Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Уфимский государственный авиационный технический университет»

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

ДИССЕРТАЦИЯ

на соискание учёной степени
доктора технических наук

Научный консультант:
доктор технических наук, профессор
Васильев Владимир Иванович

УФА – 2022

Содержание

ВВЕДЕНИЕ

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 и предмет исследования

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 и задачи работы

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

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», ОАО 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 трудов конференций и других работ.

Глава 1. Анализ современного состояния в области комплексной оценки рисков ИБ объектов КИИ

1.1 Актуальность проблемы обеспечения ИБ объекта КИИ

Стремительное внедрение цифровых технологий во всех сферах экономики сегодня сопровождается таким же бурным ростом числа компьютерных атак на значимые информационные ресурсы государственных и коммерческих организаций, промышленных предприятий, юридических и частных лиц. Так, согласно данным, приведенным в аналитическом отчете компании Positive Technologies [318], в IV квартале 2020 года был зафиксирован рост инцидентов на 3,1%, по сравнению с III кварталом и на 41,2% по сравнению с аналогичным периодом 2019 года. Целенаправленные атаки составили 80% от общего числа атак. В поле зрения злоумышленников при этом часто попадают сетевые ресурсы промышленных компаний, доступные из Интернета. В IV квартале треть всех инцидентов ИБ в промышленности связаны с эксплуатацией уязвимостей и недостатков защиты информационных систем (ИС), в 84% атак применялось вредоносное программное обеспечение (ПО). По данным Лаборатории Касперского [323], в 2019 году было выявлено 509 новых уязвимостей в различных компонентах автоматизированной системы управления технологическими процессами (АСУ ТП), более половины которых получили оценку более 7 баллов по шкале CVSS 3.0, что соответствует высокой и критической степени риска. Общий процент промышленных компьютеров в мире, на которых было обнаружено и заблокировано вредоносное ПО, в первом полугодии 2019 г. составил 41,21%, т.е. практически каждый второй компьютер подвергся атаке. В России аналогичный показатель составил 44,8%. Атакам в равной степени подвергались предприятия энергетики, машиностроения, нефтегазового сектора и других не менее важных отраслей, что, безусловно, свидетельствует об остроте складывающейся ситуации и необходимости принятия неотложных мер для ее улучшения.

В 2019 г. зафиксирован трехкратный рост востребованности предприятиями и организациями высокоинтеллектуальных средств защиты, позволяющих решать задачи по своевременному выявлению атак и инцидентов информационной безопасности промышленных и информационно-телекоммуникационных систем.

В 2019 г. запланированные на обеспечение ИБ бюджеты организаций увеличились в среднем на 20%. К 2021 году объемы мирового рынка ИБ увеличились на 66% и составили $202 млрд. При этом совокупный мировой ущерб от кибератак вырос к 2021 году на 39% до $2,1 млрд.

На международной и отечественном рынке более 80 компаний занимаются вопросами интеллектуализации систем кибербезопасности. Однако комплексное внедрение подобных решений только начинается. Разработаны требования и нормативные документы в сфере ИБ КИИ, но масштабируемой и переносимой методологии не предложено.

Ежедневно регистрируются новые уязвимости программного и аппаратного обеспечения информационных систем, но их анализ и присвоение количественной оценки уровня опасности, по-прежнему, занимает продолжительное время (до трех месяцев). Согласно статистике компании Claroty [170], за 2020 г. выявлено 893 уязвимостей, что на 24,72 % больше, чем в 2019 г. Более 70 % уязвимостей получили статус критических или высокую степень опасности.

Сегодня преобладают многошаговые скоординированные распределенные атаки со сложной организацией, сложным процессом реализации, множеством целей (APT, advanced persistent threats) [186, 147]. В подобном ландшафте угроз при обеспечении кибербезопасности объектов информационной инфраструктуры на первый план выдвигается создание интеллектуальных средств защиты, позволяющих обнаруживать сложные целевые атаки еще на начальных этапах их реализации, опираясь на множество индикаторов компрометации (IOC, Indicator of Compromise) и индикаторы атак (IOA, Indicator of Attack). Подобные индикаторы позволяют описывать отдельные вредоносные объекты, действия или подозрительное поведение системы, при совпадении с ними события кибербезопасности помечаются как потенциальные элементы атаки. При сопоставлении IOC с IOA основным инструментом становится моделирование вектора атаки на различных этапах ее жизненного цикла: обнаружение уже совершенных вредоносных действий злоумышленника, определение значимости и устранение последствий, формирование рекомендаций для предотвращения возникновения инцидентов в будущем. Построение вектора атаки без применения средств компьютерной автоматизации трудоемко и требует наличия высококвалифицированных специалистов.

Большинство (92%) кибератак в 2021 г. было направлено на объекты КИИ: госорганизации, предприятия энергетики, промышленности и оборонно-

промышленный комплекс. Большая часть атак была реализована группировками со средней квалификацией с применением доступного вредоносного ПО и уязвимостей, социальной инженерии, а их основной целью являлась монетизация атаки с помощью шифрования, майнинга или вывода денежных средств. На высокопрофессиональные группировки пришлось 18 % атак. Ключевой техникой, используемой профессиональными злоумышленниками для преодоления периметра, является фишинг (60 % атак). В 50 % атак высококвалифицированные злоумышленники эксплуатируют веб-уязвимости.

Развитие цифровой экономики обусловлено эффективной работой со стремительно увеличивающимися большими объёмами данных (Big Data), а точнее, с содержательными («умными») данными (Smart Big Data) [181]. Неизбежным следствием промышленной революции 4.0 является не только ожидаемый рост эффективности, качества и производительности производства, но и все возрастающая зависимость от безопасности и надежности функционирования инфраструктуры промышленных систем автоматизации и контроля.

Предприятия внедряют системы машинного зрения, системы управления производственными процессами и их дальнейшее развитие – киберфизические системы, оперирующие «цифровыми двойниками» элементов производства, построенными на основе достоверной информации, подкрепляемой историческими данными [329, 330].

Задачи обеспечения ИБ промышленных автоматизированных систем при этом принципиально отличаются от классических задач обеспечения информационной безопасности [12, 329, 330]. С точки зрения ИБ, главным защищаемым ресурсом в АСУ ТП является сам технологический процесс, и основная цель – это обеспечить его непрерывность (т.е. доступность всех узлов) и целостность (в том числе передаваемой между узлами информации). В корпоративных информационно-вычислительных системах главный ресурс – это информация, которая обрабатывается, передается и хранится в системе, а основная цель – обеспечение ее конфиденциальности. Таким образом, поле потенциальных рисков и угроз для АСУ ТП, по сравнению с корпоративными информационными системами, расширяется рисками потенциального ущерба жизни и здоровью персонала, населения и окружающей среде.

Непрерывно возрастает сложность киберфизических систем, информационно-управляющих систем промышленных объектов, цифровых АСУ ТП топливно-энергетического комплекса, информационных систем финансового

сектора и др. На современном этапе цифрой трансформации индустрии актуальными являются вопросы поддержания работоспособности киберфизических систем (КФС), т.е. обеспечения устойчивости протекающих в них физических процессов и непрерывности управления в условиях возможных внутренних и внешних целенаправленных деструктивных воздействий. Основным направлением развития систем защиты информации для обеспечения киберустойчивости КФС является реализация опережающей стратегии защиты (проактивная защита), основанной на предсказании угрозы (предиктивный анализ) и раннем обнаружении атак с целью адаптации системы к предполагаемому деструктивному воздействию.

Для выявления целевых атак на промышленные системы необходим анализ значительного объема входящего, исходящего и внутреннего сетевого трафика и потока событий ИБ для выявления аномальной активности, анализа вектора атаки и оценки возможного ущерба. Для решения подобных задач применяется комплексный подход – развертывание центра мониторинга и реагирования на инциденты ИБ (Security Operation Center, далее – SOC), осуществляющего, в том числе, сбор, хранение и анализ трафика [165] как корпоративного сегмента, так и сегмента промышленной сети. Это позволяет выделять шаблоны проведения атак или использования уязвимостей. Основной целью управления инцидентами ИБ является обеспечение непрерывного мониторинга событий ИБ, своевременное реагирование на инциденты, устранение последствий и формирование шаблонов реагирования для предотвращения возникновения инцидентов в будущем. Следовательно, для промышленного оборудования и пограничных систем (точек входа в промышленную сеть) необходимо обеспечить анализ трафика для обнаружения сетевых атак с поддержкой анализа промышленных протоколов. Совершенствование средств защиты сетевой инфраструктуры направлено на развитие инструментов интеллектуального мониторинга сетевого трафика и состояния объектов и узлов промышленной сети.

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 оценки рисков нарушения ИБ и выбора эффективных контрмер противодействия потенциальным внешним и внутренним угрозам ИБ. В основе принятых документов – использование риск-ориентированного подхода, суть которого заключается в выявлении основных факторов, влияющих на защищенность

информационной (автоматизированной) системы, и на основе проведенного анализа формировании определенного набора организационных и технических мер (контрмер), способствующих снижению риска ИБ и обеспечению заданного (допустимого) уровня защищенности системы.

На сегодняшний день масштабируемой и переносимой методологии еще 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 управления рисками ИБ на основе анализа структурированных и слабоструктурированных данных для обеспечения устойчивости объектов КИИ на всех уровнях информационного пространства.

1.2 Анализ нормативно-правового обеспечения проблемы кибербезопасности и ИБ объекта КИИ

Согласно федеральному закону «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ [1], к **субъектам КИИ** относятся владельцы объектов КИИ, а также организации, которые обеспечивают их взаимодействие: государственные органы, государственные учреждения, российские юридические лица, индивидуальные предприниматели. Субъекты КИИ обязаны самостоятельно категорировать принадлежащие им объекты в зависимости от масштаба возможных последствий объекту КИИ. Сведения о том, является ли организация субъектом КИИ, можно получить в следующих источниках:

- общероссийский классификатор видов экономической деятельности;
- лицензии и иные разрешительные документы на различные виды деятельности;
- уставы, положения организаций (госорганов);
- другие источники.

К **объектам критической информационной инфраструктуры [1]** относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры в одной из следующих сфер: здравоохранение, наука, транспорт, связь, энергетика, банки и иные организации финансового рынка,

топливно-энергетический комплекс, атомная энергия, оборона, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленности.

Подмножеством всех объектов КИИ являются **значимые объекты КИИ [1]** – те объекты, которым присвоена одна из категорий значимости в результате категорирования.

Усилиями ученых и специалистов всего мира сегодня активно формируется необходимая законодательная и нормативно-правовая база для решения задач, связанных с обеспечением информационной безопасности объектов критической информационной инфраструктуры.

Семейство отраслевых стандартов NERC-CIP («Защита объектов критической инфраструктуры») раскрывают вопросы обеспечения защиты АСУ и сетей коммуникации для объектов энергетического сектора от потенциальных атак [325].

Семейство стандартов ANSI/ISA-99 («Безопасность промышленных систем автоматизации и управления») ANSI/ISA-62443 [324] в качестве основного принципа вводят сегментацию промышленной сети на зоны и связывающие их тракты. Концепция сегментации (зонирования) промышленных систем стала основной разработки серии стандартов обеспечения ИБ АСУ ТП нового поколения ISA/IEC 62443.

Серия международных стандартов ISA/IEC 62443 («Безопасность промышленных систем автоматизации и управления») раскрывает вопросы обеспечения доступности, целостности и конфиденциальности информации, обрабатываемой АСУ ТП, в том числе, относящимися к объектам КИИ [330].

В ноябре 2018 г. ENISA представило документ, описывающий практические рекомендации по обеспечению ИБ систем промышленного интернета вещей [319, 320].

Основные нормативные акты, регламентирующие вопросы безопасности объектов КИИ, а также сетей электросвязи, используемых для организации взаимодействия таких объектов в РФ, является ряд документов.

федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ [1].

Для раскрытия требований, предусмотренных федеральным законом 187-ФЗ, и условий их применения, ФСТЭК России издан **Приказ «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25 декабря**

2017 г. № 239 [4]. В документе представлены рекомендации по обеспечению безопасности значимых объектов КИИ на всех этапах жизненного цикла.

Одним из основных документов является **приказ ФСТЭК России от 14 марта 2014 г. № 31** «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» раскрывающий вопросы единства комплекса мер обеспечения ИБ АСУ ТП, являющихся значимыми объектами КИИ, и мер защиты информации в АСУ ТП, не являющихся такими объектами [3].

Серия стандартов ГОСТ Р МЭК 62443 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы» – является основным документом для построения системного риск-ориентированного подхода к обеспечению ИБ АСУ ТП.

Требования к системам безопасности значимых объектов КИИ регулируются **приказом ФСТЭК России от 21.12.2017 №235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».** Система безопасности значимых объектов КИИ – это совокупность организационных, технических, правовых и других мер, создаваемая для обеспечения безопасности одного объекта или совокупности объектов. Требования, описанные в приказе, едины для объектов всех трёх категорий. Допускается применять их для обеспечения безопасности незначимых объектов.

Задачи, выполняемые системой безопасности:

1. предотвращение неправомерного доступа к информации, обрабатываемой значимыми объектами;
2. предотвращение воздействия на технические средства обработки информации, в результате которого может быть нарушено или прекращено функционирование объектов;
3. восстановление функционирования объектов, если они вышли из строя;
4. непрерывное взаимодействие с ГОССОПКА.

В состав системы безопасности входят три основных элемента: силы, средства, организационно-распорядительные документы.

Требования по обеспечению безопасности значимых объектов КИИ регулируются **приказом ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».** Требования документа распространяются на все стадии жизненного цикла системы безопасности: создание, эксплуатация, вывод из эксплуатации. Если значимый объект КИИ уже функционирует, то требования должны быть выполнены при его ближайшей модернизации. Реализация требований к ИБ, описанных в Приказе, включает в себя следующие шаги:

- формирование перечня применимых требований;
- разработка организационных и технических мер;
- внедрение организационных и технических мер по обеспечению безопасности;
- обеспечение безопасности во время эксплуатации;
- обеспечение безопасности при выводе из эксплуатации.

При отсутствии возможности реализации отдельных мер защиты информации, в первую очередь рассматриваются меры по обеспечению промышленной и физической безопасности объекта.

При выборе мер следует учитывать возможные угрозы, связанные с соответствующим категории объекта уровнем потенциалом источника, а также соотношение категории значимости и требуемого класса СЗИ.

Основные категории объектов КИИ, согласно приведенным нормативным документам, представлена в таблице 1.1.

Таблица 1.1 – Категорирование объектов КИИ

Категория объекта КИИ	**Потенциал источника угроз, который следует рассматривать при выборе мер**	**Требуемый класс СЗИ**
1 категория	Высокий	Не ниже 4 класса
2 категория	Базовый усиленный	Не ниже 5 класса
3 категория	Базовый	Не ниже 6 класса

Полный текущий перечень основных документов, которыми необходимо руководствоваться при обеспечении безопасности объектов КИИ, приведен в Приложении А.

Помимо Приказа ФСТЭК № 239, в зависимости от данных, обрабатываемых объектом КИИ, следует руководствоваться следующими документами (таблица 1.2)

Таблица 1.2 – Основные руководящие документы

Объект	Документы	
Обрабатывает государственную тайну	Законодательство в области защиты гостайны	
ГИС	Приказ ФСТЭК № 239	Приказ ФСТЭК №17 от 11.02.2013 г.
ПДн		Постановление Правительства РФ №1119 от 01.11.2012 г.
ИТКС		Нормативно-правовые акты Минкомсвязи

Не смотря на обилие нормативных документов, сегодня нет общепринятых методик и подходов к комплексной 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, разветвленными системами телекоммуникаций и т.п.

1.3 Анализ моделей и методов качественной и количественной оценки рисков ИБ объекта КИИ на основе технологий интеллектуального анализа данных

Существующие методы оценки рисков ИБ делят [27-41] на две группы, связанные с качественной и количественной оценкой уровня рисков [16, 224]. К первой группе методов относятся: OCTAVE, CRAMM, COBRA, MSAT, КОНДОР и другие, целью которых является выявление и анализ основных факторов, влияющих на уровень риска ИБ, определение их уровня относительной значимости и общая качественная оценка уровня защищенности исследуемой системы, с выдачей рекомендаций по обеспечению соответствия уровня защищенности требованиям нормативных документов. Методы, предназначенные для качественной оценки рисков (такие, как метод экспертных оценок или схема нечеткого логического вывода), базируются на неполной исходной информации и дают общую, предварительную оценку уровня защищенности системы. В основе применяемых при этом методик, как правило, используются опросные карты, предоставляемые экспертам, на которые те должны ответить «да», «нет», «частично» и т.п., после чего проводится соответствующая статическая обработка мнения экспертов по определенным правилам.

Вторая группа методов включает в себя: RiskWatch, АванГард, ГРИФ, позволяющие дать количественную оценку объема потерь (ущерба) от воздействия

возможных угроз на каждый ценный ресурс информационной системы, выяснить причины возникновения риска ИБ с подробным анализом уязвимостей, оценить экономическую эффективность принятия тех или иных контрмер. Методы, основанные на количественной оценке рисков (к которым можно отнести, например, методы ситуационного анализа, марковские модели, нейронные сети и др.), требуют для своего использования более полной информации об исследуемой системе и позволяют прогнозировать не только уровень риска, но и ожидаемый потенциальный ущерб от действия угроз, что может явиться базой для принятия более обоснованных решений по снижению уровня риска.

Недостатком данной группы методов является необходимость наличия на предприятии достоверной статистики по инцидентам в сфере ИБ, включая оценки объема потерь от угроз ИБ.

Имеется также значительное число публикаций зарубежных авторов, посвященных данной теме. В качестве примера можно привести публикации [148, 154, 211], в которых рассмотрены общие вопросы реализации риск-ориентированного подхода к обеспечению ИБ сложных и критических информационных систем, анализируются лучшие практики управления ИБ на промышленных предприятиях. Как уже отмечалось выше, сегодня 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 ТП, разветвленными системами телекоммуникаций и т.п., на сегодня нет. Существующие подходы направлены, как правило, на решение частных задач, отдельных поддающихся анализу направлений и решений, что затрудняет их применение для современных высокотехнологичных объектов КИИ.

Теоретические и фундаментальные исследования в области обеспечения ИБ объектов с многоуровневой иерархической архитектурой.

В Российской Федерации рядом известных научных школ ведутся активные исследования в данной проблемной области. Так, в лаборатории проблем компьютерной безопасности, СПИИРАН [63, 64, 74, 75, 133, 328], г. Санкт-Петербург, под руководством проф. Котенко И.В. ведутся работы по созданию систем управления информацией и событиями безопасности, интеллектуализацией сервисов защиты для критически важных инфраструктур [75].

Под руководством проф. Макаревича О.Б. в Южно-Российском региональном учебно-научном центре по проблемам информационной безопасности в

системе высшей школы ведутся работы по созданию интеллектуальных систем защиты информации на базе нейросетевых технологий в задачах защиты информационно-телекоммуникационных сетей от несанкционированных вторжений [81].

На кафедре систем информационной безопасности Казанского национального исследовательского технического университета им. А.Н. Туполева – КАИ под руководством проф. Аникина И.В. разрабатываются методы оценки и управления рисками ИБ в корпоративных и информационных системах на основе технологий нечеткой логики [13, 14].

На кафедре систем информационной безопасности ФГБОУ ВО «Воронежский государственный технический университет» под руководством проф. Остапенко А.Г. ведется разработка программных комплексов риск-анализа распределенных информационных систем [95, 96]. Решаются вопросы развития методологии временного риск-анализа в приложении к важнейшим переменным состояния атакуемых автоматизированных систем управления технологическими процессами КВО.

Под руководством проф. Ажмухамедова И.М. на факультете цифровых технологий и кибербезопасности ФГБОУ ВО «Астраханский государственный университет» [5-9, 149, 198] разрабатываются методы поиска и принятия оптимальных управленческих решений в сфере риск-менеджмента для снижения значения текущего риска до целевого уровня.

На кафедре комплексной информационной безопасности электронно-вычислительных систем ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники» [65, 70, 139, 185, 221, 281] под руководством проф. Шелупанова А.А. ведутся работы по созданию методического и алгоритмического обеспечения автоматизированной интеллектуальной системы поддержки принятия решений при проведении аудита ИБ ИСПДн.

На кафедре вычислительной техники и защиты информации ФГБОУ ВО «УГАТУ» под руководством проф. Машкиной И.В. ведутся исследования [56, 82, 83, 128, 128] по управлению защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий.

В [148] разработаны практические рекомендации и методика управления рисками ИБ объектов КИИ, включающая оценочные анкеты для экспертов, перечень угроз, классификацию и оценку ресурсов, корреляции между рисками и средствами контроля и расчета остаточного риска.

В [154] предложена методология комплексной оценки рисков ИБ, в которой активы, уязвимости, угрозы и элементы управления организации связаны между собой. Основная цель исследования – сравнить и уточнить различные виды деятельности, входные данные и результаты, необходимые для каждой модели оценки рисков информационной безопасности и анализа, который эффективно устраняет риски информационной безопасности.

В [211] предлагается интегрированный инструмент поддержки принятия решений, использующий нечеткие когнитивные карты для динамической оценки риска сложных систем. Предложенный подход имеет возможность устанавливать приоритеты факторов риска и прогнозировать, и анализировать влияние каждого отдельного фактора риска / риска на другие риски или на результаты сложных и критических систем с учетом вероятности возникновения и последствий рисков, а также с учетом сложных зависимостей между факторами риска.

Подходы к разработке методологии комплексной оценки рисков ИБ объектов КИИ с применением методов машинного обучения и нечеткого когнитивного моделирования.

