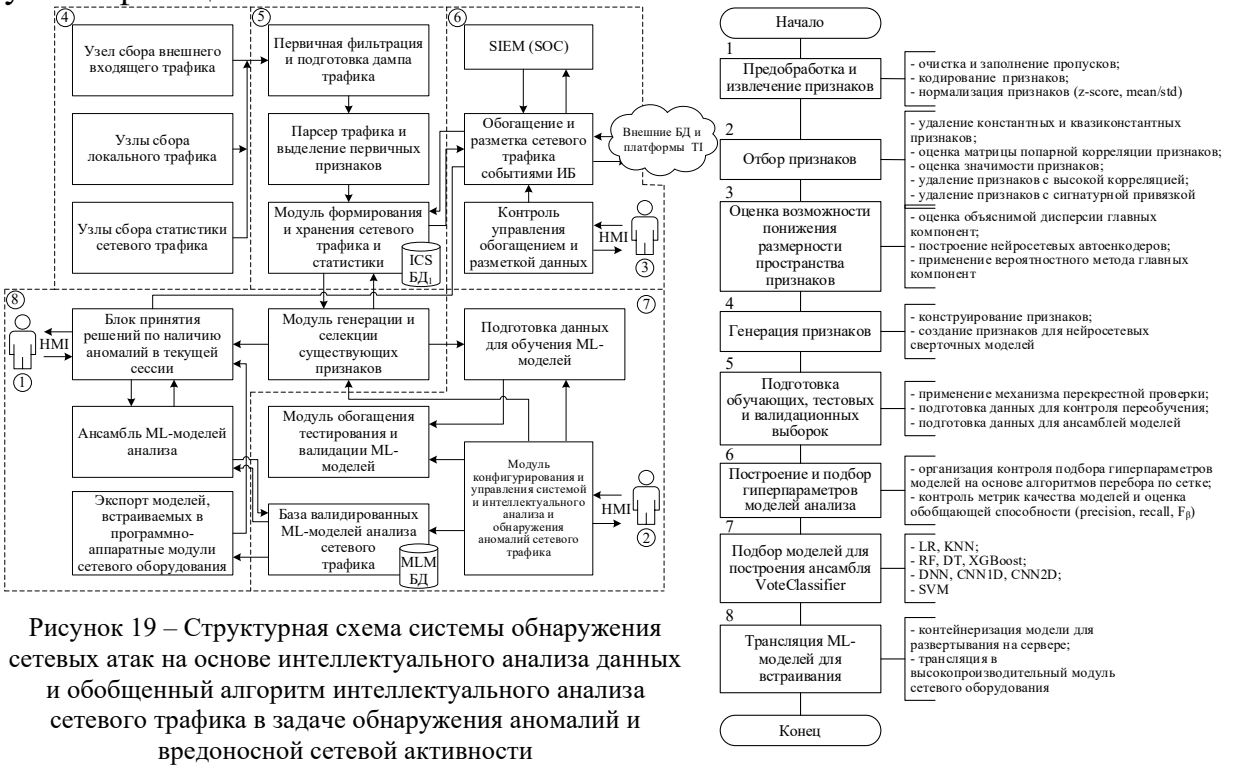


Рисунок 19 – Структурная схема системы обнаружения сетевых атак на основе интеллектуального анализа данных и обобщенный алгоритм интеллектуального анализа сетевого трафика в задаче обнаружения аномалий и вредоносной сетевой активности

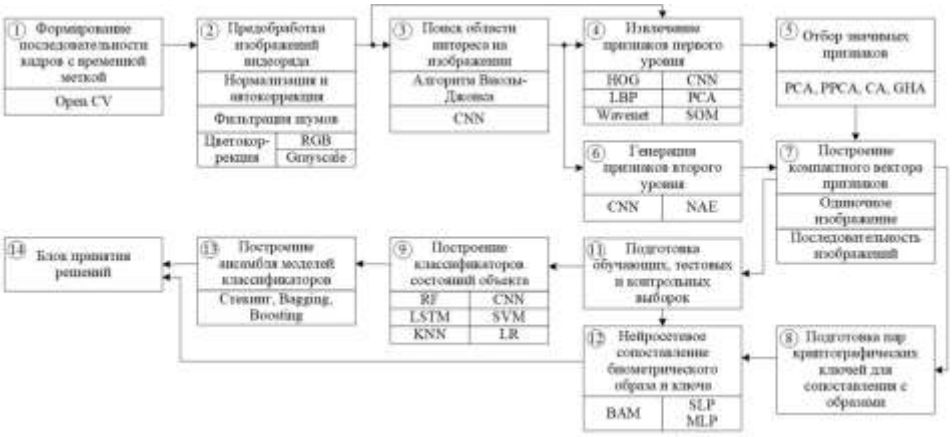


Рисунок 20 – Структура системы автоматического профилирования действий пользователя

В функции подсистемы автоматического профилирования также входит анализ информационного почерка пользователя (динамический профиль пользователя на основе анализа клавиатурного почерка), позволяющего выполнять процедуру непрерывной скрытой идентификации и аутентификации (корректность классификации пользователя составила 98 %).