В качестве наиболее перспективных подходов к созданию методологии комплексной оценки рисков ИБ объектов КИИ можно указать активно ведущиеся в последние годы исследования, связанные с получением количественной оценки рисков ИБ объекта КИИ на основе технологий ИАД и когнитивного моделирования. Подобные исследования включают в себя такие направления, как:

а) разработку моделей и алгоритмов оценки рисков с использованием нечеткой логики и нейронных сетей [23, 24, 53, 71];

б) разработку моделей и алгоритмов оценки рисков с использованием технологий когнитивного моделирования [35, 69];

в) разработку моделей и алгоритмов оценки рисков с использованием динамических байесовских сетей и скрытых марковских моделей [15, 72].

Технологии когнитивного моделирования, основанные на построении нечетких когнитивных карт, сегодня успешно используются при изучении поведения сложных социально-экономических и организационно-технических систем. Преимуществами нечетких когнитивных карт (НКК, Fuzzy Cognitive Maps, FCM), предложенных в 1986 г. Б. Коско [224], являются их наглядность, выявление структуры причинно-следственных связей между элементами сложной системы, трудно поддающейся количественному анализу традиционными методами, использование знаний и опыта экспертов в исследуемой предметной

области. Известны примеры применения НКК при решении задач оценки рисков информационной безопасности [6, 33, 34, 57, 291, 314].

Вместе с тем, на практике изучение реального сложного объекта (проблема обеспечения информационной безопасности объекта КИИ) с помощью нечеткого когнитивного моделирования встречается с рядом труднопреодолимых факторов (высокая размерность пространства состояний исследуемой системы, неоднозначность выбора состава концептов и выявления наиболее существенных (значимых) связей между ними, неопределенность в оценке силы этих связей и т.д.) – т.е. все то, что составляет «проклятие размерности». Попытки разрешить эту ситуацию, как правило, связаны с представлением исходной нечеткой когнитивной карты системы в виде совокупности из нескольких, более простых с точки зрения анализа, НКК, взаимодействующих между собой по вертикали или по горизонтали. В качестве инструмента для исследования сложных систем сегодня эффективно применяются такие модификации НКК, как иерархические НКК [290], многоагентные НКК [289], многослойные (вложенные) НКК [246, 247, 251]. В отличие от иерархических и многоагентных НКК, основной упор при построении вложенных НКК (Nested FCM) делается на последовательное раскрытие неопределенностей – каждый последующий (нижележащий) слой содержит более детальную (локальную) информацию о внутренней структуре (топологии) базовых концептов исходной НКК.

Однако, анализ работ в данном направлении показывает, что большинство из них изначально не ориентированы на задачи оценки рисков ИБ сложных автоматизированных систем контроля и управления производственными объектами и процессами, не учитывают в полной мере специфику объекта и не обладают системным характером. Анализ существующих подходов к разработке моделей и методов комплексной оценки рисков ИБ объектов КИИ показывает, что решение этой проблемы возможно на основе комплексирования и адаптации методов ИАД и технологий нечеткого когнитивного моделирования. Применение методов ИАД должно обеспечить повышение оперативности и достоверности результатов комплексной оценки уровня защищенности объектов КИИ (показателей рисков нарушения 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 и выборе эффективных контрмер по защите объектов КИИ от воздействия злоумышленников и других деструктивных факторов.

1.4 Интеграция подходов и методов интеллектуального анализа и когнитивного моделирования в задаче комплексной оценки рисков ИБ объекта КИИ

Одним из современных подходов [26] к построению систем защиты информации для обеспечения киберустойчивости КФС является концепция расширенного обнаружения и устранения угроз (XDR [87], Extended Detection and Response) – рис. 1.1, где *X* – это любой источник данных (информационно-телекоммуникационная инфраструктура, конечные системы, пользователи, киберфизические объекты (КФО)), *D* и *R* – обнаружение и реагирование. Подобные системы обеспечивают видимость и контекст на этапе анализа сложных угроз с возможностью приоритезации мер по их устранению на основе агрегации и анализа данных из множества источников.

Источниками данных для XDR являются:

1) системы анализа сетевого трафика (NTA, Network Traffic Analysis) информационно-телекоммуникационной среды КФС;
2) системы управления безопасностью и автоматизации реагирования (SOAR, Security Orchestration and Automated Response), объединяющие анализ контекста и контента в виде структурированных и неструктурированных данных в системах управления информацией и событиями безопасности (SIEM, Security Information and Event Management), реализуемый с помощью:
    - системы анализа безопасности поведения пользователей и сущностей (UEBA, User and Entity behavior Analytics);
    - системы обнаружения и реагирования на угрозы для конечных точек (EDR, Endpoint Threat Detection and Response);
    - системы обмена данными об угрозах (TI, Threat hunting);
3) системы обнаружения и устранения аномалий (ADM, Anomaly Detection and Mitigation) производственных и технологических процессов КФО.

В концепции расширенного обнаружения и устранения угроз XDR важная роль отводится предиктивному анализу, выступающему в качестве одного из методов обеспечения кибербезопасности КФС. Методы предиктивного анализа направлены на выявление предпосылок неполадок и сбоев функционирования, ведущих к деградации КФО в составе КФС, на основе анализа накапливаемых

параметров их состояния. Основным инструментом предиктивного анализа является выявление аномалий в технологических временных рядах (ТВР) накапливаемых параметров состояния КФО. Под аномалией при этом понимается отклонение в функционировании КФО или отклонения, связанные с нарушением взаимодействия устройств при обмене данными в составе КФО [67, 230].

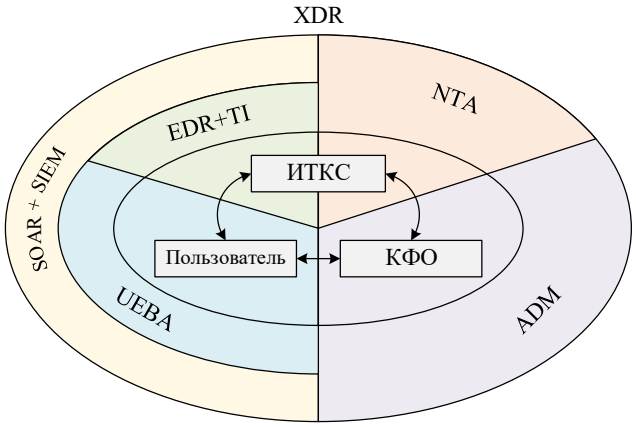


Рисунок 1.1 – Концепция расширенного обнаружения и устранения угроз (ИТКС – информационно-телекоммуникационная система)

Таким образом, применение методов, моделей и алгоритмов 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 позволят 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.

1.4.1 Анализ систем обнаружения аномалий в рамках концепции расширенного обнаружения и устранения угроз кибербезопасности

Одна из возможных [140, 263, 327] классификаций методов обнаружения аномалий и направлений их использования в задачах обеспечения кибербезопасности КФС представлена на рис. 1.2.

При построении подобных систем возникает необходимость сбора и обработки значительных объемов структурированных и слабоструктурированных данных со всех уровней КФС для формирования набора параметров, пригодных для оперативного анализа и выявления аномалий, возникающих в результате возможных действий злоумышленника. Ведущую роль при решении этой задачи

играют методы ИАД временных рядов параметров, характеризующих состояние КФО, и методы машинного обучения.

Рисунок 1.2 – Интеллектуальные методы обнаружения аномалий в рамках концепции расширенного обнаружения и устранения угроз

Применение подобных решений при обнаружении аномалий функционирования ИТКС, аномалий в поведении пользователей и аномалий параметрах КФО нашло свое отражение в ряде публикаций (таблица 1.3).

Таблица 1.3 – Применение методов ИАД и машинного обучения в задачах обнаружения аномалий в рамках концепции расширенного обнаружения и устранения угроз кибербезопасности

Тип системы	Пример
Системы анализа аномалий сетевого трафика на основе методов ИАД и машинного обучения	- Модель обнаружения гибридных аномалий в высоконагруженных сетях связи на основе методов ИАД [249]; - Платформа обнаружения аномалий для выявления кибератак на облачные вычислительные среды [252]; - Комплексная система контроля и обеспечения безопасности сбора данных, реализующая мониторинг трафика в реальном времени, обнаружение аномалий, анализ воздействия, стратегии смягчения последствий [296, 297]; - Система обнаружения аномалий на основе алгоритмов машинного обучения для устранения угроз кибербезопасности сетей Интернета вещей в умном городе [145]; - Подход на основе кластерного анализа сетевого трафика для обнаружения кибератак, вызывающих аномалии в сетях

Тип системы	Пример
	критической информационной инфраструктуры газокомпрессорных станций [219]; - Распределенная система обнаружения вторжений для систем диспетчерского управления и сбора данных [172]; - Алгоритм обнаружения аномалий и система обнаружения вторжений с фильтрацией ложных срабатываний и возможностью подтверждения атаки [293]; - Система обнаружения аномалий для обнаружения утечек конфиденциальной информации в сетевом трафике энергосистем [216]; - Методология создания надежных наборов данных для обнаружения аномалий в АСУ ТП [197]
Анализ состояния конечных систем и поведения пользователя в задаче обнаружения аномалий	- Программная платформа для обнаружения аномалий работы конечной системы в режиме реального времени на основе анализа и оценки значимых выбросов наблюдаемых параметров [203]; - Детектор аномалий для обнаружения атак на конечные системы и подсистема объяснения решения [283]; - Фильтр событий для последующего анализа на основе метода глубокого обучения для обнаружения аномальной сетевой активности из журналов конечных систем в режиме реального времени [301]; - Модели сетевых вторжений, основанных на учете человеческого фактора при реализации сложных сетевых атак [167]
Обнаружение аномалий работы КФО	- Алгоритм, основанный на гауссовском процессе (метод непараметрического машинного обучения) для мониторинга состояния установок ветрогенераторов и выявления эксплуатационных аномалий [262]; - Двухэтапная методология обнаружения аномалий в промышленных процессах [270]; - Стратегия выбора датчика и обнаружение аномалий данных с помощью методов теории информации [234]; - Компоненты онлайн-системы для диагностики и обнаружения аномалий трансформаторов силовой подстанции [164]; - Анализ отклонения прогноза нейронной сети от параметров реального объекта для выявления аномалий на водоочистной станции [196]; - Обнаружение аномального поведения с помощью метода контролируемой классификации на основе частично определенной логической функции, позволяющий извлекать закономерности из исторических измерений датчиков [173]

Основной задачей обнаружения аномалий работы КФО является разработка механизма, который не только позволяет выявлять аномалии состояния КФО, но и способен отличать имеющий место фактический отказ от проводимой кибератаки [173, 196, 214].

Рассмотрим возможную классификацию методов и алгоритмов обнаружения аномалий на основе интеллектуального анализа временных рядов параметров состояния КФО. Группа методов M_1 (рис. 1.2) основана на построении прогностической модели одномерных и многомерных временных рядов и

дальнейшем пороговом сравнении прогноза модели и реальных данных, характеризующих состояние КФО:

- модели авторегрессии (ARIMA, Auto Regressive Integrated Moving Average) и нейросетевой регрессии NARX (Nonlinear autoregressive exogenous model);
- нелинейные предикторы на основе рекуррентных нейронных сетей (Recurrent Neural Network, RNN) и сетей с долгой краткосрочной памятью (Long Short-Term Memory, LSTM).

Группа методов M_2 (рис. 1.2) основана на применении моделей, обучаемых без учителя:

- метод опорных векторов с одним классом (One-Class Support Vector machine, OSVM) – модель обучается на данных, не содержащих аномалий. Для задания порога отделения нормальных и аномальных данных необходимо иметь оценку их соотношения;
- метод изолирующего леса (Isolation Forest): ансамбль случайных деревьев решений на первых уровнях построения модели выделяет наиболее значимые аномальные данные;
- метрические методы (k-ближайших соседей, LOF (Local Outlier Factor)) основаны на оценке относительного взаимного положения данных в пространстве признаков;
- методы, основанные на кластерном анализе, оценивают удаленность точек в пространстве признаков от выделенных центров кластеров;
- методы, использующие нейросетевые автоенкодеры, строят модели, обучаемые на нормальных данных.

Группа методов M_3 (рис. 1.2) основана на построении моделей, обучаемых с учителем:

- классификация отдельных примеров наблюдений с помощью моделей, обучаемых с учителем, требует наличия размеченных исторических данных;
- методы предсказания дефектов и сбоев на основе специфических предвестников (классификация);
- прогнозирование оставшегося времени безотказной работы системы (задача регрессии).

Группа методов M_4 (рис. 1.2) понижает размерность признакового пространства описания состояния системы:

- метод главных компонент;
- вероятностный метод главных компонент.

1.4.2 Анализ аномалий состояния объектов и сущностей информационно-телекоммуникационных сетей

Наблюдается тенденция [250] к интеграции устройств промышленного Интернета вещей (IIoT) с традиционными системами сбора данных и управления (SCADA) в составе промышленных систем [50]. Глубокое проникновение IIoT в критическую инфраструктуру и производственный сектор также привело к возрастанию вероятности и количества потенциальных кибератак. Для выявления целевых атак на промышленные системы необходим анализ значительного объема входящего, исходящего и внутреннего сетевого трафика и потока событий ИБ для выявления аномальной активности, анализа вектора атаки и оценки возможного ущерба. Для решения подобных задач применяется комплексный подход – развертывание центра мониторинга и реагирования на инциденты ИБ, осуществляющего, в том числе, сбор, хранение и анализ трафика [87, 165] как корпоративного сегмента, так и сегмента промышленной сети. Это позволяет выделять шаблоны проведения атак или использования уязвимостей. Основной целью управления инцидентами ИБ является обеспечение непрерывного мониторинга событий ИБ, своевременное реагирование на инциденты, устранение последствий и формирование шаблонов реагирования для предотвращения возникновения инцидентов в будущем. Следовательно, для промышленного оборудования и пограничных систем (точек входа в промышленную сеть) необходимо обеспечить анализ трафика для обнаружения сетевых атак с поддержкой анализа промышленных протоколов. Совершенствование средств защиты сетевой инфраструктуры направлено на развитие инструментов интеллектуального мониторинга сетевого трафика и состояния объектов и узлов промышленной сети.

Одной из ключевых задач является совершенствование алгоритмов обнаружения сетевых атак в гетерогенной сети объекта КИИ на основе технологий машинного обучения в задаче обнаружения аномалий состояния объектов и сущностей (сетевого трафика [50, 51, 122], конечных систем [47], пользователей конечных систем [48, 49]) для последующей интеграции с подсистемами центра мониторинга и реагирования на инциденты ИБ.

Для создания моделей машинного обучения (ML-моделей) используются общедоступные размеченные по типам атак и режимам работы базы сетевого трафика (NSL-KDD [294], CICIDS-2017 [280], UNSW-NB15 [253], BOT-IOT и др.). Для обнаружения новых сетевых атак, реализуемых с помощью постоянно развивающегося инструментария злоумышленников, необходимо периодическое обновление тренировочных наборов с реализацией новых сценариев атак и фиксацией параметров их проведения для дообучения ML-моделей.

Так, например, в работе [295] описан стенд, построенный с применением промышленного оборудования, для исследований алгоритмов машинного обучения в задачах обнаружения сетевых атак. В ходе реализации сложных атак по различным сценариям собран сетевой трафик, соответствующий нормальной работе системы и аномальным состояниям – сетевым атакам. Особенностью этого набора данных является акцент на использование промышленных протоколов, в первую очередь, протокола Modbus в варианте Modbus-over-TCP [243].

Проведя разведку и закрепившись в промышленной сети, злоумышленник может модифицировать управляющие команды или показания датчиков, что может привести к серьезным киберфизическим последствиям. Сетевые атаки на SCADA системы условно можно разделить на три категории: разведка, внедрение управляющих команд и атаки отказа в обслуживании (DoS/DDoS).

В [295] рассматриваются разведывательные сетевые атаки сканирования для выявления возможных уязвимостей, эксплуатация которых позволит злоумышленнику закрепиться в сегменте промышленной сети. Часть атак, при реализации которых существенно возрастает количество пересылаемых пакетов, уверенно обнаруживаются стандартными сигнатурными методами. Но большая часть атак с использованием эксплоитов практически не изменяет основные характеристики трафика промышленных протоколов, что делает очень затруднительным подбор сигнатур для их обнаружения. Применение методов ML позволяет выявить особенности аномального трафика и построить соответствующий детектор.

На данный момент, применительно к промышленным сетям можно выделить следующие виды сетевых атак (таблица 1.4) [22, 322].

Из всех типов атак, реализуемых в промышленной сети, системы обнаружения сетевых атак способны наиболее эффективно справиться с сетевой разведкой, DoS-атакой, а также различными типами инъекций и атаками переполнения буфера.

Таблица 1.4 – Виды сетевых атак и типовые методы борьбы

Тип атаки	**Описание**	**Особенности реализации**	**Методы борьбы**
Переполнение буфера (buffer overflows)	Поиск уязвимостей, способных вызвать нарушение границ памяти, выполнить произвольный бинарный код от имени авторизованного пользователя	1. Подготовка кода для привилегированного выполнения. 2. Модификация последовательности команд в программе для передачи управления подготовленному коду.	- Корректировка исходных кодов программы. - Использование неисполнимых буферов. - Применение проверок выхода за границы. - Проведение проверок целостности.
Специализированные программы	Вирусы, троянский конь, сниффер, руткит	Скрытый характер функционирования в системе, сбор данных, лавинообразное распространение	- Антивирусные средства и регулярное обновление их сигнатур; - Шифрование; - Антисниффферы; - Межсетевые экраны; - Антируткиты.
Сетевая разведка	Сбор информации о сети с помощью общедоступных данных и приложений для планирования атаки	Сетевая разведка с помощью DNS- запросов, ICMP-запросов (эхо) и сканирования портов	- Блокирование ICMP эхо запросов и ответов на пограничных маршрутизаторах. - Использование систем обнаружения вторжений.
IP-спуфинг	Злоумышленник выдает себя за санкционированного пользователя системы	Вставка ложной информации или вредоносных команд в обычный поток данных	- Контроль доступа - Использование криптографической аутентификации.
Инъекции	SQL-инъекция, межсайтовый скриптинг (XSS-атака), XPath-инъекция.	Изменение параметров запроса к БД, встраивание в веб-страницу произвольного кода.	- Правила построения SQL-запросов; - Кодирование данных и управляющих символов; - Регулярное обновление.
Отказ в обслуживании (DoS)	Создание условий, при которых легитимные пользователи не могут получить доступ к системе.	Сохранение всех соединений в занятом состоянии.	- Функции анти-спуфинга. - Функции анти-DoS. - Применение систем обнаружения сетевых атак.
Phishing-атаки	Обман или социальная разработка сотрудников предприятия для воровства их идентификационных данных и передачи их для преступного использования.	Использование spam-рассылки через электронную почту или мессенджеры, применение компьютеров-ботов, методы социальной инженерии.	- Использование проверенных ресурсов; - Антивирусные средства и обновление баз сигнатур; - Обучение и подготовка сотрудников.

1.4.3 Анализ методик моделирования вектора кибератаки на основе технологий интеллектуального анализа

В общем случае кибератака представляет собой набор последовательных действий, включающих в себя комплекс мероприятий и воздействий, приближающих нарушителя к достижению цели. Одной из наиболее известных методик в области анализа кибератак является методика, основанная на моделировании сценариев их реализации на основе модели Cyber Kill Chain [217, 313].

ФСТЭК России представлена Методика моделирования угроз безопасности информации [2, 84], ориентированной на определение актуальных угроз безопасности информации, где каждый инцидент рассматривается как набор последовательных действий злоумышленника в рамках некоторого сценария. В результате определяется уровень опасности каждой угрозы безопасности информации для каждого из сценариев реализации угроз для разработки перечня актуальных угроз. Для определения всех возможных сценариев атаки [42, 44] предлагается использовать приведенные в Методике тактики и техники, а также дополнительную информацию из банка данных угроз безопасности информации (БДУ) ФСТЭК России или других баз данных компьютерных атак. На сегодняшний день основными инструментами для моделирования атак являются базы данных компании MITRE, как наиболее систематизированные источники информации о действиях злоумышленника.

База данных MITRE ATT&CK [288] представляет собой совокупность техник, которые группируются в тактики, направленные на достижение злоумышленником конечной или промежуточной цели. В отличие от тактик и техник из проекта Методики, приведенные в ATT&CK тактики подробно описывают возможные варианты поведения злоумышленника, для каждой техники представлено подробное описание и известные случаи применения, а также методы обнаружения и потенциальные меры по нейтрализации атаки. Таким образом, база данных ATT&CK позволяет детально проанализировать действия злоумышленника при моделировании кибератаки [146, 254].

Для более полного рассмотрения всех возможных шагов злоумышленников компанией MITRE был разработан стандарт CAPEC (Common Attack Pattern Enumeration and Classification) [74, 160, 257], включающий в себя перечень и классификатор шаблонов типовых атак, т.е. описание общих методов, используемых при атаках на уязвимые компоненты информационной системы. Каталог в

CAPEC представляет собой набор металшаблонов атак, сгруппированных по некоторым общим критериям. Металшаблон атаки – абстрактная характеристика конкретной методологии или техники, используемой в атаке. Хотя БДУ ФСТЭК во многом схожа с базой шаблонов атак CAPEC, она не имеет структурированной таксономии и не дает четкого понимания о том, как реализуется та или иная угроза. Кроме того, при использовании БДУ ФСТЭК нет возможности перейти от общетеоретического и высокоуровневого описания угрозы на уровень оценки конкретных действий злоумышленника при ее реализации.

В связи с этим необходимо, в дополнение к Методике ФСТЭК России, структурировать исходные данные для моделирования векторов кибератак с использованием базы CAPEC, поскольку данная база ориентирована на безопасность программных приложений и описывает используемые злоумышленником методы для эксплуатации известных слабых мест программного и аппаратного обеспечения. Целесообразно формализовывать векторы атак в виде графов атак, содержащих все возможные сценарии реализации рассматриваемой кибератаки, что позволяет наглядно оценить наиболее опасные сценарии ее реализации.

Вместе с тем, использование графов атак [64, 239, 316] в их традиционном варианте затруднено неполнотой и неопределенностью исходных данных, сложностью построения и анализа графов атак без возможности их укрупнения (т.е. композиции действий злоумышленника), а также отсутствием функциональных программных решений. Ключевой проблемой построения графов атак является сложность масштабирования подхода для сети с большим количеством конечных систем и уязвимостей.

Исходными данными для конструирования сценариев реализации атаки являются результаты работы экспертов по выявлению уязвимостей элементов ИС, а также потенциальных слабостей программного и аппаратного обеспечения. Наборы показателей системы оценки уязвимостей CVSS и базы данных угроз и уязвимостей позволяют формально описать сценарии эксплуатации уязвимостей и автоматизировать построение цепочки возможных переходов между промежуточными узлами ИС.

1.4.4 Анализ моделей параметризации текстовых описаний угроз и уязвимостей объектов КИИ и оценки степени опасности новых уязвимостей

Исследованию возможностей методов семантического анализа текстов (Text Mining) для решения задач анализа уязвимостей ПО непосредственно по их текстовым описаниям, хранящимся в базах данных (БД) уязвимостей, посвящен ряд работ [29, 37, 85, 123]. Так, в [302] предложен новый подход к структурированию описаний уязвимостей, позволяющий в явном виде выделить условия реализации уязвимости как последовательность определенных событий – действий со стороны пользователей и атакующих, что важно в первую очередь для понимания характера уязвимости и способа ее устранения.

Важность наискорейшей оценки степени опасности уязвимости с момента ее регистрации в открытых источниках обусловлена высокой вероятностью ее эксплуатации злоумышленниками. Недостаток информации о степени опасности уязвимости и ее характеристиках осложняет планирование и проведение мероприятий по защите уязвимых ИС для специалистов. Следовательно, в ходе аудита ИС и инвентаризации ПО важно иметь актуальную информацию по выявленным уязвимостям и количественным оценкам их опасности для эффективного планирования защитных мероприятий.

В [192] на примере NVD (National Vulnerability Database – хранилище данных уязвимостей, основанное на стандартах правительства США) выполнен анализ зависимости времени появления эксплоита от компонент метрик CVSS (Common Vulnerability Scoring System – общепринятый стандарт для определения степени опасности уязвимостей в программном обеспечении) уязвимостей. Показано, что существуют классы уязвимостей с очень коротким медианным временем появления эксплоитов (три дня). Отмечено, что временная задержка заполнения NIST (Национальный институт стандартов и технологий США) метрик CVSS после публикации уязвимости возросла с одного дня (для уязвимостей до 2017 года) до 19 дней (для уязвимостей, внесенных в базу в 2018 году). Напротив, среднее время появления эксплоита для уязвимостей сократилось с 296 дней в 2005 году до шести дней в 2018 году.

CVSS [20, 63] предлагает инструментарий для расчета числового показателя по десятибалльной шкале, который позволяет специалистам по безопасности оперативно принимать решение о том, как реагировать на ту или иную уязвимость. В стандарт входят три группы метрик: базовые, временные и

контекстные. Временные и контекстные метрики применяются для более точной оценки опасности. Значение метрики принято публиковать в виде пары из вектора и числового значения.

Стандарт был впервые опубликован в 2005, однако основные версии, которые можно встретить в оценках уязвимостей (CVSS 2.0 и CVSS 3.0), появились в 2007 и 2015 годах соответственно.

В [20] авторы рассматривают изменения стандарта CVSS 3.0 по сравнению с CVSS 2.0 на основе программы, разработанной для построения графов возможных атак злоумышленником. В работе показано, что новая версия CVSS устраняет неточности при оценке критичности уязвимостей по сравнению с CVSS 2.0, но все так же не является достаточной полной, авторы также отмечают, что применение версии CVSS 3.0. сложнее автоматизировать, чем CVSS 2.0.

В [326] выполнен обзор реестра уязвимостей БДУ ФСТЭК России, коммерческих реестров уязвимостей (VulnDB, Secunia Advisory and Vulnerability Database и их иные аналоги), общедоступных источников, таких, как: CVE List, NVD, Vulnerability Notes Database. Автор отмечает, что большое разнообразие реестров и баз данных уязвимостей породило, в числе прочего, проблему синхронизации оценок уязвимостей из-за различий в системах скоринга. На сегодняшний день принято считать «официальными» оценки уязвимостей из реестра NVD.

При этом, в [152] авторы исследуют вопрос надежности и точности баз данных уязвимостей с учетом качества данных NVD. Обнаружена непоследовательность и неполнота данных в NVD, которые могут повлиять на их практическое использование. Авторы продемонстрировали влияние, которое могут оказать эти проблемы с данными, сравнивая анализы с использованием оригинальной и предложенной исправленной версией NVD.

Исследованию возможностей методов семантического анализа текстов для решения задач анализа и прогнозирования опасности уязвимостей ПО непосредственно по их текстовым описаниям, хранящимся в БД уязвимостей, посвящен ряд работ [79, 101, 175, 187, 202, 218, 232, 286, 302]. Так, в [302] авторы проанализировали появление новых записей CVE (база данных общеизвестных уязвимостей информационной безопасности) за 23 месяца и установили, что в среднем существует 132-дневный разрыв между объявлением уязвимости MITRE (некоммерческая организация, специализирующаяся в области системной инженерии) и моментом, когда NIST определяет уровень опасности уязвимости и метрики CVSS. Предложена система анализа уязвимостей, позволяющая прогнозировать

эксплуатацию уязвимости и выполнять оценку компонент метрик CVSS, используя текстовые данные обсуждения Twitter, собранные за три дня после даты первого упоминания уязвимости.

Авторы статьи [286] решают задачу оценки степени опасности уязвимостей в два этапа, на первом из которых осуществляется векторизация (Word Embedding) текстовых описаний уязвимостей, а на втором производится классификация полученных векторов (наборов уникальных признаков описаний) с помощью методов машинного обучения.

В работе [202] используется аналогичный подход к оценке степени опасности уязвимостей, предполагающий на начальном этапе формирование словаря векторов слов для каждого описания уязвимости (для этого используется модель Skip-Gram алгоритма Word2Vec), а затем извлечение признаков текста на уровне предложений и классификация полученного вектора описаний уязвимости с помощью сверточной нейронной сети.

В работе [175] использованы модели машинного обучения и обработки естественного языка для прогнозирования последствий кибератак. Представлена модель векторизации текстовых описаний новых кибератак и прогнозирования последствий для конечных пользователей. Создан набор данных о кибератаках с указанием их технических и нетехнических последствий. При помощи методов вложения слов (Doc2Vec) подготовлены данные для ансамбля моделей машинного обучения (LinearSVC, NB, MLP), оценка качества прогнозирования составила до 60 %.

В работе [187] предложена модель для прогнозирования компонент базовой метрики CVSS с возможностью объяснения прогноза, которая использует текстовые описания новых уязвимостей. Применяются технологии Bag-of-Word и оценка энтропии вхождения слов в текстовые описания.

В работе [218] рассмотрен метод оценки CVSS на основе текстовых описаний уязвимостей из базы данных OSVDB. Выполнено извлечение и предобработка текстового описания уязвимостей, использованы методы LDA и PCA для уменьшения размеров вектора признаков, применены алгоритмы SVM и Random Forest, а также нечеткие системы для прогнозирования оценок компонент оценки CVSS. Лучший предиктор был получен с помощью нечеткой системы с точностью прогноза по шкале CVSS на уровне 88 %.

Методы работы с данными об уязвимостях направлены на решение трех основных задач:

1. определение степени опасности уязвимости;

2. оценка вероятности реализации уязвимости;

3. построение модели рисков и угроз на основе данных уязвимостей.

При этом, задача определения степени опасности уязвимости (CVSS score) является основной, поскольку данные оценки используются для решения следующих задач.

Методы оценки CVSS метрик в основном реализованы на базе статистических алгоритмов и методов ИИ. Популярными являются подходы «мешок слов», инструменты снижения размерности векторов LDA и PCA, модели классификации SVM, Random Forest, а также нечеткие системы [187, 218]. Экспериментальная часть в [218] показала, что по сравнению с SVM и Random Forest, нечеткие системы показали более точный результат, а также были намного проще и быстрее.

Не менее важной задачей является оценка вероятности использования уязвимости (*эксплойты*). В [166] авторы, на основе 23-месячной статистики, говорят о том, что от момента раскрытия информации об уязвимости и до момента появления CVSS метрик в базе NVD проходит в среднем 132 дня. Система состоит из нескольких предикторов, в качестве исходных данных, использующих данные за 3 дня из обсуждений в Twitter после даты раскрытия уязвимости.

В [192] на основе анализа данных NVD и базы данных эксплойтов обнаружено, что существуют классы уязвимостей с очень коротким медианным временем использования (всего три дня).

В работах [175, 190, 277] посвященных прогнозированию эксплойтов и оценке угроз, используются подходы интеллектуального анализа текста. Описывается построение систем предсказания на основе моделей FastText, Doc2Vec.

1.4.5 Анализ графовых моделей текстовых описаний угроз и уязвимостей

В [257] решается задача поиска подходящих шаблонов атак в базе данных CAPEC по запросу пользователя (специалиста по ИБ). При этом, в соответствии с технологией Text Mining, шаблоны атак рассматриваются как элементы многомерного векторного пространства, в котором с помощью меры семантической близости осуществляется кластеризация шаблонов атак. Результаты, в свою очередь, отображаются в виде соответствующих диаграмм.

В работе [205] предложено связать тактики и техники из MITRE ATT&CK Matrix, CWE, CVE и список CAPEC на основе существующих в гипертекстовых

документах перекрестных ссылок. Сохраняются все дескрипторы безопасности объектов ИС и взаимосвязи источников, одновременно обеспечивается двунаправленная реляционная связь в результирующем графе. Ограничения подхода: используются только данные NVD, и не учитывается множество уязвимостей из других баз и уязвимостей, не имеющих идентификаторов CVE. Данные для построения взяты из разных источников и не всегда удается сохранить непротиворечивость и полноту результирующего графа.

В статье [312] предлагается объединить дескрипторы из отдельных баз данных (CVE, CWE, CAPEC) в согласованный граф знаний. Предложен метод построения графа знаний, который включает не только реляционную, но и текстовую информацию о дескрипторах безопасности в непрерывном векторном пространстве, развивая методы построения вложений для текстовых данных (Word2Vec).

Для взаимодействия с иерархией классов атак, представляющих текстовые, категориальные и ссылочные данные в документах CAPEC, в работе [258] применяется визуализация двудольного графа ссылок на шаблоны атак на дескрипторы CWE.

NVD предоставляет возможность экспорта описаний уязвимостей в машиночитаемых форматах. Часть записей CVE не содержат меток Common Platform Enumeration (CPE) -version, -product и -vendor, что затрудняет автоматическое обнаружение уязвимостей. В работе [309] предложена процедура автоматического сопоставления перечней CVE с CPE с помощью алгоритмов машинного обучения, реализующих методы распознавания именованных сущностей (NER).

Таким образом, предпринимаются активные усилия по разработке методов и подходов к построению семантических моделей для формализации знаний о текстовых описания угроз и уязвимостей объектов на основе технологий Text Mining.

1.5 Концепция комплексной оценки рисков ИБ объектов КИИ с применением технологи нечеткого когнитивного моделирования и методов машинного обучения

Обеспечение ИБ объектов КИИ является комплексной проблемой, требующей решения разнообразных задач: идентификации активов в рамках выбранной области деятельности; определения ценности идентифицированных

активов; идентификация угроз и уязвимостей для идентифицированных активов; оценка рисков для возможных случаев успешной реализации угроз информационной безопасности в отношении идентифицированных активов автоматизированной системы управления технологическими процессами предприятий; выбор критериев оценки рисков; подготовка плана обработки рисков. Становится необходимым также и анализ значительного объёма входящего и исходящего сетевого трафика и потока событий информационной безопасности для выявления аномальной активности, анализа вектора атаки и оценки возможного ущерба.

Особая роль отводится применению технологий интеллектуального анализа данных, позволяющих дать более точную количественную оценку рисков ИБ и, как следствие, обеспечить более обоснованный выбор компонент объекта КИИ и необходимых контрмер для реализации стратегии многоуровневой эшелонированной защиты (defense in depth).

Разработана 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.

Глава 2. 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, 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 [10, 19, 25, 27-30, 34, 37, 40-43, 47, 48, 50-52, 73, 78, 85, 88-90, 92, 104, 106, 113, 171], 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.

2.1 Общие требования к комплексу моделей для оценки рисков ИБ объекта КИИ

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.).

На сегодняшний день систематизированные текстовые описания, характеризующие различные аспекты безопасности программного и аппаратного обеспечения информационной инфраструктуры, консолидированы в виде слабосвязанных групп иерархических гипертекстовых документов в отдельных базах данных [74, 133, 321, 326]:

- CVE (Common Vulnerabilities and Exposures) – база данных (стандарт) в области унификации именования и регистрации обнаруженных уязвимостей ПО;
- CWE (Common Weakness Enumeration) – база данных недостатков (слабых мест) ПО, которые могут быть использованы нарушителями при проведении атак;
- NDV (NIST National Vulnerability Database) – представительная база данных уязвимостей ПО;
- CVSS (Common Vulnerability Scoring System) – система рейтинговой оценки опасности уязвимостей ПО;
- CAPEC (Common Attack Pattern Enumeration and Classification) – стандарт описания классов атак и их иерархических отношений, каталог известных кибератак;
- MITRE ATT&CK Matrix – формальное описание техник и тактик реализации кибератак;

- CPE (Common Platform Enumeration) – формальный язык описания всех возможных продуктов, операционных систем и аппаратных устройств при описании уязвимостей;
- Банк данных угроз безопасности информации (БДУ) ФСТЭК России – база данных уязвимостей и угроз.

В феврале 2021 года утвержден методический документ ФСТЭК России «Методика оценки угроз безопасности информации» [2] (далее – Методика), который определяет порядок моделирования и оценки актуальности угроз и возможные сценарии их реализации в информационных системах на основе БДУ ФСТЭК и перечисленных выше баз данных компьютерных атак.

Широкое применение получили различные системы классификации и оценки критичности уязвимостей (NIPC, SANC, nCircle, CVSS, WIVSS, и др.) [133].

В то же время, возможность открытого доступа к подобной информации еще сама по себе не гарантирует ее эффективность, поскольку специалист по ИБ пока вынужден «вручную» справляться с огромным объемом данных. Так, база данных NDV по состоянию на начало 2021 года содержит более 150 тысяч записей об уязвимостях, а БДУ ФСТЭК России – около 30 тысяч записей об уязвимостях и 222 записи об угрозах безопасности информации. Указанная информация хранится в виде текстовых описаний, анализ которых требует существенных временных затрат и определенных профессиональных навыков. Поэтому понятен тот интерес, который сегодня проявляется к использованию методов семантического (интеллектуального) анализа текстов [7, 8, 18, 21, 310], применение которых позволило бы решить в какой-то степени проблему автоматизации поиска и анализа необходимой специалисту конкретной информации в перечисленных выше источниках данных. Во многих исследованиях сегодня активно поднимается проблема автоматизации поиска и анализа уязвимостей ПО с использованием существующих БД и систем оценки уязвимостей [179, 292].

На основе семантического сходства текстовых описаний, заимствованных из БДУ ФСТЭК России и баз CAPEC и MITRE ATT&CK, предлагается построение и формализация логической цепочки: «множество выявленных уязвимостей ПО → множество релевантных угроз → множество наиболее вероятных сценариев реализации угроз → возможные киберфизические последствия → количественная оценка рисков ИБ» с учетом требований нормативных документов

ФСТЭК. Формализация логических отношений выполнена в нотации семантических моделей и нечетких когнитивных моделей.

«Методика оценки угроз безопасности информации» ФСТЭК России [2] ориентирована прежде всего на оценку антропогенных угроз безопасности информации (БИ), вызванных действиями внешних и внутренних нарушителей (злоумышленников). Основные этапы оценки угроз БИ при этом включает в себя:

1) определение негативных последствий, которые могут наступить от реализации (возникновения) угроз БИ;

2) определение возможных объектов воздействия угроз БИ;

3) оценка возможностей реализации (возникновения, угроз БИ и определение их актуальности).

В качестве модели угрозы ИБ таким образом рассматривается следующая формула:

$$УБИ_i = [\text{нарушитель (источник угрозы); объекты воздействия; способы реализации угроз; негативные последствия}].$$

Актуальность возможных угроз БИ определяется в данном случае наличием сценария их реализации, что в свою очередь, предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно нарушителем с использованием существующих уязвимостей объектов воздействия. В качестве исходных данных для оценки угроз БИ могут использоваться общий перечень угроз, содержащихся в БДУ ФСТЭК России, а также описания векторов атак (шаблоны) компьютерных атак, содержащиеся в международных базах знаний и др.

«Методика оценки угроз безопасности информации» ФСТЭК России [2] определяет порядок моделирования и оценки актуальности угроз для всех типов ИС на основе перечня актуальных уязвимостей. Функциональная модель оценки угроз и сценариев их реализации на основе перечня уязвимостей представлена на рис. 2.1.

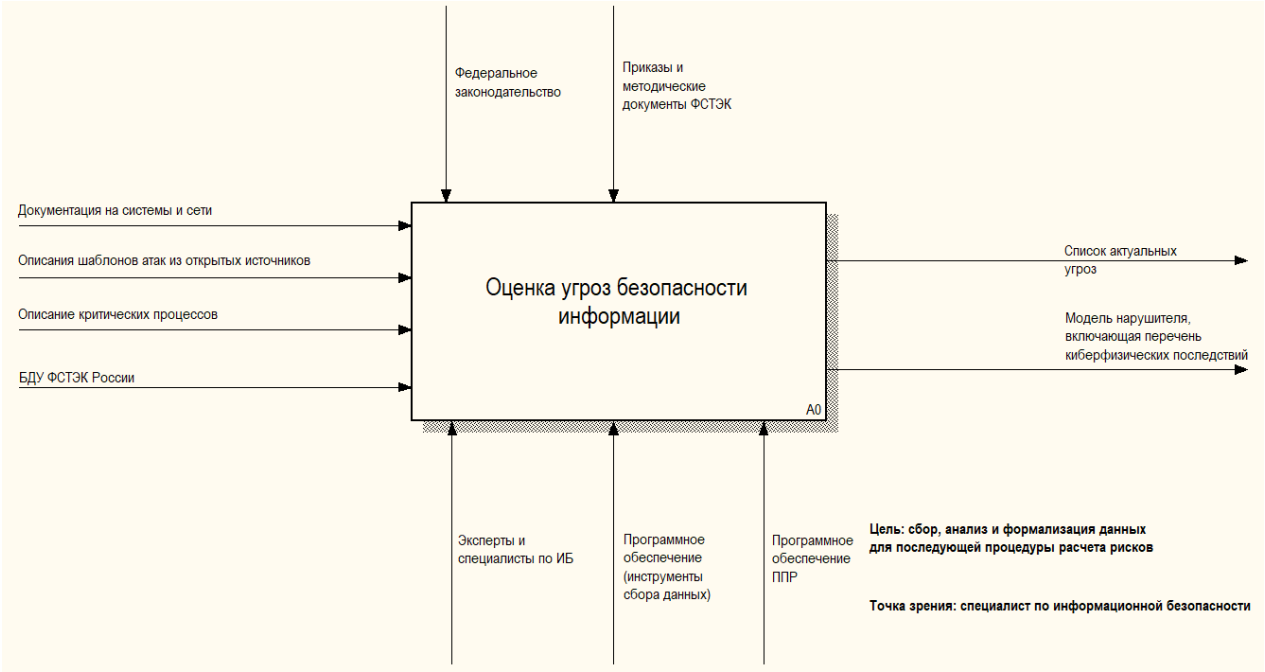


Рисунок 2.1 – Функциональная модель методики оценки угроз безопасности информации

Декомпозиция первого уровня функциональной модели раскрывает стратегический (определение нарушителя, целей воздействия, основных негативных последствий) уровень построения модели угроз (рис. 2.2).