В шестой главе решаются практические прикладные задачи комплексной оценки рисков ИБ и обеспечения защищенности объектов КИИ с использованием ИСППР.

Разработана архитектура ИСППР по оценке рисков ИБ объектов КИИ, включающая в себя следующие базовые модули: подсистема анализа угроз и уязвимостей объекта КИИ на основе технологий семантического анализа их текстовых описаний; подсистема оценки степени опасности уязвимостей на основе прогнозирования набора метрик с помощью анализа текстового описания; подсистема построения и анализа семантической модели текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения зоны безопасности объекта КИИ; подсистема обнаружения сетевых атак в гетерогенной сети объекта КИИ; подсистема автоматического профилирования.

Особенностью данной ИСППР является возможность автоматизации основных этапов комплексной оценки рисков ИБ объектов КИИ, что позволяет отслеживать эволюцию объекта защиты и выполнять уточнение оценок вероятностей реализации угроз и эксплуатации уязвимостей, а также реализацию опережающей стратегии защиты (проактивная защита).

В качестве объекта КИИ рассмотрена АИС сбора, хранения и обработки ТМИ предприятия-изготовителя изделий авиационной техники. Для автоматизации предложенной процедуры комплексной оценки рисков ИБ разработано прикладное алгоритмическое и программное обеспечение. Применение предложенного способа мониторинга целостности данных, получаемых с бортовых систем мобильного объекта, позволило снизить оценку риска ИБ для рассматриваемой системы на 45 %.

Предложено решение задачи оценки рисков ИБ промышленной сети АСУ ТП нефтедобывающего предприятия с использованием технологий когнитивного моделирования на основе классических, серых, интуиционистских НКК и их ансамбля, позволяющего учесть

неопределенность мнений экспертов в оценке риска ИБ. Полученные оценки рисков ИБ после оптимизации распределения ресурсов, выделенных на контрмеры, уменьшились как в отношении разброса, так и в отношении центрального значения оценок на 70-80 %, снизилась оценка стоимости эксплуатации контрмер.

В процессе решения поставленной практической задачи противодействия кибермошенничеству (создания антифрод-системы) предложен алгоритм сбора, обработки данных, характеризующих пользовательское окружение конечной системы, а также алгоритм анализа изменения паттернов динамических биометрических признаков пользователя в случае удаленного управления пользовательским сеансом. В качестве объекта воздействия угрозы (фрода) в данном случае выступает ИС, в которой хранится и обрабатывается информация, представляющая интерес для злоумышленника. Предложена гетерогенная модель обнаружения удаленного управления пользовательским сеансом на основе анализа цифрового отпечатка пользователя (точность 93 %).

Проведен анализ угроз нарушения ИБ и соответствующих им мер противодействия по уровням архитектуры программно-определяемых сетей объектов КИИ. Разработаны и реализованы инструменты (алгоритмическое и программное обеспечение, архитектура системы взаимодействия) защиты управляющего трафика программно-определяемых сетей на основе традиционных моделей машинного обучения и гетерогенных нейросетевых моделей (F_1-мера достигает 96 %) с возможностью программно-аппаратной реализации.

С целью осуществления мониторинга и обмена данными об инцидентах ИБ в финансовой сфере (в составе платформы IRP/SOAR) разработана структурная схема системы мониторинга банковских транзакций в составе антифрод-системы, которая включает модуль интеллектуального анализа текстовых меток операций. Внедрение модуля позволяет делать выводы о принадлежности транзитной операции к одному из предложенных классов, строить динамический профиль пользователя и повысить обоснованность рекомендаций системы мониторинга (точность классификации операций составила 81 %).

Разработан проблемно-ориентированный программный комплекс «Полигон», предназначенный для тестирования и отладки методов, моделей и алгоритмов когнитивного моделирования и интеллектуального анализа слабоструктурированных данных при построении базы знаний ИСППР, реализованный на масштабируемой (открытой) инструментальной платформе (в том числе на кластерной) с возможностью сопряжения / встраивания в существующие система корреляции событий ИБ и ситуационные операционные центры.

В заключении приводятся основные результаты и выводы по проведенной работе.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ

Таким образом, в ходе диссертационного исследования разработаны научно обоснованные технические и технологические решения, направленные на решение проблемы разработки моделей и методов комплексной оценки рисков ИБ объектов КИИ на основе методов и технологий интеллектуального анализа данных, имеющей важное хозяйственное значение. Основные выводы и результаты работы можно сформулировать следующим образом:

1. Предложена концепция комплексной оценки рисков ИБ объектов КИИ, основанная на интеграции технологий нечеткого когнитивного моделирования и методов машинного обучения, отличающаяся применением комплекса проблемно-ориентированных моделей, методов и алгоритмов комплексной оценки рисков ИБ объектов КИИ, что позволяет повысить оперативность и снизить эффект неопределенности от влияния субъективных факторов.