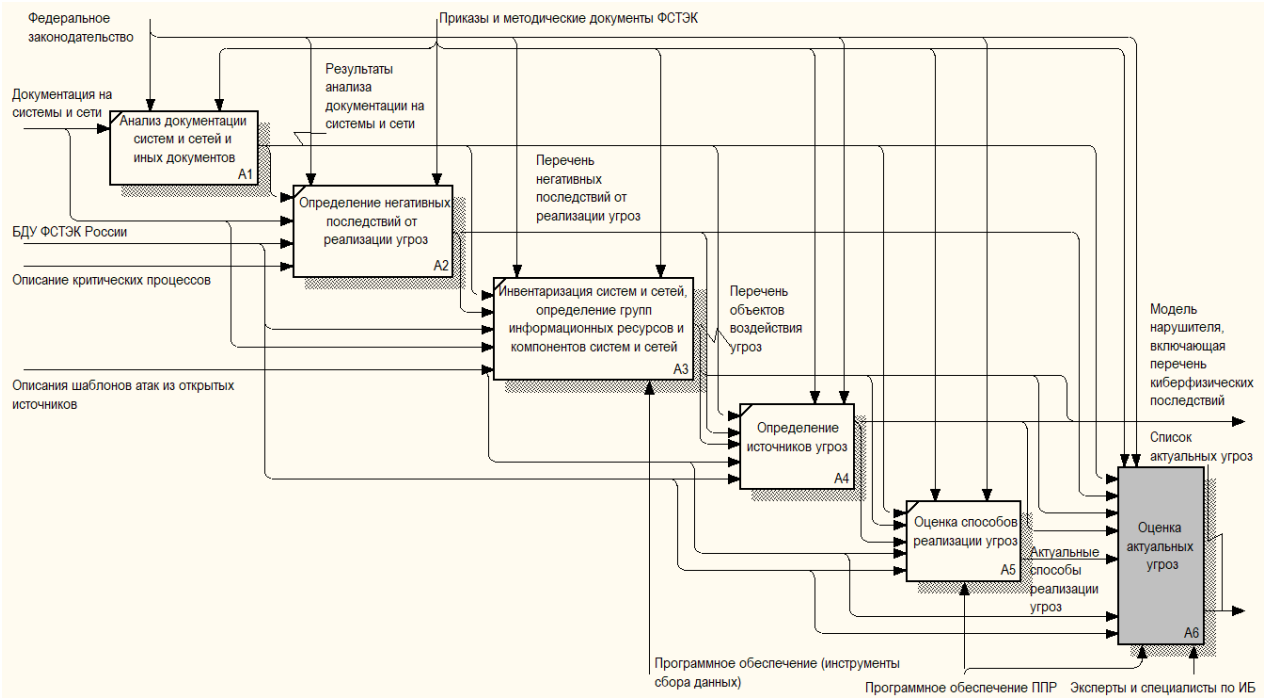


Рисунок 2.2 – Функциональная модель методики оценки угроз безопасности информации

Наибольших усилий и временных затрат со стороны эксперта требует оценка перечня актуальных угроз из списка возможных и построение сценариев их реализации на основе совокупности тактик и техник (декомпозиция блока А6, рис. 2.3).

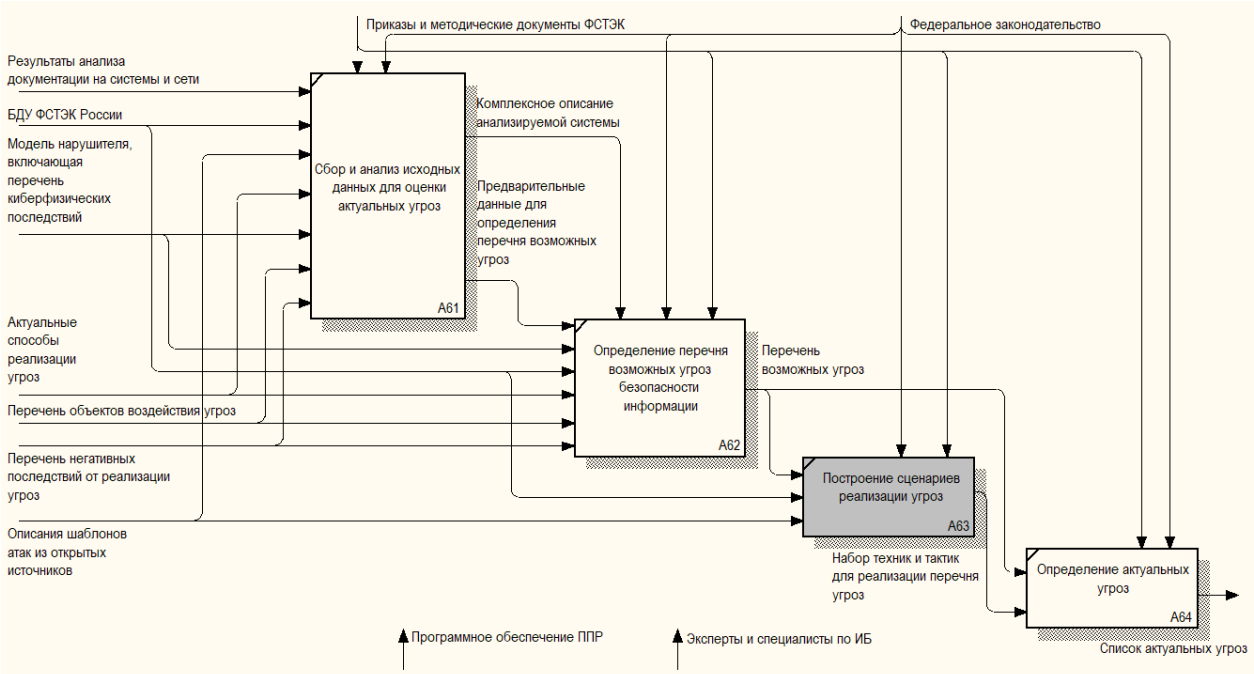


Рисунок 2.3 – Второй уровень декомпозиции блока А6 функциональной модели методики оценки угроз безопасности информации

Проблемой является отсутствие инструментов поддержки принятия решений в задаче подбора возможных техник и тактик для построения сценариев реализации угроз на основе подготовленных на предыдущих шагах (А63-А64 на рис. 2.3) перечней актуальных уязвимостей, типов доступа, типов нарушителей, видов ущерба, объектов воздействия, целей и т.п.

Методика объединяет стратегический (определение нарушителя, цели воздействия, основные негативные последствия) и тактический (применяемые тактики и техники эксплуатации уязвимостей, образующие возможные сценарии реализации угроз) уровни построения модели угроз. Основные затруднения при использовании текущей редакции Методики заключаются в трудоемкости разработки сценариев [324] (декомпозиция блоков А5 и А6 на рис. 2.2) и их слабой связанности с сформированными на предыдущих шагах (А1-А4 на рис. 2.2) перечнями актуальных уязвимостей, типов доступа, типов нарушителей, видов ущерба, целей и т.п., а также в отсутствии инструментов поддержки принятия решение и моделирования сценариев реализации угроз.

Следовательно, актуальным является автоматизация низкоуровневого моделирования сценариев эксплуатации уязвимостей и реализации угроз на основе описания шаблонов компьютерных атак, содержащихся в базах данных и иных источниках, опубликованных в сети «Интернет». Для этого предлагается обобщить рассмотренные ранее подходы к построению семантических моделей

текстовых описаний угроз и уязвимостей объектов ИС, рассмотренные в [324] методы оценки актуальных угроз и уязвимостей на основе технологий Text Minining, и технологии когнитивного моделирования, предложенные в [11, 31, 42].

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

Собранные данные позволяют перейти к построению когнитивной модели оценки рисков ИБ для целевых сущностей в зоне объекта КИИ, что позволит получить детализированную оценку рисков ИБ и сделать более обоснованный выбор средств защиты информации за счет возможности моделирования различных сценариев реализации угрозы. Исходными данными для построения когнитивных карт являются не только экспертные оценки, но и формализованные и систематизированные данные из открытых баз данных угроз и уязвимостей, что существенно повышает обоснованность и полноту моделирования.

2.2 Модели параметризации угроз и уязвимостей на основе семантического анализа текстовых описаний

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

Предлагается при анализе описания уязвимостей ПО использовать дополнительно информацию, полученную путем сопоставления описаний этих уязвимостей с описаниями спроецированных (связанных с ними) угроз, взятыми из БД угроз.

Основное внимание уделено установлению аналогий (семантического сходства) текстовых описаний, заимствованных из БДУ ФСТЭК России, позволяющий выстроить логическую цепочку: «выявленная уязвимость ПО → целевой объект воздействия злоумышленника → множество релевантных угроз». В методическом плане излагаемый подход наиболее близок к подходу, использованному авторами публикации [121], где предложена методика автоматизированного определения взаимосвязей между выявленными уязвимостями ПО и

угрозами безопасности информации с использованием БДУ ФСТЭК России. Вместе с тем, последующее изложение существенно отличается от рассмотренного в [121] не только большей общностью постановки рассматриваемой задачи, но и использованием большего разнообразия методов Text Mining, что заметно повышает эффективность процедуры анализа.

Для того чтобы перейти к использованию методов машинного обучения, необходимо прежде всего произвести предварительную обработку текстовых описаний уязвимостей, записанных на естественном языке с помощью следующих операций [99]:

– нормализация (приведение текста к более простому виду удаление знаков пунктуации, аббревиатур, стоп-слов, не несущих смысловой нагрузки союзов, предлогов, междометий.);

– стеммизация (приведение слова к его корню, путем устранения суффиксов, приставок, окончаний);

– лемматизация (приведение слова к смысловой канонической форме – инфинитив, именительный падеж единственного числа и т.д.).

Следующим шагом преобразования полученного «рафинированного» текста является переход от слов и предложений к их векторному представлению в многомерном семантическом пространстве признаков.

Широкую известность в качестве метода векторного представления слов (Word Embedding) получил разработанный в 2013 г. группой исследователей под руководством Т. Миколова (корпорация Google) алгоритм Word2Vec [244]. Данный алгоритм обучается на прочтении большого количества документов (в нашем случае – текстовых описаний из БД уязвимостей) с последующим запоминанием того, какое слово возникает в схожих контекстах. По завершении процесса обучения на достаточном количестве данных Word2Vec генерирует вектор заданной длины для каждого слова в образованном таким образом словаре, в котором слова со схожим значением располагаются ближе друг к другу. Разновидности данного алгоритма – модель непрерывного «мешка слов» (Continuous Bag-Of-Words, CBOW), когда по текущему слову в предложении предсказываются слова из его контекста, и модель Skip-Gram, когда по окружению слова, т.е. по его контекстным словам, предсказывается центральное слово сегмента текста. В качестве расширения алгоритма Word2Vec предложен алгоритм Doc2Vec. Он формирует так называемый paragraph vector (вектор абзаца) – алгоритм обучения без учителя, который создает пространство признаков фиксированной длины из

документов разной длины. Для оценки меры семантической близости слов (точек в рассматриваемом многомерном пространстве) при этом могут использоваться различные метрики расстояния (евклидова, косинусная метрика и др.) [21, 143].

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. 2.4)**.

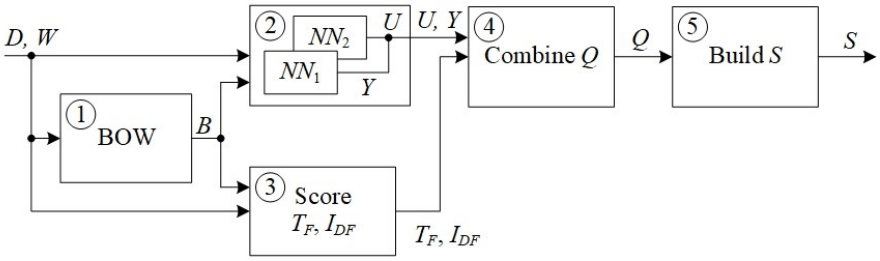


Рисунок 2.4 – Модель параметризации и оценки семантической близости текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения объектов КИИ, где
D – множество текстовых описаний; W – множество уникальных термов;
B – разреженная матрица вхождений термов; NN_1, NN_2 – 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

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. Ключевым элементом структуризации – выстраивания отношений между сущностями (угрозы, уязвимости, объекты воздействия) – является оценка семантической близости их текстовых описаний на основе косинус-расстояния между векторами вложений, построенных с помощью предобученных моделей Doc2Vec и Word2Vec для русского языка:

$$similarity = cos(\theta) = \frac{A \cdot \mathrm{B}}{\|A\| \cdot \|B\|} = \frac{\sum_{i=1}^{n} A_i B_i}{\sqrt{\sum_{i=1}^{n} A_i^2} \cdot \sqrt{\sum_{i=1}^{n} B_i^2}}, \quad (2.1)$$

где A и B – векторы формализованных признаков текстовых описаний.

В литературе отмечается [141, 177, 238], что модели вложений Doc2Vec или Paragraph2Vec не всегда пригодны для обработки коротких документов, как и в рассматриваемой задаче. Поэтому предлагается строить вектор формализованных признаков для текстовых описаний как комбинацию вектора вложений модели Doc2Vec и взвешенной с помощью коэффициентов TF-IDF суммы векторов вложений каждого слова из документа, полученных с помощью модели Word2Vec CBOW.

Коэффициенты TF-IDF [212] определяются следующим образом:

TF (*term frequency*) – отношение числа вхождений некоторого слова к общему числу слов документа.

$$\mathrm{tf}(t,d) = \frac{n_t}{\sum_k n_k} \quad (2.2)$$

где n_t – число вхождений слова в документ, а $\sum_k n_k$– общее число слов в документе.

IDF (*inverse document frequency*) – инверсия частоты, с которой некоторое слово встречается в документах коллекции.

$$\mathrm{idf}(t,D) = log\frac{|D|}{|\{d_i \in D \mid t \in d_i\}|} \quad (2.3)$$

где |D| — число документов в коллекции;

$|\{d_i \in D \mid t \in d_i\}|$– число документов из коллекции , в которых встречается

Итоговая мера TF-IDF определяется как:

$$\text{tf-idf}(t,d,D) = \mathrm{tf}(t,d) \times \mathrm{idf}(t,D) \quad (2.4)$$

Следовательно, результирующий вектор формализованного представления вложений на уровне документа и взвешенной комбинации на уровне отдельных слов в документе рассчитывается как:

$$TFIDF_1 \times \overset{W_1}{\begin{bmatrix} W_{11} \\ W_{12} \\ \dots \\ W_{1n} \end{bmatrix}} + TFIDF_2 \times \overset{W_2}{\begin{bmatrix} W_{21} \\ W_{22} \\ \dots \\ W_{2n} \end{bmatrix}} + \dots + TFIDF_m \times \overset{W_m}{\begin{bmatrix} W_{m1} \\ W_{m2} \\ \dots \\ W_{mn} \end{bmatrix}} = \overset{W2V(TF\text{-}IDF)}{\begin{bmatrix} \frac{W_{11}^* + W_{21}^* + \dots W_{m1}^*}{m} \\ \dots \\ \frac{W_{1n}^* + W_{2n}^* + \dots W_{mn}^*}{m} \end{bmatrix}}$$

$$D2V = \begin{bmatrix} U_1 \\ U_2 \\ \dots \\ U_n \end{bmatrix} \quad (2.5)$$

$W = \{W2V; D2V\}$	

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

2.2.2 Модель количественной оценки степени опасности новых уязвимостей

Целью является повышение точности и оперативности оценки степени опасности уязвимостей с помощью прогнозирования компонент метрики на основе анализа текстового описания.

Анализ публикаций также показал, что прогнозирование оценки метрики CVSS опасностей уязвимостей выполнено для англоязычных описаний уязвимостей. Открытым остается вопрос о повышении оперативности оценки степени опасности уязвимостей для программных продуктов и систем, распространенных на локальных рынках, и для которых описания уязвимостей представлены, например, на русском языке. На примере БДУ ФСТЭК России рассмотрим возможность прогнозирования компонент базовой метрики CVSS 2.0/3.0 и оценки степени опасности уязвимостей на основе технологий Text Mining. Компоненты базовой метрики CVSS 2.0/3.0 представлены в таблице 2.1.

Таблица 2.1. Компоненты базовой метрики CVSS 2.0/3.0

Метрика	Буквенное обозначение	Возможные значения
Способ получения доступа (Access Vector – v2) (Attack Vector – v3)	AV	Physical (v3.0)
		Local (v2.0, 3.0)
		Adjacent (v2.0, 3.0)
		Network (v2.0, 3.0)
Сложность эксплуатации уязвимости (Access Complexity – v2) (Attack Complexity – v3)	AC	Lower (v2.0, 3.0)
		High (v2.0, 3.0)
		Medium (v2.0)
Показатель аутентификации (Authentication – v2) (Privileges Required – v3)	Au (v2.0) Pr(v3.0)	None
		Low (v3.0)
		High (v3.0)
		Single (v2.0)
		Multiple (v2.0)
Влияние на конфиденциальность	C	None
		Low (v3.0)
		High (v3.0)
		Partial (v2.0)
		Complete (v2.0)
Влияние на целостность	I	None

		Low (v3.0)
		High (v3.0)
		Partial (v2.0)
		Complete (v2.0)
Влияние на доступность	A	None
		Low (v3.0)
		High (v3.0)
		Partial (v2.0)
		Complete (v2.0)
Необходимость взаимодействия с пользователем (User Interaction)	UI	None (v3.0)
		Required (v3.0)
Границы эксплуатации (Scope)	S	Unchanged (v3.0)
		Changed (v3.0)

Оценка степени опасности уязвимости на основе базовой метрики (CVSS 2.0) определяется как:

$$BaseScore = (0{,}6 \cdot Impact + 0{,}4 \cdot Exploitability - 1{,}5) \cdot f(Impact), \quad (2.6)$$

где оценка воздействия:

$$Impact = 10{,}41 \cdot (1 - \big(1 - C \cdot (1 - I) \cdot (1 - A)\big), \quad (2.7)$$

оценка возможности эксплуатации:

$$Exploitability = 20 \cdot AC \cdot Au \cdot AV,$$
$$f(Impact) = 0, \text{ если } Impact = 0;$$
$$f(Impact) = 1{,}176 \text{ в других случаях.} \quad (2.8)$$

Следовательно, возможно два подхода для оценки BaseScore CVSS 2.0/3.0:

– построение ансамбля предикторов для оценки отдельных значений компонент (AV, AC, Au, C, I, A) по формализованному текстовому описанию с последующим расчетом по (2.6)-(2.8) результирующего значения;

– построение модели регрессии для непосредственной оценки результирующего значения по формализованному текстовому описанию.

Разработана **модель количественной оценки степени опасности новых уязвимостей (рис. 2.5)**, для которых экспертная оценка метрики CVSS 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.

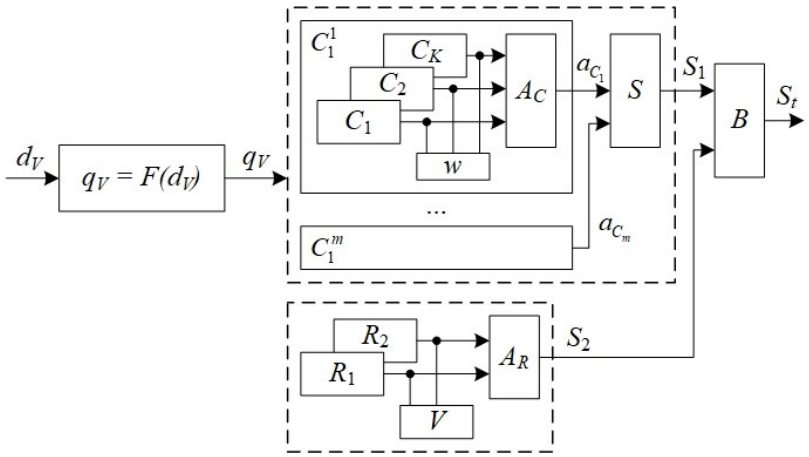


Рисунок 2.5 – Ансамбль моделей для прогнозирования базовой метрики оценки степени опасности уязвимости на основе формализованного текстового описания
d_V – текстовое описание уязвимости, q_V – формальный вектор признаков текстового описания; C – ансамбль моделей-классификаторов набора метрик; R – модели-регрессоры 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.

Применение модели позволяет получить оценку метрики опасности (и ее компонент) зарегистрированной уязвимости на основе анализа семантической близости ее текстового описания к уже имеющимся в реестре записям. Ансамбль моделей позволяет получить оценку компонент метрики опасности уязвимости CVSS на уровне F_1 = 0,80-0,85 и оценку MSE =0,865 для ансамбля регрессоров.

2.2.3 Семантическая модель текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения

Для автоматизации низкоуровневого моделирования сценариев эксплуатации уязвимостей и реализации угроз на основе описания шаблонов компьютерных атак, содержащихся в базах знаний (БДУ ФСТЭК России и баз 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. 2.6)** 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 $v_i, v_j \in V$.

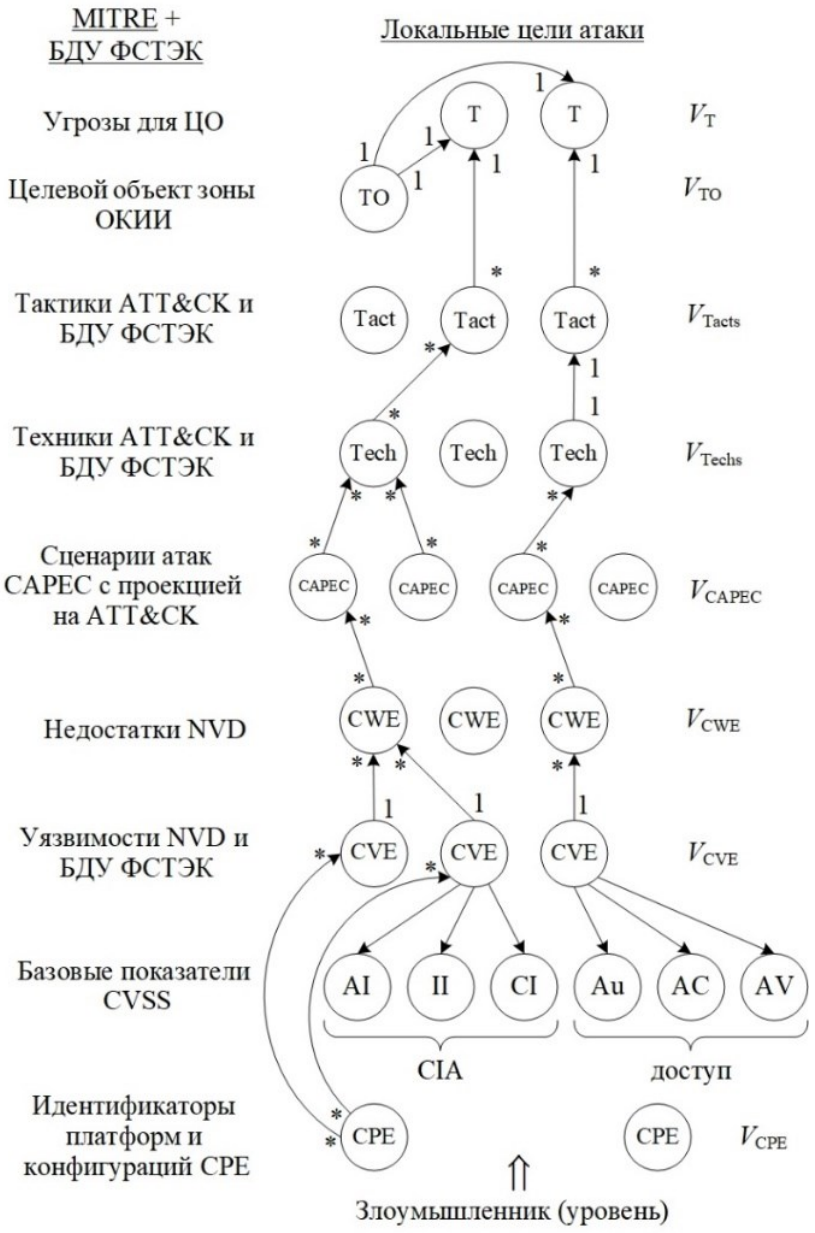


Рисунок 2.6 – Семантическая модель текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения объектов КИИ в задаче анализа актуальных угроз и уязвимостей.