2. Разработан комплекс проблемно-ориентированных моделей параметризации угроз и уязвимостей объектов КИИ, основанных на использовании технологий интеллектуального анализа данных и обнаружения аномалий в накапливаемых данных мониторинга их состояния, отличающийся применением ансамбля гетерогенных моделей машинного обучения при оценке опасности уязвимостей и построении детекторов аномалий и эффективным использованием дополнительной информации из открытых баз знаний с помощью технологий анализа текстовых описаний, что позволяет снизить трудоемкость и автоматизировать низкоуровневое моделирование сценариев эксплуатации уязвимостей и реализации угроз, а также обеспечивает видимость и контекст потенциальной атаки.

3. Разработаны метод, алгоритмы и методика качественной оценки уровня рисков ИБ объектов КИИ, основанные на использовании технологий семантического анализа текстовых описаний угроз и уязвимостей, отличающиеся подходом к формализации слабоструктурированных текстовых описаний с помощью гетерогенных нейросетевых моделей вложений в виде графовой семантической модели, что позволяет обеспечить выявление потенциальных угроз, уязвимостей и сценариев реализации атак с возможностью их ранжирования по приоритетам, а также автоматизировать основные этапы процедуры оценки рисков.

4. Разработаны метод, алгоритмы и методика количественной оценки рисков ИБ объектов КИИ, основанные на построении иерархии вложенных когнитивных карт, соответствующих структурно-функциональной организации объекта КИИ, отличающиеся построением и декомпозицией укрупненной нечеткой когнитивной карты, сценарным моделированием сложных многошаговых целенаправленных кибератак с использованием базы меташаблонов атак с дальнейшей формализацией в виде иерархической НКК, что позволяет получить количественную оценку рисков ИБ объектов КИИ с учетом совокупности объективных и субъективных факторов

неопределенности, а также автоматизировать сценарное моделирование сложных многошаговых атак с использованием базы меташаблонов.

5. Разработаны метод и алгоритмы оценки рисков ИБ объектов КИИ на основе обнаружения аномалий временных рядов накапливаемых параметров, характеризующих состояние этих объектов, сетевого трафика промышленных сетей и поведения пользователей конечных систем, основанные на применении методов интеллектуального анализа многомерных временных рядов, что позволяет повысить достоверность и оперативность поиска скрытых зависимостей в накапливаемых данных и повысить достоверность результатов оценивания рисков ИБ за счет уточнения априорных оценок вероятностей реализации угроз и эксплуатации уязвимостей.

6. Разработана архитектура ИСППР по оценке рисков ИБ объектов КИИ, интегрирующая предложенные в работе технические решения. Проведенные исследования с использованием данной ИСППР показывают, что:

– применение предложенного способа мониторинга целостности телеметрических данных, получаемых с бортовых систем мобильного объекта, позволило снизить оценку риска ИБ для рассматриваемой системы на 45%; оценка вероятности успешного распознавания атаки с помощью системы мониторинга целостности данных, основанного на правилах нечеткой логики, составила 0,85, а на основе нейронечеткого модуля – 0,98;

– предложенные алгоритмы обнаружения аномалий в данных мониторинга состояния АСУ ТП нефтедобычи позволяют корректно классифицировать до 78-95 % состояний, в том числе, вызванных воздействием злоумышленника;

– предложенные решения по цифровому профилированию и анализу совокупности отпечатков (fingerprints) пользовательских окружений и динамических пользовательских профилей в задаче противодействия кибермошенничеству (создания антифрод-системы) обеспечивают повышение точности определения удаленного управления на 17 % и повышение точности классификации мошеннических операций на 23 %;

– предложенные решения в задачах обнаружения аномалий сетевого трафика в гетерогенных промышленных сетях позволяют добиться оценки F_1-меры на уровне 96 %.

Перспективы дальнейшей разработки темы. Дальнейшее развитие темы диссертационного исследования планируется в двух направлениях:

1. исследование технологий ИАД текстовых описаний угроз и уязвимостей на основе моделей трансформеров, что позволит использовать мультиязычные базы знаний для сопоставления угроз, уязвимостей и сценариев их эксплуатации и повысит достоверность оценок рисков ИБ;

2. исследование методов и алгоритмов моделирования сложных технических объектов с применением специализированных глубоких нейронных сетей с целью повысить достоверность результатов оценивания рисков ИБ за счет уточнения априорных оценок вероятностей реализации угроз и эксплуатации уязвимостей.