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;

Семантическая модель G текстовых описаний угроз и уязвимостей объектов зоны КИИ строится на основе перекрестных ссылок (r) в гипертекстовых

документах (текстовых описаний объектов ИС – *V* графа) с поддержкой основных типов отношений между сущностями в нотации реляционных моделей и в нотации UML диаграмм вариантов использования. Дополнительно ребра модели нагружаются весовым коэффициентом $D(r)$, характеризующим метрику семантической близости текстовых описаний смежных вершин.

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).

2.3 Модели обнаружения аномалий состояния объектов и сущностей в зоне анализируемого объекта КИИ

На этапе анализа сценариев реализации угроз с возможностью приоритезации 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. 2.7)**, 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 / сенсоров в зоне безопасности объекта КИИ. Аномалии представляют собой отрезки временного ряда. Применение адаптивного оконного анализа позволяет выделять непрерывные подпоследовательности ВР, для которых выполняется процедура построения признакового описания на основе статистических функций (среднее, отклонение от среднего, минимальное и максимальное значение и пр.), параметрических моделей, приближающих сегмент ВР, семейства регрессионных моделей (линейных и авторегрессионных) и нелинейных нейросетевых авторегрессионных моделей.

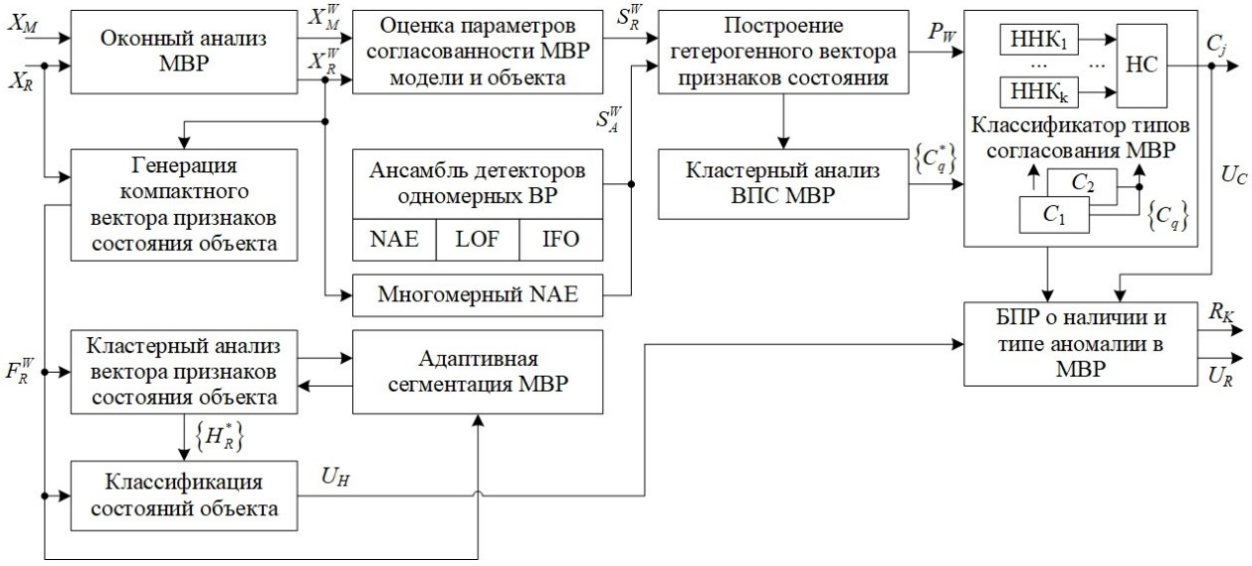


Рисунок 2.7 – Модель обнаружения аномалий состояния объектов подсистемы в зоне объекта КИИ

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 в состоянии объекта КИИ, пользователя конечной системы, пользовательского окружения объекта КИИ.

2.3.1 Система обнаружения аномалий наблюдаемых параметров состояния киберфизического объекта

Структурная схема предложенной системы обнаружения аномалий технологического процесса, основанная на применении методов анализа собираемых данных телеметрии, позволяющая выявить действия злоумышленника, получившего доступ в промышленную сеть управления технологическим процессом, представлена на рис. 2.8. Технологические временные ряды представляют собой последовательность измерений, собранных с датчиков промышленных объектов. Аномалии представляют собой отрезки временного ряда. На этапе предварительной обработки входные данные подвергаются нормализации и фильтрации. С

помощью метода скользящего окна из временных рядов набора данных формируются обучающие и тестовые выборки.

Для создания детектора аномалий используются данные о нормальном состоянии для построения модели нормального поведения. Обучающая выборка содержит только данные о нормальном поведении системы, тестовая – содержит данные как нормального класса, так и класса аномалий (одиночные атаки и их комбинации).

В данном исследовании применяется несколько алгоритмов для построения моделей машинного обучения с целью обнаружения аномалий. Рассматриваются следующие модели:

- детектор на основе нейросетевого автоенкодера LSTM для одномерного и многомерного ТВР;
- детектор выбросов с автоподстройкой порога (LOF-детектор);
- детектор аномалий на основе изолирующего леса (IFO-детектор);
- детектор аномалий на основе машины опорных векторов (One-class SVM).

На рис. 2.8 обозначены:

- X_R – нормализация каждого из рядов многомерного ТВР (1);
- X_R^P – сглаженные многомерные ТВР (2);
- X_R^W – скользящее окно длины W с шагом S, формирует набор отсчетов для анализа по каждому из ТВР (рис. 2.8, б) (3);
- подготовленные данные для построения, тестирования и использования ансамбля детекторов (4);
- ансамбль автоенкодеров на основе нейронной сети LSTM (5): детектор выбросов с автоподстройкой порога (LOF детектор); детектор аномалий на основе модели изолирующего леса (IFO); детектор аномалий на основе машины опорных векторов (One class SVM);
- многомерный детектор НС LSTM (рис. 2.8, в);
- суммирование оценок детекторов в каждом окне W одномерных ТВР (7);
- блок принятия решений о наличии аномалий в окне анализа W одномерных ТВР (8);
- специалист по интеллектуальному анализу данных (9);
- оператор системы обнаружения аномалий (10).

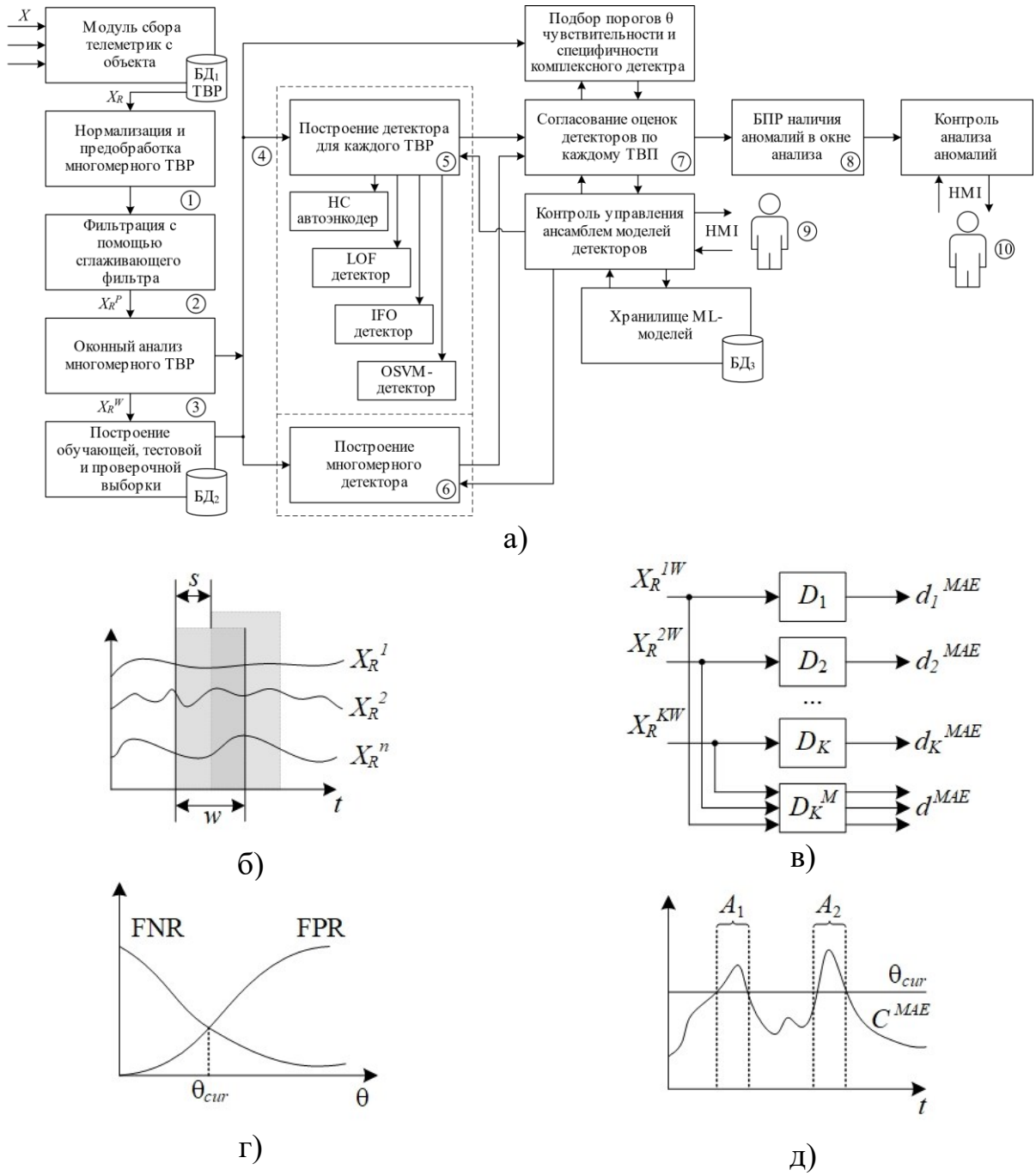


Рисунок 2.8 – Структурная схема системы обнаружения аномалий (а); процесс формирования с помощью скользящего окна фрагментов многомерного ТВР (б); многомерный нейросетевой детектор (в); подбор порогового значения для определения окна анализа на основе оценок относительного количества ложно-положительных (FPR) и ложно-отрицательных (FNR) срабатываний (г); визуализация разметки аномальных фрагментов ТВР на основе порогового сравнения ошибки восстановления образа с помощью детектора (д)

Нейросетевой автоенкодер (НА) в задаче обнаружения аномалий предназначен для восстановления (реконструкции) фрагмента ТВР. Обнаружение аномалий осуществляется на основе порогового сравнения среднеквадратической (или абсолютной) ошибки между фактическими данными и восстановленным образом. Применяемая архитектура НА на основе долгой краткосрочной памяти

(LSTM) является разновидностью архитектуры рекуррентных нейронных сетей глубокого обучения, способной к анализу долговременных зависимостей.

Автоенкодер состоит из двух частей (рис. 2.9):

- кодер – отображает входные данные $x \in R^{d_x}$ на внутреннее представление $z \in R^{d_z}$, $z = f(x, W_x)$, $W \in R^{d_z * d_x}$ – матрица весов;
- декодер – выполняет обратное отображение из внутреннего представления во входное пространство (реконструкция): $x = g(z) = g(f(x, W_x))$, $W' \in R^{d_z * d_x}$ – матрица весов.

Процедура обучения автоенкодеров состоит в нахождении набора параметров: $\theta = (W)$, который минимизируют функцию потерь; $L(x, g(f(x)))$, определяющую качество реконструкций образа – выходная реконструкция образа x должна быть как можно ближе к исходному входному вектору x. Типичный выбор для функции потерь – это среднеквадратичная ошибка:

$$L(x, g(f(x))) = \|x - x\|_2^2 .$$

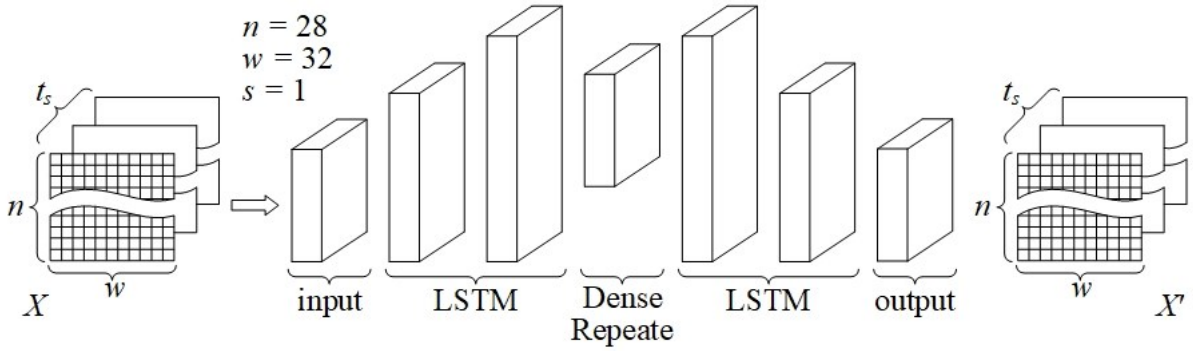


Рисунок 2.9 – Схема применяемого многомерного автоенкодера на основе LSTM, n – количество анализируемых параметров (количество ТВР), w – длина скользящего окна анализа, s – шаг скользящего окна анализа, t_S – глубина погружения в ТВР

Основным преимуществом применения моделей автоенкодеров в задаче обнаружения аномалий является возможность построения модели нормального поведения системы. При появлении новых типов аномалий или изменении характера текущих аномалий детектор на основе автоенкодера по-прежнему, оценивая ошибку реконструкции образа, способен выявлять подобные образы [268].

Итоговая модель ансамбля детекторов для обнаружения аномалий в многомерном технологическом временном ряду, характеризующем ход технологического процесса, включает группу детекторов для одномерных ТВР и детектор

для многомерного ТВР на основе нейросетевых автоенкодеров, LOF и IFO моделей (рис. 2.10).

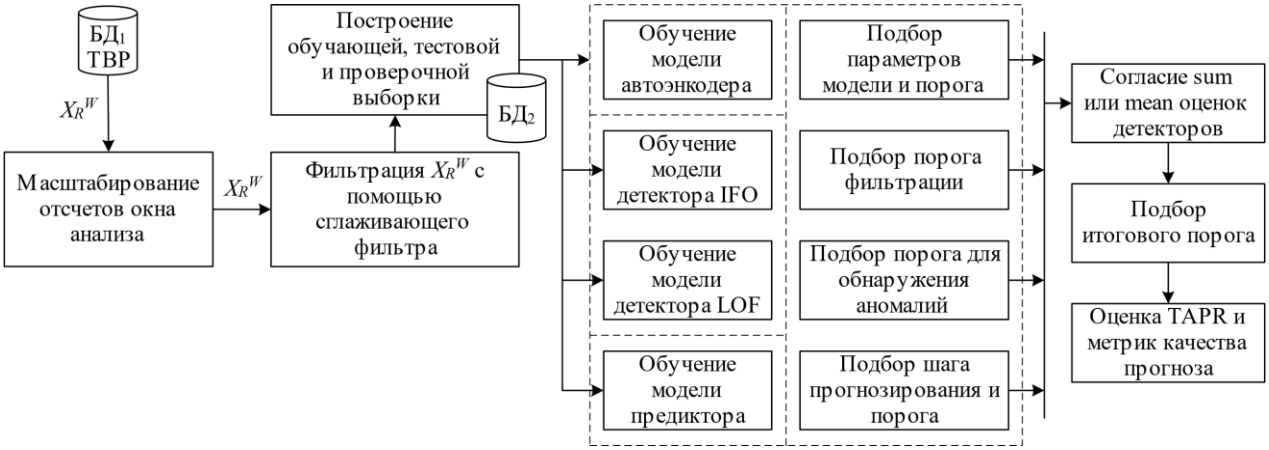
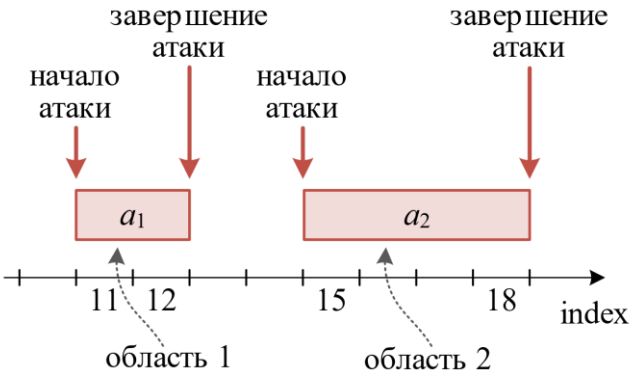


Рисунок 2.10 – Модель обнаружения аномалий на основе ансамбля детекторов

Оценка качества методов обнаружения аномалий в временных рядах параметров производится с помощью традиционных метрик качества классификации и TaPR – метрики оценки обнаружения аномалии и корректности границ аномалии во временных рядах. Как показано на рис. 2.11, конечная цель заключается в определении области действия атаки в совокупности отсчетов ТВР, например, область действия для двух атак a_1 и a_2.



Index	Label	
10	0	
11	1	область 1
12	1	
13	0	
14	0	
15	1	область 2
16	1	
17	1	
18	1	
19	0	

Рисунок 2.11 – Модель обнаружения аномалий на основе ансамбля детекторов

Метрика TaPR реализует две стратегии: оценка обнаружения аномалии, TaR (сколько аномалий обнаружено), и оценка корректности границ обнаруженной аномалии, TaP (насколько точно обнаруживается каждая аномалия) (рис. 2.12) [157].

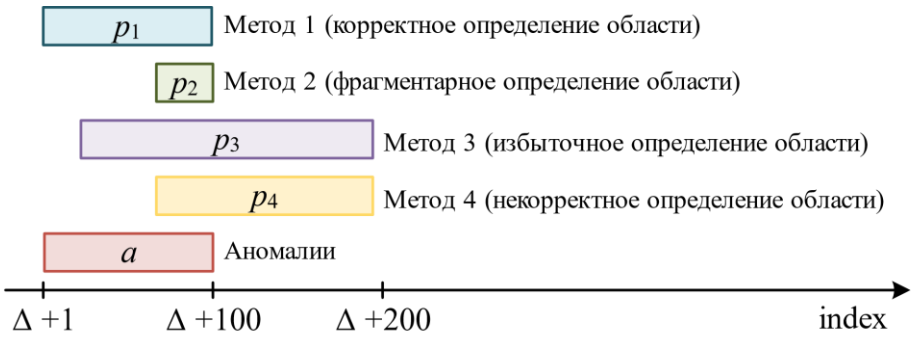


Рисунок 2.12 – Метрики оценки TaPR

Обобщенный алгоритм анализа ТВР в задаче обнаружения аномалий, вызванных воздействием злоумышленника, пытающегося перехватить управление или навязать алгоритм управления КФО, представлен на рис. 2.13.