ОСНОВНЫЕ ПОЛОЖЕНИЯ ДИССЕРТАЦИИ ОПУБЛИКОВАНЫ В СЛЕДУЮЩИХ РАБОТАХ

Монографии

1. Digital Forensic Science. / Eds.: S. Shetty, P. Shetty (Chapter 2: Vasilyev V.I., Vulfin A.M., Chernyakhovskaya L.R. Cybersecurity Risk Analysis of Industrial Automation Systems on the Basis of Cognitive Modeling Technology), IntechOpen Pub., London, UK, 2019. ISBN: 978-1-83880-260-8; eBook (PDF) ISBN: 978-1-83968-742-6. – DOI: 10.5772/intechopen.78450.
2. Методы и модели поддержки принятия решений при управлении инновационными проектами в производственно-экономических системах /Под общей ред. Черняховской Л.Р. (Глава 3: Анализ и управление рисками инновационных проектов и промышленных объектов с помощью технологий когнитивного моделирования. – С. 118–157). – М.: Издательский Дом «Академия Естествознания», 2020. – 230 с. ISBN: 978-5-91327-668-1. – DOI: 10.17513/пр.437.

В рецензируемых научных изданиях, входящих в перечень ВАК

3. Вульфин А.М., Фрид А.И. Нейросетевая модель анализа технологических временных рядов в рамках методологии Data Mining // Информационно-управляющие системы. – 2011. – № 5(54). – С. 31–38.
4. Васильев В.И., Вульфин А.М., Кудрявцева Р.Т. Анализ и управление рисками информационной безопасности с использованием технологии нечеткого моделирования // Доклады ТУСУРа. – 2017. – Т. 20, № 4. – С. 61–66.
5. Защищенный доступ к базе данных о состоянии систем автоматического управления (САУ) авиационными ГТД через веб-приложение / М.Б. Гузаиров, А.М. Вульфин, А.И. Фрид, В.В. Берхольц // Информация и безопасность. – 2017. – Т. 20, № 3. – С. 410–413.
6. Чуйков А.В., Вульфин А.М., Васильев В.И. Нейросетевая система преобразования биометрических признаков пользователя в криптографический ключ // Доклады ТУСУРа. – 2018. – Т. 21, № 3. – С. 35–41.
7. Васильев В.И., Гузаиров М.Б., Вульфин А.М. Оценка рисков информационной безопасности с использованием нечетких продукционных когнитивных карт // Информационные технологии. – 2018. – Т. 24, № 4. – С. 266–273.
8. Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт / В.И. Васильев, А.М. Вульфин, М.Б. Гузаиров, А.Д. Кириллова // Информационные технологии. – 2018. – Т. 24, № 10. – С. 657–664.
9. Сравнительный анализ алгоритмов когнитивного моделирования при оценке рисков информационной безопасности / М.Б. Гузаиров, А.М. Вульфин, В.М. Картак, А.Д. Кириллова, К.В. Миронов // Труды ИСА РАН. – 2019. – Т. 69, № 4. – С. 62–69.
10. Система обнаружения атак в беспроводных сенсорных сетях промышленного интернета вещей / В.И. Васильев, А.М. Вульфин, В.М. Картак, А.Д. Кириллова, К.В. Миронов // Труды ИСА РАН. – 2019. – Т. 69, № 4. – С. 70–78.
11 Об интерпретируемости нечетких когнитивных моделей на этапе оценки рисков инновационных проектов / В.И. Васильев, А.М. Вульфин, А.Д. Кириллова, Л.Р. Черняховская // Вестник УрФО. Безопасность в информационной сфере. – 2019. – № 4(34). – С. 45–57.
12. Фрид А.И. Вульфин А.М., Берхольц В.В. Способ мониторинга целостности телеметрической информации о состоянии двигателя летательного аппарата // Безопасность информационных технологий. – 2020. – Т. 27, № 4. – С. 65–76.

13. Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт / В.И. Васильев, А.М. Вульфин, М.Б. Гузаиров, В.М. Картак, Л.Р. Черняховская // Информационные технологии. – 2020. – Т. 26, № 4. – С. 213–221.
14. Васильев В.И., Черняховская Л.Р., Вульфин А.М. Моделирование процессов управления инновационной деятельностью в регионе с применением нечетких когнитивных карт // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2020. – № 3. – С. 15–25.
15. Васильев В.И., Вульфин А.М., Черняховская Л.Р. Анализ рисков инновационных проектов с использованием технологии многослойных нечетких когнитивных карт // Программная инженерия. – 2020. – Т. 11, № 3. – С. 142–151.
16. Вульфин А.М. Интеллектуальный анализ видеоданных в системе контроля соблюдения правил промышленной безопасности [Электронный ресурс] // Моделирование, оптимизация и информационные технологии. – 2020. – № 8(2). – С. 1–16. – Режим доступа: https://moit.vivt.ru/wpcontent /uploads /2020/05/Vulfin_2_20_1.pdf
17. Вульфин А.М. Интеллектуальный анализ данных пользовательского окружения в задаче обнаружения удаленного управления [Электронный ресурс] // Моделирование, оптимизация и информационные технологии. – 2020. – № 8(2). – С. 1–19. – Режим доступа: https://moit.vivt.ru/wpcontent /uploads/2020/05/Vulfin_2_20_2.pdf
18. 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.
19. Васильев В.И. Вульфин А.М., Кучкарова Н.В. Автоматизация анализа уязвимостей программного обеспечения на основе технологии Text Mining // Вопросы кибербезопасности. – 2020. – № 4(38). – С. 22–31.
20. Васильев В.И., Кириллова А.Д., Вульфин А.М. Когнитивное моделирование вектора кибератак на основе меташаблонов CAPEC // Вопросы кибербезопасности. – 2021. – № 2(42). – С. 2–16.
21. Вульфин А.М. Система управления данными киберразведки [Электронный ресурс] // Моделирование, оптимизация и информационные технологии. – 2021. – № 9(1). – С. 1–18. – Режим доступа: https://moitvivt.ru/ru/journal/pdf?id=925
22. Система оценки метрик опасности уязвимостей на основе технологий семантического анализа данных / В.И. Васильев, А.М. Вульфин, А.Д. Кириллова, А.В. Никонов // Вестник УрФО. Безопасность в информационной сфере. – 2021. – № 2(40). – С. 31–43.
23. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining / В.И. Васильев, А.М. Вульфин, А.Д. Кириллова, Н.В. Кучкарова // Системы управления, связи и безопасности. – 2021. – № 3. – С. 110–134.
24. Вульфин А.М. Анализ защищенности веб-приложения для доступа к системе хранения критически важных данных/ [Электронный ресурс] // Моделирование, оптимизация и информационные технологии. – 2021. № 9(4). – С. 1-16. – Режим доступа: https://moitvivt.ru/ru/journal/pdf?id=1112 DOI: 10.26102/2310-6018/2021.35.4.038.

25. Васильев В. И., Вульфин А. М., Гвоздев В. Е., Картак В. М., Атарская Е. А. Обеспечение информационной безопасности киберфизических объектов на основе прогнозирования и обнаружения аномалий их состояния // Системы управления, связи и безопасности. 2021. №6. С. 90-119. DOI: 10.24412/2410-9916-2021-6-90-119.
26. Вульфин А.М. Обнаружение сетевых атак в гетерогенной промышленной сети на основе технологий машинного обучения // Программная инженерия. – 2022. – Т. 13. – № 2, С. 68-80. DOI: 10.17587/prin.13.68-80

В научных журналах и трудах конференций, индексируемых в Scopus и Web of Science

27. Vulfin A.M., Frid A.I., Giniyatullin V.M. Neural-base model for detection and recognition of technological situations within the scope of data mining strategy // Optical Memory and Neural Networks (Information Optics). – 2010. – Vol. 19, no. 3. P. 207–212.
28. Anti-fraud system on the basis of Data Mining technologies / M.U. Sapozhnikova, A.V. Nikonov, A.M. Vulfin, M.M. Gayanova, K.V. Mironov, D.V. Kurennov // 2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 2017). – IEEE. – 2017. – P. 243–248. – URL: https://ieeexplore.ieee.org/abstract/document/8388649
29. Distributed infrastructure for Big Data processing in the transaction monitoring systems / M.U. Sapozhnikova, M.M. Gayanova, A.M. Vulfin, A.V. Nikonov, A.V. Chuykov // 4th International Conference on Information Technology and Nanotechnology: CEUR Workshop Proceedings. – 2018. – P. 228–235. – URL: http://ceur-ws.org/Vol-2212/paper32.pdf
30. Simulation modelling of the transmission system of the telemetric information on the status of the on-board aircraft status / M.B. Guzairov, A.I. Frid, A.M. Vulfin, V.V. Berkholts // 4th International Conference on Information Technology and Nanotechnology: CEUR Workshop Proceedings. – 2018. – P. 105–111. – URL: https://pdfs.semanticscholar.org/d2cb/4dfe2ccb4753ed2f1aeae2b202 ce e20 f1f23.pdf
31. Sapozhnikova M.U., Nikonov A.V., Vulfin A.M. Intrusion detection system based on data mining technics for industrial networks // International Conference on Industrial Engineering, Applications and Manufacturing, (ICIEAM). – IEEE. – 2018. – P. 1–5. – URL: https://ieeexplore.ieee.org /abstract/document/8728771
32. Frid A.I., Vulfin A.M., Berkholts V.V. Architecture of modular system for assessing security of telemetry information transmission system // International Conference on Industrial Engineering, Applications and Manufacturing, (ICIEAM). – IEEE. – 2018. – P. 1–6. – URL: https://ieeexplore.ieee.org/abstract/document/8728730
33. The concept of integrity of telemetric information about the state of an aircraft power plant monitoring / M.B. Guzairov, A.I. Frid, A.M. Vulfin, V.V. Berkholts // 2019 International Conference on Electrotechnical Complexes and Systems (ICOECS). – IEEE. – 2019. – P. 1–6. – URL: https://ieeexplore.ieee.org/ abstract/document/8950020
34. Intelligent integrity monitoring system for technological process data / M.I. Arpishkin, A.M. Vulfin, V.I. Vasilyev, A.V. Nikonov // Journal of Physics: Conference Series. IOP Publishing. – 2019. – Vol. 1368, no. 5. – P. 1–16. – URL: https://iopscience.iop.org/article/10.1088/1742-6596/1368/5/052029/meta
35. Intrusion detection system on the basis of data mining algorithms in the industrial network / M.A. Gurin, A.M. Vulfin, V.I. Vasilyev, A.V. Nikonov // 5th International Conference on Information Technology and Nanotechnology: CEUR Workshop Proceedings. – 2019. – P. 553–565. – URL: http://ceur-ws.org/Vol-2416/paper68.pdf