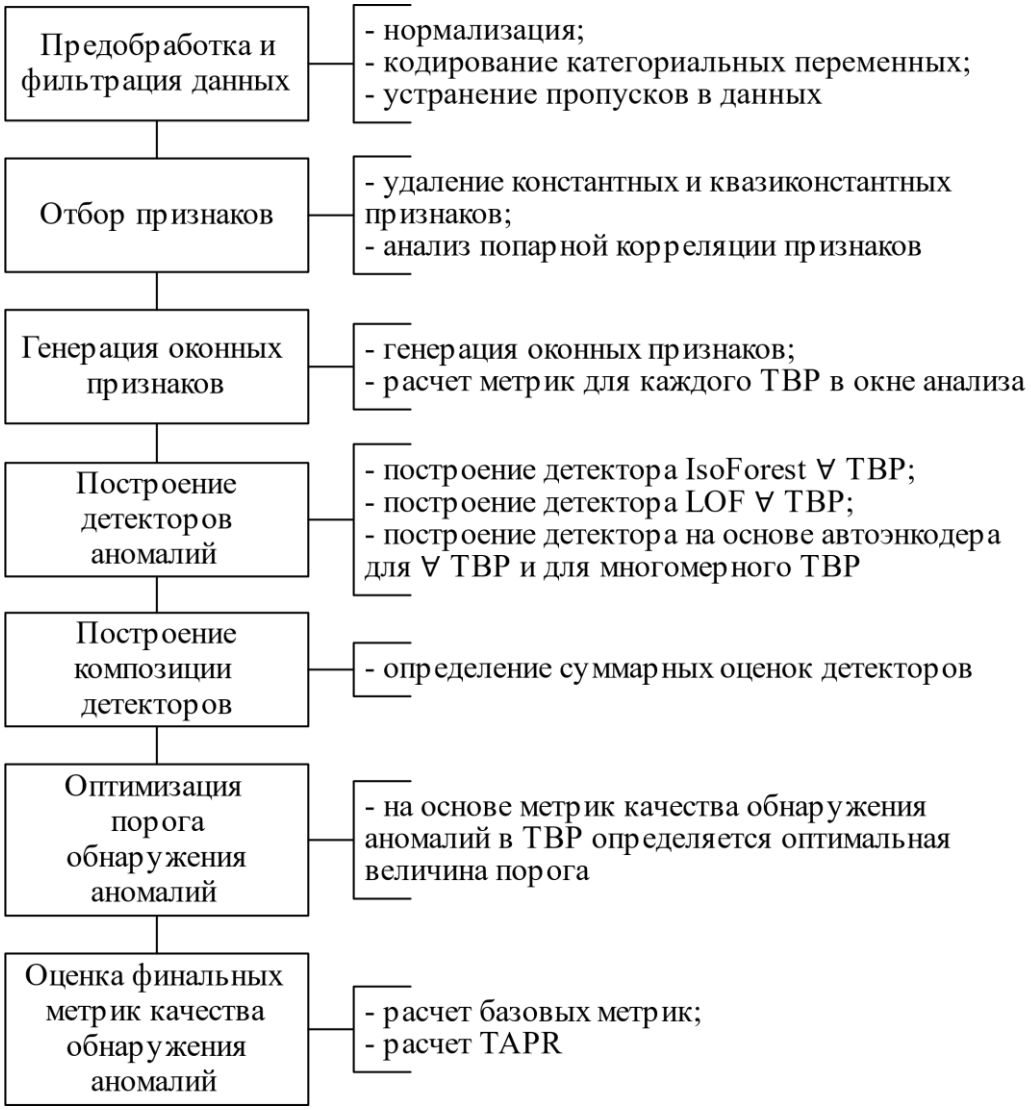


Рисунок 2.13 – Обобщенный алгоритм анализа аномалий

Предложена структурная схема системы обнаружения аномалий технологического процесса, основанная на применении методов предиктивного анализа собираемых данных телеметрии и позволяющая выявить воздействия

злоумышленника, получившего доступ в промышленную сеть управления технологическим процессом.

Разработана гетерогенная модель ансамбля детекторов для обнаружения аномалий в многомерном технологическом временном ряду параметров, характеризующих ход технологического процесса. Модель включает группу детекторов для одномерных ТВР и детектор для многомерного ТВР на основе нейросетевых автоенкодеров, LOF и IFO моделей.

2.3.2 Нейросетевая модель адаптивной сегментации технологических временных рядов наблюдаемых параметров состояния киберфизического объекта в задаче обнаружения аномалий

Функционирование КФО можно рассматривать как последовательную смену состояний на некотором временном промежутке (t_0, t_k). Технологические сигналы несут в себе признаки происходящих на объекте событий. Следовательно, разработка модели анализа технологических сигналов представляет собой задачу идентификации дискретных эпох технологического сигнала и соотнесения их с событиями в соответствующих процессах, характеризующих состояние объекта диагностирования [52, 68, 94]. Выход параметров за пределы допустимых значений означает переход объекта во внештатную ситуацию. Следовательно, пространство состояний, характерное для исследуемого объекта, можно разделить на два множества: множество опасных состояний и множество штатных состояний.

Набор значений технологических параметров, описывающих состояние объекта в момент времени $t \in (t_0, t_k)$, является ситуацией. Множество всевозможных ситуаций необходимо для построения соответствия между ситуацией и набором диагностических решений.

Технологический временной ряд – это последовательность дискретных упорядоченных в неслучайные равноотстоящие моменты времени измерений $y(t_1), y(t_2), \dots, y(t_N)$ параметра, характеризующего состояние технологического объекта.

Рассматривается задача моделирования временных рядов рассматриваемого ТП в общем виде может быть сформулирована следующим образом. Пусть заданы значения временного ряда $Y = \{y(1), y(2), \dots, y(N)\}$, где $y(t)$ — значение показателя исследуемого процесса, зарегистрированного в t-м такте времени

$(t = 1,2, \dots, N)$. Требуется построить оценки будущих значений ряда $\hat{Y} = \{\hat{y}(N+1), \hat{y}(N+2), \dots, \hat{y}(N+\tau)\}, 1 \leq \tau \leq N$, где τ – горизонт прогнозирования [62].

Общей моделью временного ряда служит модель вида (2.9):

$y_t = f(x_t, a) + \varepsilon_t$	(2.9)

где y_t – наблюдаемый временной ряд;

$f(x_t, a)$ – систематическая компонента;

ε_t – случайная компонента.

Контролируемые параметры ТП представляют собой проявления нестационарных процессов, являясь примером динамических систем:

– переменные условия работы аппаратуры, когда параметры среды резко меняются (например, переключение режима работы установки);

– продолжительный период работы узлов и агрегатов, когда динамические характеристики системы меняются, и один и тот же вход вызывает различные реакции системы.

Может быть выделен временной интервал, на котором параметры объекта изменяются несущественно, и считаются условно постоянными. Таким образом, разбиение технологического временного ряда на интервалы сводится к построению детектора смены типа динамики, описывающей состояние объекта. В рабочем режиме функционирование технологического объекта характеризуется стационарностью, устойчивостью значений параметров и постоянством развития во времени. Большая часть рабочих режимов, характерных для объекта, является установившимися во времени процессами. Совокупное время переходных процессов в сети T_{per} существенно меньше общего времени T функционирования сети. Хронологию работы технологического объекта можно рассматривать как временную последовательность статических режимов, сменяемых относительно короткими переходными процессами.

Модели ТВР необходимо строить по набору отсчетов ТВР, в котором параметры модели полагаются условно стационарными. Размер окна анализа зависит от характера распределения параметров ТВР и при обработке отсчетов, попавших в окно, используется 5-50 близлежащих точек наблюдения.

При анализе используются данные ТВР, образованные результатами наблюдений за входом $u(t)$ и выходом $y(t)$, что представлено на рис. 2.14, где $u(k)$,

$y(k)$ – значение входа и выхода в k-й момент времени $t=kT$; T – период дискретизации по времени; L – размер временного окна.

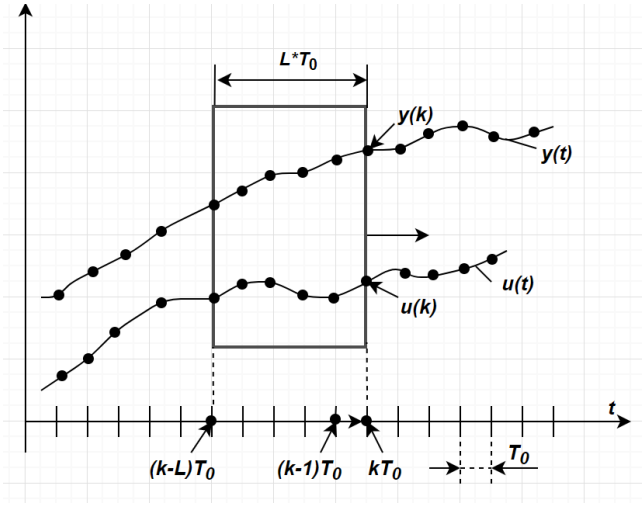


Рисунок 2.14 – Отсчеты ТВР, попадающие в скользящее окно $u(t)$ и $y(t)$

Следовательно, может быть сформирована выборка, содержащая (L+1) пару отсчетов «вход-выход» (2.10):

$$\{(u(k-L), y(k-L)); \dots; (u(k-1), y(k-1)); (u(k), y(k))\}, \quad (2.10)$$

Для получения нелинейной адаптивной модели $y=F(u)$ объекта по входным/выходным данным предлагается использовать нейросетевую модель. Для этого сравниваются выход объекта *y(t)* и выход нейронной сети (НС) $\hat{y}(t)$ при одном и том же входном воздействии *u(t)*, а процедура обучения НС состоит в изменении весов ее связей таким образом, что уменьшить рассогласование $\varepsilon(t) = y(t) - \hat{y}(t)$ до приемлемой (достаточно малой) величины.

С учетом приведенных особенностей ТВР, образованных параметрами объекта, подходящими моделями анализа являются NARX модель (Nonlinear autoregressive with exogenous inputs), позволяющие учитывать нелинейные процессы смена типа динамики (2.11):

$$y_t = F(y_{t-1}, y_{t-2}, y_{t-3}, \dots, u_t, u_{t-1}, u_{t-2}, u_{t-3} \dots) + \varepsilon_t, \quad (2.11)$$

где y – искомая переменная, а u – это внешняя определенная переменная, ε_t — белый шум.

Алгоритм адаптивной сегментации ТВР основан на работах Боденштайном и Преториусом (1977) и использует построение моделей ТВР в скользящих «окнах» (рис. 2.15):

1. Модель строится для некоторого начального референтного участка ТВР;

2. Затем результаты прогнозирования модели сравниваются с оставшимися отсчетами ТВР, поступающими через последовательно скользящее окно, перемещающееся по ТВР;

3. Если характеристики ТВР в референтном участке и в движущемся окне различаются более чем на некоторый порог, проводится граница сегмента, сразу после которой берется новый референтный участок, и процедура повторяется;

4. Сегментация заканчивается, когда окно достигает конца ряда [88].

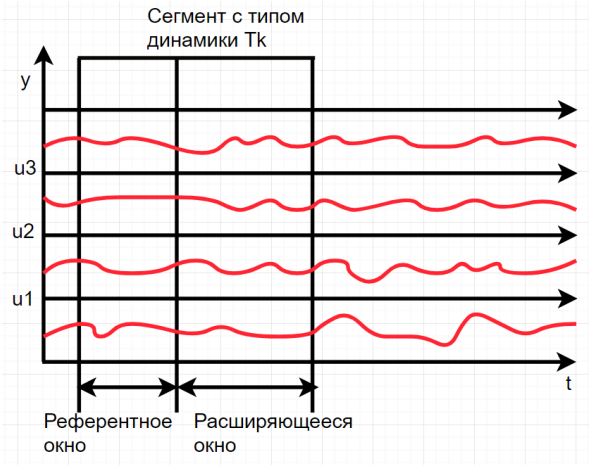


Рисунок 2.14 – Процесс построения адаптивного сегмента с помощью NARX

Для оценки величины отклонения моделируемых значений от реальных данных использует параметрический глобальный метод:

- выбирается отсчет в текущем скользящем окне, который делит ТВР на два сегмента;
- вычисляется эмпирическая оценка расхождения модельных значений и натурных данных для каждого сегмента;
- в каждой точке сегмента измеряется, насколько отклоняется эмпирическая оценка от модельных значений. Рассчитывается отклонения для всех точек;
- рассчитывается суммарная невязка в каждом сегменте;
- изменение местоположения точки деления выполняется до минимизации полной остаточной ошибки.

Для того чтобы объединить сегменты в группы по степени сходства моделей ТВР, сопоставленных с данными сегментами, используется алгоритм кластеризации k-means.

При анализе используются данные ТВР, образованные результатами наблюдений за входом $u(t)$ и выходом $y(t)$. Следовательно, может быть сформирована выборка, содержащая (L+1) пару отсчетов «вход-выход» (2.12):

$$\left\{\left\{\left(u(k-L),y(k-L)\right);\ldots;\left(u(k-1),y(k-1)\right);\left(u(k),y(k)\right)\right\},C_m\right\} \quad (2.12)$$

где C_m – класс известного типа события, поставленного в соответствие для текущего сегмента, по которому стоится очередной пример выборки.

Схема реализации процесса обучения NARX модели представлена на рис. 2.15.

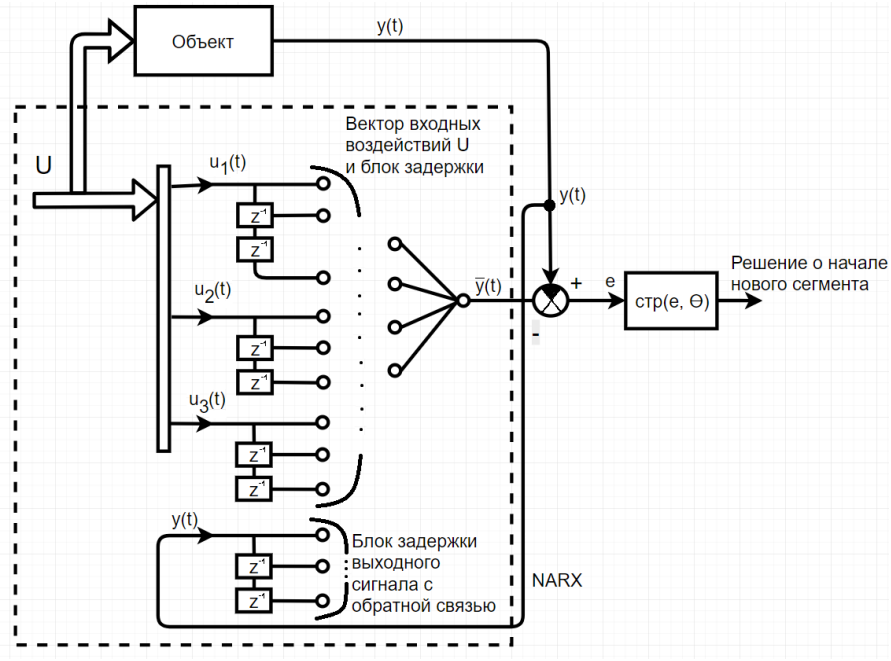


Рисунок 2.15 – Схема реализации процесса обучения NARX модели

На вход модели подается сформированный временной ряд параметров технологического процесса U: $u_1(t), u_2(t), u_3(t)$), для обучения НС прогнозировать ход ТП в пределах адаптивного окна и разбиения ряда на сегменты. Выходной параметр $y(t)$ подается на выход НС для сравнения прогнозированного значения выходного параметра с реальным значением, если значения не совпадают, то происходит создание нового сегмента.

Алгоритм мониторинга ТП в задаче выявления состояний объекта, включает этапы:

1. адаптивная сегментация ТВР;
2. слияние сегментов и кластеризация оставшихся сегментов по параметрам моделей выделенных участков ТВР;
3. Сопоставление истории состояния технологического объекта (ТО) и сегментов ТВР;
4. Обучение классификатора, анализирующего динамику текущего окна анализируемых параметров;
5. Принятие решения о типе состояния ТО.

В данном алгоритме выполняется процесс получения данных о ходе ТП в виде ТВР, сегментация данного ТВР и объединение сегментов по схожему типу поведения ТВР. Далее идет обучение классификатора, который анализирует динамику ТП и принимает решение о типе технологического состояния ТО.

2.3.3 Модель анализа поведения пользователей конечной системы

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. 2.16)**, включающий:

- построение цифрового отпечатка пользователя (модель пользовательского окружения конечной системы и модель динамического профиля взаимодействия пользователя с конечной системой);
- профилирование состояния пользователя.

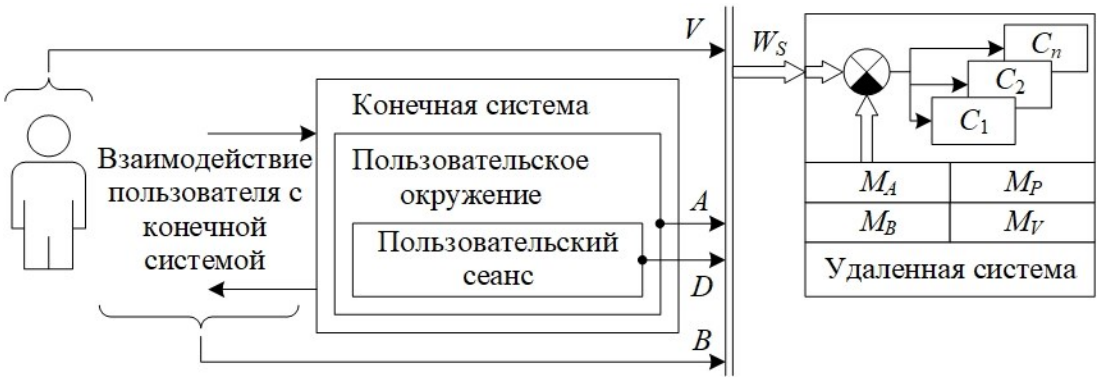


Рисунок 2.16 – Комплекс моделей обнаружения аномалий поведения пользователя и состояния пользовательского окружения, где A – цифровой отпечаток пользовательского окружения при работе с удаленной Web-системой, B – цифровой отпечаток паттернов динамических биометрических признаков пользовательского сеанса; D – цифровой отпечаток динамического профиля пользователя (характер действий в удаленной системе), V – образ автоматического профилирования пользователя (видеоаналитика); M – соответствующие модели обнаружения аномалий;

2.4 Когнитивные модели оценки рисков ИБ объекта КИИ

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

Можно указать достаточно большое число примеров успешного применения НКК для решения задач оценки рисков ИБ [6, 32, 57, 128]. Основные направления исследований в данной области связаны с дальнейшей разработкой математических основ построения НКК, оценкой адекватности, структурной сложности и устойчивости НКК, выбором алгоритмов их обучения, обеспечивающих желаемые характеристики НКК для достижения поставленных целей [119, 158, 159, 162, 195, 220, 235, 265] в задачах комплексной оценки рисков ИБ.

2.4.1 Оценка рисков информационной безопасности с использованием нечетких когнитивных карт

Под *нечеткой когнитивной картой* понимается модель исследуемой системы (объекта, проблемы) в форме ориентированного графа (орграфа), заданного с помощью набора множеств

НКК = <**C**, **F**, **W**>,	(2.13)

где **C** = $\{C_i\}$– множество вершин графа, называемых *концептами*, в качестве которых выступают факторы (понятия), наиболее существенные с точки зрения изучения рассматриваемой системы;

F = $\{F_k\}$ – множество направленных дуг графа – связей между концептами;

W = $\{W_{ij}\}$ – множество весов дуг (связей).

Предполагается, что связи между концептами могут быть положительными, «усиливающими» влияние концепта C_i на концепт C_j ($W_{ij} > 0$), или отрицательными, «ослабляющими» влияние концепта C_i на концепт C_j ($W_{ij} < 0$). В простейшем случае $W_{ij} = +1$ или $W_{ij} = -1$, при этом говорят о *знаковом* орграфе. Значения весов (силы связей) W_{ij} могут задаваться с помощью нечеткой лингвистической шкалы, представляющей собой упорядоченное множество лингвистических значений (термов) оценок силы связи, например, вида

СИЛА_СВЯЗИ = {Не_влияет; Слабая; Средняя; Сильная; Очень_сильная}.

Каждому из этих значений ставится в соответствие некоторый числовой диапазон, принадлежащий отрезку [0,1] для положительных связей (пример – таблица 1), или отрезку [-1,0] для отрицательных связей.

Предполагается, что, отвечая на вопрос о силе связи между концептом C_i и концертом C_j, эксперт выбирает одно из приведенных здесь лингвистических значений и некоторую «точечную» оценку силы связи – число внутри этого

диапазона (если экспертов несколько, то в качестве веса W_{ij} принимается среднее из данных ими оценок).

Таблица 2.1 – Оценка силы связи между концептами

Лингвистическое значение	Числовой диапазон
Не_влияет	0
Очень_слабая	(0; 0,15]
Слабая	(0,15; 0,35]
Средняя	(0,35; 0,6]
Сильная	(0,6; 0,85]
Очень_сильная	(0,85; 1]

Знаковый орграф полностью задается своей *матрицей смежности*

$$\mathbf{W} = \begin{Vmatrix} W_{11} & W_{12} & \dots & W_{1n} \\ W_{21} & W_{22} & \dots & W_{2n} \\ \dots & \dots & \dots & \dots \\ W_{n1} & W_{n2} & \dots & W_{nn} \end{Vmatrix}, \quad (2.14)$$

элементы которой W_{ij} принимают значения +1 (положительная связь), -1 (отрицательная связь) или 0 (отсутствие связи); n – число концептов НКК.

В общем случае, для взвешенного орграфа с произвольными значениями весов $W_{ij} \in [-1, 1]$ можно говорить о динамике изменения его состояния во времени. Состояние орграфа (НКК) при этом определяется совокупностью состояний его концептов C_i, ($i = 1, 2, \dots, n$), каждое из которых описывается переменной состояния $X_i(t)$, принимающей значения из интервала [0, 1]. Последнее достигается путем нормирования первоначальных («физических») переменных состояния $\overline{X_i}$ по формуле

$$X_i = \frac{\overline{X}_i - X_{imin}}{\overline{XX}_{imin_{imax}}} \quad (2.15)$$

где $\overline{X}_{i\,\min}$ и $\overline{X}_{i\,\max}$ – минимальное и максимальное значения переменной $\overline{X}_i$, ($i = 1, 2, \dots, n$).

Знаковый орграф считается линейным, его уравнения состояния записываются как

$$X(t+1) = \mathbf{W} \cdot X(t), \quad (2.16)$$

где $\mathbf{X} = (X_1, X_2, \dots, X_n)^T$ – вектор состояния орграфа; $\mathbf{W}$ – матрица смежности; $t = 0, 1. 2, \dots$ – дискретное время.

Для взвешенного орграфа с произвольно заданными значениями весов W_{ij} уравнения состояния обычно записываются в следующем виде:

$$X_i(t+1) = f\left(\sum_{j=1}^{n} W_{ji} X_j(t)\right), \quad (i = 1, 2, \ldots, n), \qquad (2.17)$$

где $f(\,)$ – некоторая нелинейная «сжимающая» функция, отображающая значения аргумента в единичный интервал [0, 1].

Этому условию удовлетворяет, например, сигмоидная функция

$$f(x) = \frac{1}{1+e^{-x}} \qquad (2.18)$$

Важным этапом анализа НКК является анализ устойчивости ее равновесных состояний для знакового орграфа, который сводится к вычислению собственных чисел матрицы смежности, т.е. корней характеристического уравнения

$$|\,\mathbf{W} - \lambda \cdot \mathbf{I}\,| = 0 \qquad (2.19)$$

где **I** – единичная матрица размера n x n; λ - комплексная переменная.

Необходимо различать *импульсную устойчивость* орграфа, когда для заданного ненулевого начального состояния $X_i(0)$ одной из его вершин, например, $X_1(0)=1$, $X_2(0)= \ldots = X_n(0) = 0$, последовательность значений импульсов $p_i(t) = X_i(t) - X_i(t\text{-}1)$ ограничена в любой момент времени t=1,2,… для любой его вершины, и *абсолютную устойчивость*, когда для каждой вершины орграфа (i = 1, 2, …,n) ограничена последовательность значений $X_i(t)$, t=1,2,… . При этом справедливо следующее

Утверждение 1. Знаковый орграф импульсно (абсолютно) устойчив, если все ненулевые собственные числа матрицы **W** равны по абсолютной величине единице.

При определении устойчивости взвешенного орграфа можно воспользоваться другим утверждением, основанном на оценке абсолютных значений весов НКК.

Утверждение 2. Взвешенный орграф, описываемый уравнениями (5)-(6), абсолютно устойчив, причем существует единственное равновесное (установившееся) решение этих уравнений («неподвижная точка») X^*, в том и только в том случае, если

$$\left(\sum_{i=1}^{n}\sum_{j=1}^{n} W_{ij}^2\right)^{\frac{1}{2}} < 4, \qquad (2.20)$$

где n – число концептов НКК.

Общая постановка процедуры анализа НКК включает в себя два этапа.

Задача анализа: для заданных начальных условий ($X_1(0)$, $X_2(0)$, …, $X_n(0)$), рассчитать переходные процессы $X_i(t)$, (t=0,1,2,…), вызванные этими начальными условиями или некоторым внешним воздействием; определить установившиеся (равновесные) значения переменных состояния X_i^*.

Задача синтеза: найти такие скорректированные значения весов связей W_{ij}, а возможно и добавить новые концепты или связи, при которых обеспечивались бы желаемые установившиеся значения X_i^* целевых концептов C_e, (l= 1,2,…,n_1; $n_1 < n$) – выходов НКК.

2.4.2 Нечеткие продукционные когнитивные карты

Нечеткие продукционные когнитивные карты (НПКК), или нечеткие когнитивные карты, основанные на правилах (Rule Based Fuzzy Cognitive Maps), впервые предложенные в 1999 г. Х. Карвалью и Х. Томе [163], привлекают внимание многих исследователей в силу ряда своих несомненных преимуществ. Во-первых, они представляют собой действительно нечеткие системы, позволяющие описать качественное поведение сложных систем и их компонентов с помощью системы нечетких правил; во-вторых, они обладают значительной общностью, допуская использование различных видов нечетких связей (отношений), включая обратные связи, между входящими в их состав концептами; в-третьих, они учитывают фактор времени, позволяя моделировать динамику сложных, плохо формализуемых систем.

2.4.3 Нечеткие серые когнитивные карты

Важное место среди семейства НКК занимают нечеткие «серые» когнитивные карты (НСКК) (Fuzzy Grey Cognitive Maps, FGCM), впервые предложенные в 2010 г. Хосе Салмероном [274]. Основное отличие НСКК от других разновидностей НКК – использование интервальных оценок (диапазонов) значений переменных состояния концептов и весов связей между этими концептами вместо использования значений (термов) лингвистических переменных, описываемых с помощью нечетких чисел или функций принадлежности нечетких множеств, как это традиционно делается в НКК. Операции нечеткой логики заменяются при этом интервальной арифметикой над «серыми» (интервальными) числами (grey numbers). Нечеткие серые когнитивные карты (которые с равным успехом можно назвать также «интервальными» НКК) считаются удачным расширением НКК, поскольку они лучше соответствуют представлениям экспертов, обладают

большей интерпретируемостью и представляют больше степеней свободы лицу, принимающему решение (ЛПР) на основании результатов моделирования. Очевидно, что применение НСКК для решения задач интервального оценивания рисков ИБ имеет свои перспективы.

Фундаментом построения НСКК является теория серых систем (Grey Systems Theory), предложенная в 1989 г. Дж. Денгом [178]. Предметом изучения данной теории являются объекты и системы с высокой неопределенностью, представленные малыми выборками неполных и неточных данных. В зависимости от располагаемой известной информации, изучаемые системы при этом делятся на 3 вида:

– «белые» системы (внутренняя структура и свойства системы полностью известны);

– «серые» системы (известна частичная информация о системе»;

– «черные» системы (внутренняя структура и свойства системы полностью неизвестны).

В соответствии с терминологией теории серых систем, нечеткая серая когнитивная карта – это когнитивная модель системы в виде ориентированного графа, заданного с помощью следующего набора множеств

$\text{НСКК} =< C, F, W >,$	(2.21)

где $C = \{C_i\}$ – множество концептов (вершин графа), $(i = 1,2, \dots, n)$; $F = \{F_{ij}\}$ – множество связей между концептами (дуг графа); $W = \{W_{ij}\}$ – множество отношений между концептами, определяющих веса указанных связей (дуг графа), $(i, j) \in \Omega$. Здесь $\Omega = \{(i_1, j_1), (i_2, j_2), \dots, (i_L, j_L)\}$ – множество пар индексов смежных (связанных между собой) вершин, $L \le n(n-1)$.

В отличие от традиционного понимания НКК, веса связей НСКК задаются с помощью «серых» (интервальных) чисел $\otimes W_{ij}$, определяемых как

$\otimes W_{ij} \in \left[\underline{W}_{ij}, \overline{W}_{ij}\right]$, где $\underline{W}_{ij} < \overline{W}_{ij}, \left\{\underline{W}_{ij}, \overline{W}_{ij}\right\} \in [-1,1],$	(2.22)

где $\underline{W}_{ij}$ – нижняя граница серого числа $\otimes W_{ij}$; $\overline{W}_{ij}$ – верхняя граница серого числа. Таким образом, вес связи между i-м и j-м концептами $\left(C_i \to C_j\right)$ может принимать любое значение в пределах заданного диапазона изменения $\left[\underline{W}_{ij}, \overline{W}_{ij}\right] \in [-1,1]$. В частном случае, когда $\underline{W}_{ij} = \overline{W}_{ij}$, получаем $\otimes W_{ij} \in \left[\underline{W}_{ij}, \underline{W}_{ij}\right]$ – «белое» (четкое, обычное) число.

Основные операции над серыми числами:

1) $\otimes W_1 + \otimes W_2 \in \left[\underline{W_1} + \underline{W_2}, \overline{W_1} + \overline{W_2}\right]$;

2) $-\otimes W \in \left[-\overline{W}, -\underline{W}\right]$;

3) $\otimes W_1 - \otimes W_2 \in \left[\underline{W_1} - \overline{W_2}, \overline{W_1} - \underline{W_2}\right]$;

4) $\otimes W_1 \times \otimes W_2 \in [\min(S), \max(S)]$,

где $S = \left\{\underline{W_1} \cdot \underline{W_2}, \underline{W_1} \cdot \overline{W_2}, \overline{W_1} \cdot \underline{W_2}, \overline{W_1} \cdot \overline{W_2}\right\}$

5) Если $\lambda > 0$, $\lambda \in \mathbb{R}$, то $\lambda \cdot \otimes W \in [\lambda\underline{W}, \lambda\overline{W}]$.

При выборе серых значений весов $\otimes W_{ij}$ экспертам необходимо ориентироваться на некоторую нечеткую шкалу, наподобие той, которая представлена в Таблице 2.2, начиная с выбора «центров» соответствующих интервалов W_{ij}^0. Здесь значения термов: Z – Zero; VS – Very Small; S – Small; M – Middle; L – Large; VL – Very Large. Следующим шагом, определяющим действия эксперта, будет выбор границ интервала $\left[\underline{W_{ij}}, \overline{W_{ij}}\right]$, определяющего серое значение силы связи $\otimes W_{ij}$. Это могут быть равноотстоящие от центрального значения W_{ij}^0 числа, например: $\otimes W_{ij} \in \left[W_{ij}^0 - \delta_{ij}, W_{ij}^0 + \delta_{ij}\right]$, где $\pm\delta_{ij}$ – разброс оценки относительно центра W_{ij}^0, но возможны и другие варианты.

Таблица 2.2 – Оценка силы (весов) связей между концептами

Лингвистическое значение силы связи	Терм	Числовой диапазон
Не влияет	Z	0
Очень слабая	VS	(0; 0,15]
Слабая	S	(0,15; 0,35]
Средняя	M	(0,35; 0,6]
Сильная	L	(0,6; 0,85]
Очень сильная	VL	(0,85; 1]

Введение процедуры обучения для связей концептов в НСКК повышает гибкость модели.

Предполагается, что изменение состояния концептов во времени описывается уравнениями

$$\otimes X_i(k+1) = f\left(\otimes X_i(k) + \sum_{\substack{j=1 \\ (j \neq i)}}^{n} \otimes W_{ji} \otimes X_j(k)\right), (i = 1,2, \dots, n) \qquad (2.23)$$

где $\otimes X_i(k)$ – «серая» (интервальная) переменная состояния i-го концепта C_i, которая в каждый момент времени $k = 0,1,2, \dots$ принимает некоторое значение

внутри определенного интервала (диапазона изменения), заданного границами $\underline{X}_i(k)$ и $\overline{X}_i(k)$; $f(\cdot)$ – нелинейная функция активации i-го концепта, отображающая значения аргумента в интервал $[-1,1]$. В качестве функции активации $f(\cdot)$, как правило, принимаются:

а) линейная функция с ограничением:

$$f(x) = \begin{cases} x, \text{если } |x| \le 1, \\ \text{Sign } x, \text{если } |x| > 1; \end{cases}$$

б) двухполярная сигмоидная функция (гиперболический тангенс):

$$f(x) = (1 - e^{-x})/(1 + e^{-x}) = \text{th}\left(\frac{x}{2}\right);$$

в) однополярная сигмоида:

$$f(x) = 1/(1 + e^{-x})$$

Для решения системы уравнений (2.23) требуется задать начальные значения переменных состояния $\otimes X_i(0)$, которые также должны рассматриваться как серые числа $\otimes X_i(0) \in \left[\underline{X}_i(0), \overline{X}_i(0)\right]$. Наибольший интерес обычно представляет получение равновесного (установившегося) решения, которое представляет собой «серый» вектор $\lim\limits_{k\to\infty}[\otimes X_i(k)] = \otimes X^* \in \left[\underline{X}^*, \overline{X}^*\right]$ или предельный цикл (странный аттрактор).

Для определения устойчивости установившегося решения $\otimes X^*$ можно воспользоваться теоремой [274], согласно которой единственное равновесное (установившееся) решение уравнений вида (2.23) («неподвижная точка») существует в том и только в том случае, если выполняется условие

$$\left(\sum_{i,j=1}^{n} W_{ij}^2\right)^{\frac{1}{2}} < H,$$

где значение положительной константы H зависит от выбора функции активации концептов: $H = 1$ для функции (4); $H = 2$ для функции (5); $H = 4$ для функции однополярной сигмоиды. Очевидно, что проверка выполнения условия должна производиться для верхних границ серых чисел $\overline{W}_{ij}$, $(i, j = 1,2, \dots n)$.

В отличие от классических способов построения нечетких когнитивных карт, в данном случае для оценки силы взаимосвязей между концептами используются интервальные оценки («серые» числа), характеризующие некоторую меру естественной неопределенности (размытости) в суждениях эксперта или группы экспертов относительно взаимовлияния указанных концептов.

2.4.4 Обобщенные нечеткие когнитивные карты

Переходя к рассмотрению обобщенных НКК, будем полагать, что уравнения состояния НКК (1) в общем виде могут быть переписаны как

$$\tilde{X}_i(t+1) = f\left(\tilde{X}_i(t) \oplus \left(\bigoplus_{\substack{j=1 \\ (j\neq i)}}^{n} \widetilde{W}_{ji} \otimes \tilde{X}_j(t)\right)\right),\ (i = 1,2,\dots,n), \quad (2.24)$$

где веса связей $\widetilde{W}_i$ и переменные состояния $\tilde{X}_i(t+1)$, $\tilde{X}_i(t)$ представляют собой интервальные числа, определяемые как элементы некоторых нечетких интервальных множеств; $\oplus$ и $\otimes$ – операции сложения и умножения интервальных чисел, заданные на нечетких интервальных множествах; f – функция активации.

В качестве основы для построения НКК могут использоваться различные способы задания интервальных нечетких множеств (НМ).

Понятие интуиционистского нечеткого множества (intuitionistic fuzzy set) было впервые введено в 1986 г. болгарским математиком К. Атанасовым.

Под интуиционистским нечетким множеством при этом понимается множество вида

$$A = \{< x, \mu_A(x), \nu_A(x) > | x \in X\}, \quad (2.25)$$

где $\mu_A(x)$ и $\nu_A(x)$ определяют соответственно степень принадлежности и степень непринадлежности элемента $x \in X$ (интуиционистского нечеткого числа) множеству $A \subseteq X$; $0 \leq \mu_A(x) \leq 1$; $0 \leq \nu_A(x) \leq 1$. Существенное отличие от «обычных» нечетких множеств заключается в выполнении условия: $\mu_A(x) + \nu_A(x) \leq 1$, , т.е. допускается случай, когда сумма значений $\mu_A(x)$ и $\nu_A(x)$ меньше единицы. Таким образом, в рассмотрение вводится еще один параметр, называемый степенью нерешительности (сомнения, неуверенности – hesitancy degree) и определяемый как

$$\pi_A(x) = 1 - \mu_A(x) - \nu_A(x);\ 0 \leq \pi_A(x) \leq 1. \quad (2.26)$$

Имеется в виду, что эксперт зачастую затрудняется определить значения функции принадлежности $\mu_A(x)$ и непринадлежности $\nu_A(x)$ элемента x множеству A в силу недостоверности располагаемых им данных или отсутствия у него достаточно полной информации. При этом всегда имеет место равенство $\mu_A(x) +$

$\nu_A(x) + \pi_A(x) = 1$. Очевидно, что если $\pi_A(x) = 0$, то мы имеем дело с обычным нечетким множеством, где $\mu_A(x) + \nu_A(x) = 1$.

Веса связей в интуиционистской НКК задаются в виде значений принадлежности и непринадлежности веса W_{ij} соответствующему нечеткому подмножеству, т.е. парой чисел $< W_{ij}^{\mu}, W_{ij}^{\nu} >$, или с помощью значений принадлежности и степени нерешительности $< W_{ij}^{\mu}, W_{ij}^{\pi} >$. Эти способы задания весов равноценны, поскольку всегда выполняется условие $W_{ij}^{\pi} = 1 - W_{ij}^{\mu} - W_{ij}^{\nu}$.

В отношении расчета переменных состояния концептов, авторами работы [201] предложены два различных подхода: 1) концепция интуиционистского НМ, основанная на введении понятия степени нерешительности W_{ij}^{π}, используется только при определении силы взаимного влияния концептов $\widetilde{W}_{ij}$ (соответствующий вариант интуиционистской НКК получил в [201] обозначение iFCM-I); 2) интуиционистская оценка нерешительности используется как при определении силы взаимного влияния $\widetilde{W}_{ij}$, так и для определения текущего состояния каждого концепта C_i на основе уравнения (2.24), т.е. состояние каждого концепта описывается парой значений $< X_i^{\mu}, X_i^{\nu} >$ в терминах принадлежности и непринадлежности соответствующему подмножеству (значению лингвистической переменной $\tilde{X}_i$), – данный вариант интуиционистской НКК авторы [201] назвали iFCM-II).

Учитывая более высокую сложность модели iFCM-II по сравнению с моделью iFCM-I, выберем для дальнейшего анализа более простой вариант интуиционистской НКК – когнитивную карту iFCM-I, уравнения состояния которой принимают в данном случае следующий вид:

$X_i(t+1) = f\left(X_i(t) + \sum X_i(t) W_{ji}^{\mu}\left(1 - W_{ji}^{\pi}\right)\right), \ \ (i = 1,2,\dots,n).$	(2.27)

Заметим, что весовой фактор $W_{ji}^{\mu}\left(1 - W_{ji}^{\pi}\right)$ принимает нулевое значение, если 2 концепта C_j и C_i не связаны между собой $\left(W_{ji} = 0\right)$ или если степень нерешительности W_{ji}^{π} становится равной 1.

2.4.5 Об интерпретируемости нечетких когнитивных моделей на этапе оценки рисков ИБ

Преимуществами НКК, являются их наглядность, выявление структуры причинно-следственных связей между элементами сложной системы (проблемы,

ситуации), трудно поддающейся количественному анализу традиционными методами, использование знаний и опыта экспертов в конкретной предметной области. Сегодня существует большое число разновидностей нечетких когнитивных карт (НКК) – реляционные НКК [134], интервально-значные НКК [201], серые НКК [274], грубые (rough) НКК [189], интуиционистские НКК [265, 266], продукционные НКК [162, 163], динамические НКК [241] и др. Такое разнообразие когнитивных моделей имеет своей целью приспособиться к учету различных факторов неопределенности, отразить специфику их взаимного влияния и воздействия на исследуемую систему, предложить эффективный инструментарий моделирования сложных плохоформализуемых систем.

Вместе с тем, как отмечается многими авторами, попытки распространить данный подход на задачи моделирования сложных систем нередко сталкиваются с «проклятием размерности» – в результате моделирования получаются НКК, содержащие большое число концептов и их взаимосвязей, что существенно затрудняет их анализ (НКК становятся «непрозрачными» и плохо интерпретируемыми).

Таким образом, проблема *интерпретируемости* (interpretability) результатов, полученных с помощью нечетких когнитивных моделей, приобретает самостоятельный интерес и становится одной из центральных в методологии когнитивного моделирования и машинного обучения. Существуют различные трактовки этого понятия. Так, в [80] интерпретируемость понимается как прозрачность работы нечеткой модели для пользователя, ее способность отражать поведение исследуемой системы в понятной для человека манере. При этом подчеркивается, что одним из условий построения нечетких моделей с хорошей интерпретируемостью является их максимальное упрощение, т.е. уменьшение числа входящих в них структурных компонент. В [303] отмечается, что проблема интерпретируемости должна решаться на 2-х уровнях: на уровне машинных моделей (где решается вопрос о выборе адекватных средств моделирования и формировании рекомендаций ЛПР по результатам моделирования) и на уровне человека-эксперта, который должен понять суть предложенных ему решений (альтернатив) и принять окончательное решение по существу поставленной задачи. В [182] под интерпретируемостью понимается способность объяснить полученные результаты или представить их с помощью терминологии, понятной человеку. При выборе критериев оценки интерпретируемости предлагается воспользоваться разделением возможных подходов на 3 класса: 1) учет специфики

конкретной предметной области (Application-grounded Evaluation); 2) ориентация на знания и опыт эксперта (Human-grounded Metrics); 3) ориентация на известные, хорошо апробированные методы исследования (Functionally-grounded Evaluation).

2.4.6 Общая схема построения нечеткой когнитивной модели оценки рисков информационной безопасности

Предлагается **общая схема построения нечеткой когнитивной модели оценки рисков ИБ объекта КИИ (рис. 2.17)**:

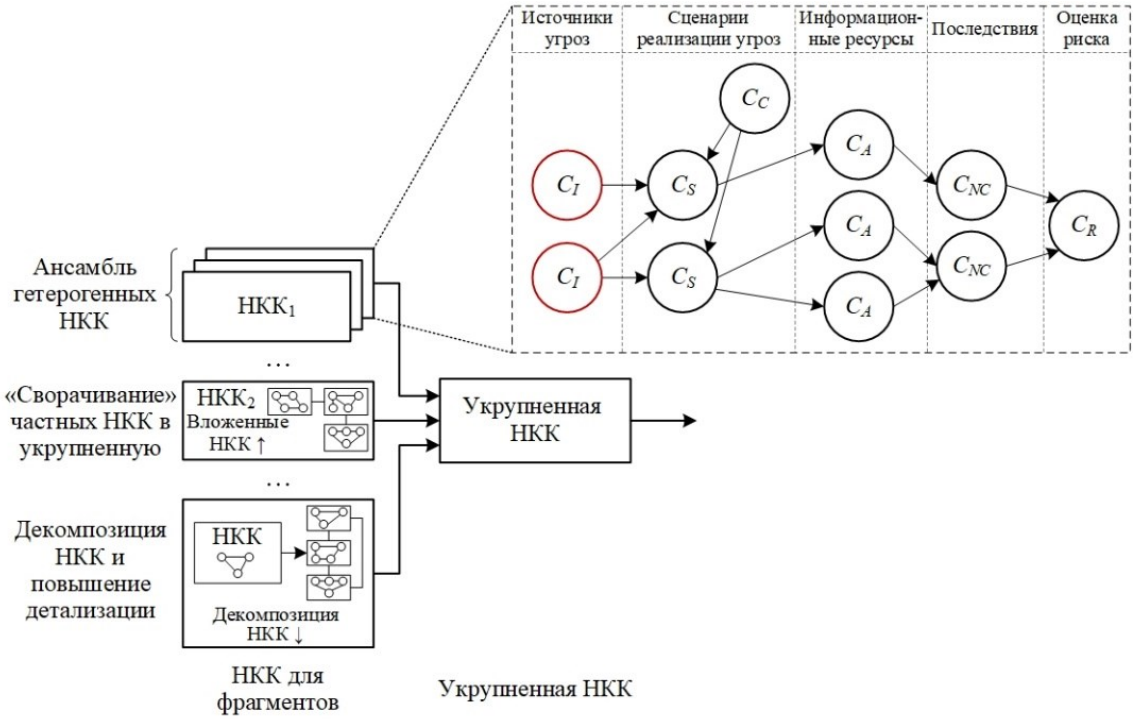


Рисунок 2.17 – Обобщенная схема построения нечеткой когнитивной модели оценки рисков ИБ объекта КИИ

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 – оценки 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;
5. Выбор рационального способа и средств защиты объекта КИИ с учетом требований нормативной базы и имеющихся ограничений.