36. Analysis of Financial Payments Text Labels in the Dynamic Client Profile Construction / A.S. Startseva, A.M. Vulfin, V.I. Vasilyev, A.V. Nikonov, A.D. Kirillova // 2020 International Conference on Information Technology and Nanotechnology (ITNT). – IEEE. – 2020. – P.1–10.
37. Hidden Authentication of the User Based on Neural Network Analysis of the Dynamic Profile / A.A. Sivova, A.M. Vulfin, K.V. Mironov, A.D. Kirillova // Proceedings of the 8th International Conference on Applied Innovations in IT. – 2020. – P. 1–10. URL: https://opendata.uni-halle.de/bitstream/1981185920/32948 /1/2_5_Sivova.pdf
38. Architecture of the Security Access System for Information on the State of the Automatic Control Systems of Aircraft / A.I. Frid, A.M. Vulfin, V.V. Berholz, D.Yu. Zakharov, K.V. Mironov // Acta Polytechnica Hungarica. – 2020. – Vol. 17, no. 8. – P. 151–164.
39. Secure Data Exchange in the Industrial Internet of Things Network of the Fuel and Energy Complex / E.R. Hajrullin, A.M. Vulfin, K.V. Mironov, A.I. Frid, M.B. Guzairov, A.D. Kirillova // Proceedings ICOECS 2020 International Conference on Electrotechnical Complexes and Systems. – IEEE. – 2020. – P. 353–358.
40. Neural network biometric cryptography system / A.M. Vulfin, V.I. Vasilyev, A.V. Nikonov, A.D. Kirillova // Proceedings of the Information Technologies and Intelligent Decision Making Systems (ITIDMS2021) (January 20, 2021). CEUR. – 2021. – Vol-2843.
41. Cognitive security modeling of biometric system of neural network cryptography / A.M. Vulfin, V.I. Vasilyev, A.D. Kirillova, A.V. Nikonov // Proceedings of the Information Technologies and Intelligent Decision Making Systems (ITIDMS2021), (January 20, 2021). CEUR. – 2021. – Vol-2843.
42. Berkholts V.V., Vulfin A.M., Frid A.I. Telemetry data integrity monitoring system // IOP Conf. Series: Materials Science and Engineering, 2nd Scientific Conference on Fundamental Information Security Problems in terms of the Digital Transformation. – 2021. – Vol. 1069. – 012003.
43. Software-hardware complex for modeling secure IIoT distributed ledger / A.R. Makhmutov, S.V. Trishin, K.V. Mironov, A.M. Vulfin // IOP Conf. Series: Materials Science and Engineering, 2nd Scientific Conference on Fundamental Information Security Problems in terms of the Digital Transformation (FISP 2020) (30 November 2020). – 2021. – Vol. 1069. – 012018.
44. Algorithms for detecting network attacks in an enterprise industrial network based on data mining algorithms / A.M. Vulfin, V.I. Vasilyev, S.N. Kuharev, E.V. Homutov, A.D. Kirillova // International Scientific and Practical Conference “Information Technologies and Intelligent Decision Making Systems” (ITIDMS-II 2021) (1 July 2021). – Journal of Physics: Conference Series. – 2021. –Vol. 2001. – 012004.
45. Network traffic analysis based on machine learning methods / A.M. Vulfin, V.I. Vasilyev, V.E. Gvozdev, K.V. Mironov, O.E. Churkin // International Scientific and Practical Conference “Information Technologies and Intelligent Decision Making Systems”. – Journal of Physics: Conference Series. – 2021. –Vol. 2001. – 012017.

В других изданиях

46. Vulfin A.M., Frid A.I. Safety Increasing of Oil Companies Engineering Networks Operation with Use of Artificial Intelligence Systems // Proceedings of the 16th International Workshop. Computer Science and Information Technologies (CSIT'2014). – 2014. – Vol. 3. – P. 167–171.

47. The architecture of the web application for protected access to the informational system of processing critically important information / A.I. Frid, A.M. Vulfin, V.V. Berkholts, D.Ju. Zakharov, K.V. Mironov // Proceedings of the 19th International Workshop. Computer Science and Information Technologies (CSIT'2017). – 2017. – Vol. 1. – P. 16–22.
48. Data Mining technologies in the problem of designing the bank transaction monitoring system / K.V. Mironov, M.U. Sapozhnikova, M.M. Gayanova, A.M. Vulfin, A.V. Nikonov // Proceedings of the 19th International Workshop. Computer Science and Information Technologies (CSIT'2017). – 2017. – Vol. 1. – P. 45–55.
49. Simulation modelling of the transmission system of the telemetric information on the status of the on-board aircraft status / M.B. Guzairov, A.I. Frid, A.M. Vulfin, V.V. Berkholts // IV Международная конференция и молодежная школа «Информационные технологии и нанотехнологии». – 2018. – С. 2275–2281. URL: https://pdfs.semanticscholar.org/d2cb/4dfe2ccb4753ed2f1aeae2b202c ee 20f1f23.pdf
50. Frid A.I., Vulfin A.M., Berkholts V.V. Analysis of the methods of constructing information attack models for the system of telemetric information transmission // Труды VI Всероссийской конференции «Информационные технологии интеллектуальной поддержки принятия решений» (ITIDS'2018) (с приглашением зарубежных ученых). – 2018. – С. 226–229.
51. Концепция мониторинга целостности телеметрической информации о состоянии энергетической установки летательного аппарата / А.И. Фрид, М.Б. Гузаиров, А.М. Вульфин, В.В. Берхольц // Сборник докладов XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (ИНФОБЕЗОПАСНОСТЬ-2019). – 2019. – С. 7–14.
52. Васильев В.И., Вульфин А.М., Муслимова К.И. Методика оценки рисков кибербезопасности АСУ ТП промышленного объекта // Труды VII Всероссийской научной конференции «Информационные технологии интеллектуальной поддержки принятия решений» (с приглашением зарубежных ученых). – 2019. – С. 197–201.
53. Кучкарова Н.В., Васильев В.И., Вульфин А.М. Сравнительный анализ систем классификаций АСУ ТП объектов критической информационной инфраструктуры // Труды VII Всероссийской научной конференции «Информационные технологии интеллектуальной поддержки принятия решений» (ITIDS'2019) (с приглашением зарубежных ученых). – 2019. – С. 214–219.
54. Васильев В.И., Кириллова А.Д., Вульфин А.М. Методы управления рисками кибербезопасности АСУ ТП промышленных объектов // Труды Восьмой всероссийской научной конференции «Информационные технологии интеллектуальной поддержки принятия решений». – 2020. – Т. 1. – С. 185–191.
55. Берхольц В.В., Вульфин А.М., Фрид А.И. Система мониторинга целостности телеметрической информации // Сборник докладов II Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (с приглашением зарубежных ученых). – 2020. – С. 129–134.
56. Васильев В.И., Кириллова А.Д., Вульфин А.М. Моделирование кибератак на объекты АСУ ТП с помощью нечетких когнитивных карт // Приоритетные направления развития науки и технологий: доклады XXVIII международной науч.-практич. конф.; под общ. ред. В.М. Панарина. – Тула: Инновационные технологии. – 2021. – С. 132–132.

Патенты и свидетельства о государственной регистрации программ для ЭВМ

57. Способ и система мониторинга целостности данных: пат. 2740544 C1 Российская Федерация: МПК G06F 21/31 / А.И. Фрид, А.М. Вульфин, В.В. Берхольц. – № 2020122967; заявл. 06.07.2020; опубл. 15.01.2021.
58. Программа анализа текстовых меток на основе технологий интеллектуального анализа естественного языка в системе мониторинга финансовых операций: свидетельство о государственной регистрации программы для ЭВМ 2021615311 Российская Федерация / А.М. Вульфин, А.В. Никонов, И.О. Самойлов, Э.Р. Хайруллин, В.И. Васильев. – № 2021614180; заявл. 26.03.2021; опубл. 06.04.2021.
59. Программа для обнаружения удаленного управления на основе интеллектуального анализа данных пользовательского окружения: свидетельство о государственной регистрации программы для ЭВМ 2020618433 Российская Федерация / А.Ю. Карунас, А.М. Вульфин, В.П. Рыбалко, Г.В. Исахин, К.А. Гайнуллин, В.В. Тихомиров. – № 2020617656; заявл. 14.07.2020; опубл. 28.07.2020.
60. Программа анализа текстовых данных для формирования корпуса: свидетельство о государственной регистрации программы для ЭВМ 2021618418 Российская Федерация / И.О. Самойлов, Э.Р. Хайруллин, А.М. Вульфин, А.В. Никонов, В.И. Васильев. – № 2021614030; заявл. 17.03.2021; опубл. 26.05.2021
61. Программа скрытой аутентификации пользователя на основе нейросетевого анализа динамического профиля: свидетельство о государственной регистрации программы для ЭВМ 2020615185 Российская Федерация / А.Ю. Карунас, А.М. Вульфин, А.Е. Сивова, Г.В. Исахин, А.Д. Кириллова. – № 2020614093; заявл. 03.04.2020; опубл. 18.05.2020.
62. Нейросетевая программа преобразования биометрических признаков пользователя в криптографический ключ: свидетельство о государственной регистрации программы для ЭВМ 2020618661 Российская Федерация / В.П. Рыбалко, А.М. Вульфин, А.В. Чуйков, И.О. Самойлов, В.И. Васильев, В.В. Тихомиров. – № 2020617732; заявл. 14.07.2020; опубл. 31.07.2020.
63. Программа интеллектуального контроля целостности данных технологического процесса: свидетельство о государственной регистрации программы для ЭВМ 2020618556 Российская Федерация / В.П. Рыбалко, А.М. Вульфин, М.И. Арпишкин, И.О. Самойлов, А.Д. Кириллова. – № 2020617650; заявл. 14.07.2020; опубл. 30.07.2020.
64. Программное средство мониторинга целостности телеметрической информации о состоянии энергетической установки летательного аппарата: свидетельство о государственной регистрации программы для ЭВМ 2020618662 Российская Федерация / А.Ю. Карунас, А.М. Вульфин, В.В. Берхольц, Г.В. Исахин, А.И. Фрид. – № 2020617702; заявл. 14.07.2020; опубл. 31.07.2020.
65. Программа анализа многомерных цифровых сигналов для поддержки принятия решений: свидетельство о государственной регистрации программы для ЭВМ 2020618604 Российская Федерация / А.В. Никонов, А.М. Вульфин, М.Ю. Никонова. – № 2020617653; заявл. 14.07.2020; опубл. 30.07.2020.
66. Программа нейронечеткой классификации многомерных цифровых сигналов: свидетельство о государственной регистрации программы для ЭВМ 2020618741 Российская Федерация / А.В. Никонов, А.М. Вульфин, М.Ю. Никонова. – № 2020617654; заявл. 14.07.2020; опубл. 04.08.2020.

67. Программа, реализующая протокол защищенного обмена для индустриальных систем Crisp 1.0: свидетельство о государственной регистрации программы для ЭВМ 2020618278 Российская Федерация / Э.Р. Хайруллин, А.М. Вульфин. – № 2020616891; заявл. 03.07.2020; опубл. 22.07.2020.
68. Программа инвентаризации программного и аппаратного обеспечения локальной вычислительной сети: свидетельство о государственной регистрации программы для ЭВМ 2020618555 Российская Федерация / А.С. Спирин, А.М. Вульфин. – № 2020617637; заявл. 14.07.2020; опубл. 30.07.2020.
69. Программа оценки метрики опасности уязвимостей на основе технологий интеллектуального анализа и обработки естественного языка: свидетельство о государственной регистрации программы для ЭВМ 2021615015 Российская Федерация / А.М. Вульфин, А.В. Никонов, Е.М. Карасева, Н.В. Кучкарова, В.И. Васильев, А.Д. Кириллова. – № 2021614255; заявл. 26.03.2021; опубл. 02.04.2021.
70. Программа анализа уязвимостей программного обеспечения на основе технологий интеллектуального анализа и обработки естественного языка: свидетельство о государственной регистрации программы для ЭВМ 2021615080 Российская Федерация / А.М. Вульфин, А.В. Никонов, Д.Н. Габбасова, Н.В. Кучкарова, В.И. Васильев, А.Д. Кириллова. – № 2021614120; заявл. 26.03.2021; опубл. 02.04.2021.
71. Программа моделирования нечетких когнитивных карт: свидетельство о государственной регистрации программы для ЭВМ 2021615069 Российская Федерация / А.М. Вульфин, Р.Р. Ягафаров, А.Д. Кириллова, В.И. Васильев. – № 2021614134; заявл. 26.03.2021; опубл. 02.04.2021.
72. Программа интеллектуального анализа данных банковских транзакций в составе системы противодействия финансовому мошенничеству: свидетельство о государственной регистрации программы для ЭВМ 2021615066 Российская Федерация / М.Ю. Никонова, А.М. Вульфин, А.В. Никонов. – № 2021614115; заявл. 26.03.2021; опубл. 02.04.2021.
73. Программа анализа и моделирования кибератак на основе меташаблонов в нечетком когнитивном базисе: свидетельство о государственной регистрации программы для ЭВМ 2021619894 Российская Федерация / А.Д. Кириллова, А.М. Вульфин, Р.Р. Ягафаров, Л.Ю. Зиязетдинова. – № 2021618903; заявл. 07.06.2021; опубл. 18.06.2021.
74. Программное средство мониторинга целостности телеметрической информации о состоянии системы автоматического управления газотурбинным двигателем: свидетельство о государственной регистрации программы для ЭВМ 2020664123 Российская Федерация / В.В. Берхольц, А.М. Вульфин, А.И. Фрид. – № 2020663466; заявл. 02.11.2020; опубл. 09.11.2020.

Диссертант А.М. Вульфин