2.5 Выводы по главе

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 и связывающие их тракты с учетом требований к уровню их безопасности.

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

Собранные данные позволяют перейти к построению когнитивной модели оценки рисков ИБ для целевых сущностей в зоне объекта КИИ, что позволит получить детализированную оценку рисков ИБ и сделать более обоснованный выбор средств защиты информации за счет возможности моделирования различных сценариев реализации угрозы. Исходными данными для построения когнитивных карт являются не только экспертные оценки, но и формализованные и систематизированные данные из открытых баз данных угроз и уязвимостей, что существенно повышает обоснованность и полноту моделирования.

Разработана **модель оценки степени опасности новых уязвимостей**, для которых экспертная оценка еще не определена, на основе прогнозирования компонент метрики с помощью анализа текстового описания текстовых описаний угроз и уязвимостей. Предложено два подхода для оценки базовой метрики CVSS опасности уязвимостей по формализованному текстовому описанию: построение ансамбля предикторов для оценки отдельных значений компонент вектора с последующим расчетом результирующего значения и построение ансамбля регрессоров для непосредственной оценки результирующего значения.

Для автоматизации низкоуровневого моделирования сценариев эксплуатации уязвимостей и реализации угроз на основе описания шаблонов

компьютерных атак, содержащихся в базах знаний, характеризующих различные аспекты безопасности программного и аппаратного обеспечения, предложена **семантическая модель текстовых описаний угроз и уязвимостей** зоны объекта КИИ

На этапе анализа сценариев реализации угроз с возможностью приоритезации 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**, основанная на применении методов машинного обучения и интеллектуального анализа собираемых данных мониторинга состояния объектов и сущностей в виде многомерных временных рядов.

С целью параметризации и оценки угрозы нарушения конфиденциальности и целостности информации и оценки соблюдения требований политики информационной безопасности объекта КИИ разработан **комплекс моделей анализа поведения пользователей конечной системы**

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

Предложена **общая схема построения нечеткой когнитивной модели оценки рисков информационной безопасности.**

Таким образом, 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.

Глава 3. Разработка метода и алгоритмов комплексной оценки рисков ИБ объекта КИИ на основе семантического анализа текстовых описаний угроз и уязвимостей

Предлагаемая ФСТЭК России Методика [2] оценки угроз безопасности информации предусматривает последовательный анализ каждой угрозы из полного перечня с оценкой возможного сценария ее реализации посредством эксплуатации цепочки уязвимостей. Непосредственное сопоставление угроз и уязвимостей осуществляется экспертом вручную на основе работы с веб-интерфейсом поиска и фильтрации перечней угроз и уязвимостей по ключевым параметрам на сайте ФСТЭК. Проблемой является трудоемкость соотнесения угроз, уязвимостей и объектов воздействия злоумышленника.

3.1 Метод ранжирования по приоритетам угроз с учетом зависимостей между угрозами и выявленными для каждой зоны безопасности объекта КИИ уязвимостями

На основе предложенной в работе модели оценки семантической близости текстовых описаний угроз и уязвимостей разработан **метод приоритезации угроз с учетом зависимостей между угрозами и выявленными для каждого элемента зоны объекта КИИ уязвимостями (рисунок 3.1)**. 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 $\mathrm{T} = \{T_1, T_2, \dots, T_l\}$ и множества уязвимостей $\mathrm{V} = \{V_1, V_2, \dots, V_t\}$ на основе анализа матрицы S оценок семантической близости текстовых описаний:

$$\begin{pmatrix} & V_1 & V_2 & \cdots & V_m \\ T_1 & d(T_1,V_1) & d(T_1,V_2) & \cdots & d(T_1,V_m) \\ T_2 & d(T_2,V_1) & d(T_2,V_2) & \cdots & d(T_2,V_m) \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ T_n & d(T_n,V_1) & d(T_n,V_2) & \cdots & d(T_n,V_m) \end{pmatrix} \quad (3.1)$$

Пороговая фильтрация и экспертная корректировка разреженной матрицы позволяет для каждого 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**.

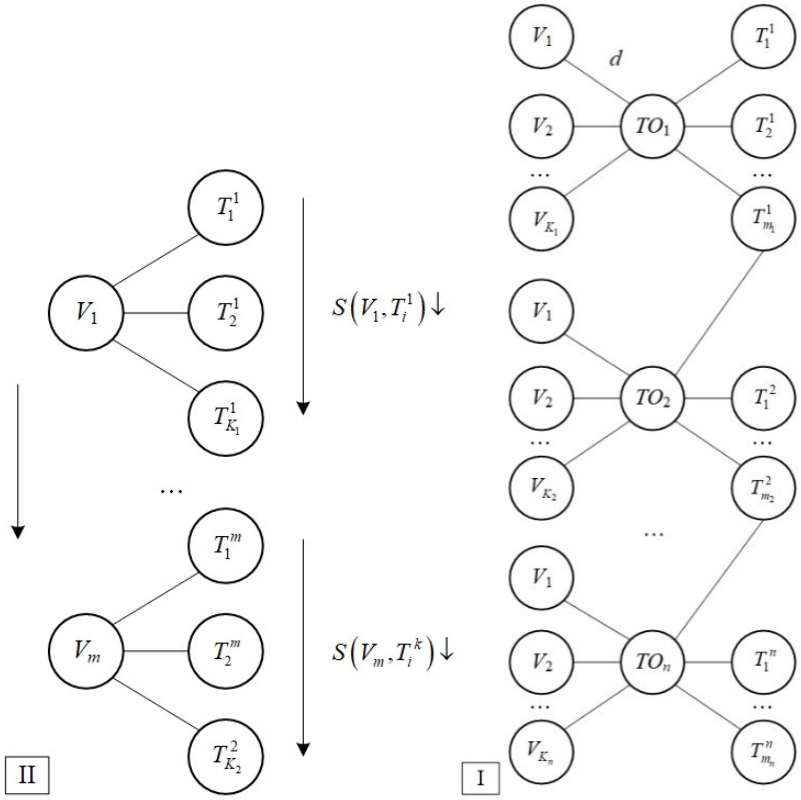


Рисунок 3.1 – а) Список актуальных уязвимостей, ранжированных по степени критичности, и сопоставленные с ними угрозы (в порядке убывания метрики семантической близости), б) соотнесения множества угроз T и уязвимостей V через промежуточные узлы – объекты воздействия TO (TO_j – объект воздействия, $j = \overline{1,n}$; T_j^i – угроза, связанная с TO_j; $i = \overline{1,m_j}$; V_{K_j} – уязвимость, связанная с TO_j)

Предлагается следующий алгоритм сопоставления множеств **T** и **V**:

- формирование перечня возможных объектов воздействия злоумышленника, предусмотренных в БДУ ФСТЭК;
- группировка и обобщение объектов воздействия на основе семантической близости их текстовых описаний;
- соотнесение с каждым объектом воздействия списка угроз на основе ссылок в БДУ;
- сопоставление с каждым объектом воздействия списка потенциальных уязвимостей программного обеспечения на основе оценки семантической близости текстового описания характеристик уязвимости и объекта воздействия.

Подобная схема соотнесения позволяет выбрать те объекты, которые присутствуют в конкретной информационной системе, и предварительно

отфильтровать из общего перечня угроз и уязвимостей БДУ только те сущности, для которых установлено соответствие через выделенные ТО, что существенно сокращает трудозатраты эксперта на ручную сортировку и перебор вариантов.

Ключевым элементом структуризации – выстраивания отношений между сущностями (угрозы, уязвимости, объекты воздействия) – является оценка семантической близости их текстовых описаний на основе косинус-расстояния (2.1) между векторами вложений, построенных с помощью предобученных моделей Doc2Vec и Word2Vec для русского языка.

3.1.1 Архитектура конвейера по обработке текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения объекта КИИ

Разработана **архитектура конвейера по обработке текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения объекта КИИ** (рисунок 3.2). Основные этапы предобработки и формализации текстовых описаний описаны в таблице 3.1 и реализованы в виде NLP-pipe конвейера согласно предложенной архитектуре с применением специализированных фреймворков Text Mining с учетом особенностей русского языка.

Таблица 3.1 – Основные этапы предобработки текстовых описаний угроз и уязвимостей на русском языке

Этап		**Методы и инструменты**
Предобработка	Токенизация	Токенизация на основе адаптивной нейросетевой модели Razdel [272]
	Символьная фильтрация	Регулярные выражения формата regexp, 38 регулярных выражений для фильтрации URLs, HTML-tags и пр.
	Фильтрация токенов	NLTK словари русского и английского языка, дополненные выделенным вручную списком стоп-слов, 400 токенов
Нормализация	Лемматизация	Фреймворк Natasha (нейросетевая модель Morph)
Модель вложений	Doc2Vec Distributed Memory	Модель Gensim (минимальная частота встречаемости слова – 1, количество отбрасываемых слов – 3, размер вектора вложений – 100)
	Word2Vec CBOW	Модель Gensim (минимальная частота встречаемости слова – 1, количество отбрасываемых слов – 3, размер вектора вложений – 100)
Вектор признаков	Композиция	Агрегированный вектор: Doc2Vec и нормированный TF-IDF Word2Vec для лексем в тексте

Загрузка данных из локальной БД (1) – преобразования 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) (рисунок 3.3), редуцированного пространства признаков с помощью метода главных компонент (PCA) или приближения и проекции однородного многообразия (UMAP).

Визуальная оценка при разной заданной избирательности модели векторизации позволяет оценить, насколько компактными и отделимыми являются формируемые группы текстовых описаний угроз и уязвимостей. Основная задача данного этапа – оценить, имеется ли структура в данном признаковом пространстве у данных, т.е. присутствует ли группировка семантически близких сущностей в отделимые кластеры.

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 3.2 – Архитектура конвейера по обработке данных текстовых описаний угроз и уязвимостей

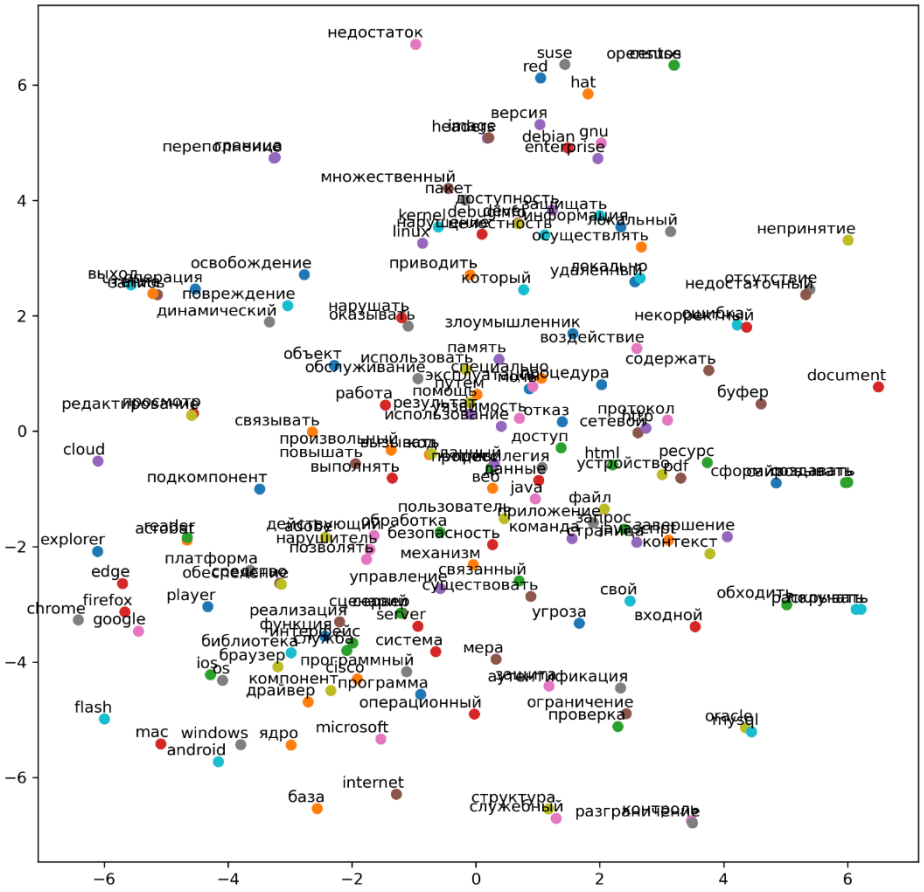


Рисунок 3.3 – Двухмерная визуализация стохастического вложения соседей с t-распределением (TSNE) редуцированного пространства признаков распределенного векторного представления Doc2Vec

Текстовые описания угроз и уязвимостей из БДУ обрабатываются с помощью описанной выше схемы конвейера NLP-pipe (таблица 3.1). Для подготовленных описаний строится композиция моделей вложений Doc2Vec и Word2Vec (TF-IDF). Затем композиция формализованных векторов используется для построения реляционной базы хранения текстовых описаний угроз и уязвимостей с соответствующими признаками.

Из описаний каждой угрозы выделяется текстовое поле «Объект воздействия», записи группируются в 22 определенные экспертно категории с предобработанным текстовым описанием и формализованным вектором признаков **ТО** на основе их семантической близости. Далее выполняется кластеризация формализованных описаний уязвимостей **V** с заданными центрами кластеров в виде векторов **ТО**. С каждым кластером на основе ссылок связана группа угроз **T**.

Источниками информации о выявленных или потенциальных уязвимостях программного обеспечения системы являются:

– система сбора и корреляции событий информационной безопасности SIEM (1),

– результаты работы сканеров безопасности,

– система инвентаризации программного и аппаратного обеспечения,

– обогащенные данные с платформы TI.

Существует тенденция интеграции перечисленных выше систем в состав центра мониторинга и оперативного реагирования на ИБ-инциденты (SOC). По запросу специалиста по ИБ, осуществляющего мониторинг и оценку уровня защищенности системы, формируется перечень потенциальных уязвимостей программного обеспечения и перечень объектов воздействия злоумышленника (целевых информационных ресурсов). Затем эксперт с помощью списка объектов потенциального воздействия злоумышленника для конкретной системы и определяет соответствие выявленных уязвимостей и релевантных им угроз нарушения ИБ.

3.1.2 Анализ корпуса русскоязычных текстов – описаний уязвимостей БДУ ФСТЭК

Корпус текстов для анализа построен из агрегированных текстовых описаний уязвимостей на русском языке из БДУ ФСТЭК России. Составное текстовое поле включает данные о характеристике уязвимости и вариантах ее эксплуатации:

Количество документов	22275
Размер словаря	8975
Общее число токенов после предобработки	598436

Структура конвейера NLP-Pipe для обработки данных представлена в таблице 3.2.

Таблица 3.2. – Структура конвейера NLP-Pipe

Этап	**Шаги**	**Действия**	**Инструменты**
Предобработка	символьная фильтрация	Удаление нерелевантных символов, разворачивание сокращений, очистка от html-тегов	Набор из 40 регулярных выражений и библиотека Buitiful-Soup
	токенизация	Разбивка текста на токены с помощью предобученной для русского языка нейросетевой модели	Razdel [272] (фреймворк Natasha)
	фильтрация нерелевантных токенов	Удаление дат, цифр, чисел, ссылок, сокращений	Регулярные выражения
Нормализация	лемматизация	Приведение слов в исходную форму с помощью предобученной нейросетевой модели	Morph (фреймворк Natasha)

Постобработка	частеречная фильтрация	Остаются только существительные, глаголы, прилагательные, наречия, местоимения	Morph (фреймворк Natasha)
	фильтрация на основе стоп-словарей	Фильтрация нерелевантных лемм с помощью составного стоп-словаря, включающего наиболее часто встречающиеся слова корпуса текстов	NLTK-russian, NLTK-english
	Формирование документа-строки	Объединение лемм в нормализованную строку-документ	

Предварительный анализ корпуса текстов для оценки структуры корпуса и возможности применения моделей для построения предикторов приведен в Приложении Б.

Далее для формализации признаков строится нейросетевая модель векторного вложения для текстовых документов Distributed memory (PV-DM) Doc2Vec [240] (таблица 3.3).

Таблица 3.3 – Параметры Distributed memory (PV-DM) Doc2Vec Model

Параметр	**Значение**
Размерность вектора признаков	100
Размер окна анализа	5
Минимальная частота встречаемости слова для включения в модель	2
Количество эпох обучения	100

Для каждого документа корпуса с помощью обученной D2V и W2V модели строится вектор формальных признаков, на основе которого может быть оценена семантическая близость документов как косинус мера расстояния между векторами [21]. Это позволяет выполнять более качественный по сравнению с частотно-словарным (TF-IDF) поиск наиболее близких по смыслу документов (таблица 3.4).

Таблица 3.4 – Фрагмент из БД описания угроз и уязвимостей

Идентификатор УБИ	**Объект воздействия**	**text**	**tokens**	**doc_vec**	**w2v_vec**
1	Ресурсные центры грид-системы	Угроза автоматического распространения вредоно...	[угроза, автоматический, распространение, вред...	[0.7531, 0.0704, -0.0610, -1.0642...	[-0.3071, -0.1333, -0.1...
…	…	…	…	…	…
Идентификатор	**Класс уязвимости**	**text**	**tokens**	**doc_vec**	**w2v_vec**
BDU:2014-00001	Уязвимость архитектуры	Уязвимость микропрограммного обеспечения прогр...	[микропрограммный, обеспечение, программироват...	[0.3814, 0.2239, -0.1751, -0.2505...	[-0.2814, 0.0188, -0...

Предварительно рассчитанная разреженная матрица попарных расстояний позволяет существенно ускорить процедуру поиска и группировки уязвимостей. Пример поиска семантически близких описаний уязвимостей представлен в таблице 3.5.

Таблица 3.5 – Семантически близкие текстовые описания уязвимостей в порядке убывания косинус-меры

№	Документ	Мера близости
0	Уязвимость микропрограммного обеспечения программируемого логического контроллера Schneider Electric Modicon Quantum, позволяющая злоумышленнику получить авторизованный доступ к устройству. Микропрограммное обеспечение модуля 140NOE77111 контроллера Schneider Electric Modicon Quantum содержит множество пар логин: пароль, предустановленных по умолчанию. Это позволяет любому пользователю, имеющему доступ к устройству по протоколу FTP, получить авторизованный доступ к устройству	1
1	Уязвимость FTP-сервера микропрограммного обеспечения программируемых логических контроллеров Schneider Electric Modicon Premium, Modicon Quantum, Modicon M340 и Modicon BMXNOR0200, позволяющая нарушителю получить доступ к устройству. Уязвимость FTP-сервера микропрограммного обеспечения программируемых логических контроллеров Schneider Electric Modicon Premium, Modicon Quantum, Modicon M340 и Modicon BMXNOR0200 связана с использованием предустановленных учетных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к устройству	0,6742
…	…	…
25	Уязвимость микропрограммного обеспечения программируемого логического контроллера Modicon, связанная с раскрытием информации, позволяющая нарушителю получить доступ к конфиденциальной информации. Уязвимость микропрограммного обеспечения программируемого логического контроллера Modicon связана с раскрытием информации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить доступ к конфиденциальной информации протокола SNMP при чтении блоков памяти контроллера с использованием протокола Modbus	0,5761

Анализ таблицы 3.5 показывает, что выделенные уязвимости семантически близки к исходному документу, предварительно построенная матрица попарных расстояний близости описаний позволяет за константное время выполнять поиск близких описаний уязвимостей и их ранжирование для представления специалисту, проводящему аудит защищенности системы.

Таким образом, предложен метод и алгоритм семантического анализа текстовых описаний угроз и уязвимостей, отличаются подходом к формализации слабоструктурированных текстовых описаний угроз и уязвимостей с помощью гетерогенных нейросетевых моделей вложений, что позволяет обеспечить

выявления потенциальных угроз и уязвимостей с возможностью их приоритезации, а также автоматизировать основные этапы процедуры оценки рисков.

3.2 Система анализа угроз и уязвимостей объекта КИИ на основе технологий семантического анализа их текстовых описаний

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) и приоритезации для последующего структурирования, выявления наиболее опасных сценариев реализации атак и оценки их последствия на основе предложенных моделей и метода разработана **автоматизированная система анализа угроз и уязвимостей объекта КИИ на основе технологий семантического анализа их текстовых описаний**.

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

Структурно-функциональная организация системы анализа угроз и уязвимостей объекта КИИ включает в себя следующие основные подсистемы (рисунок 3.4):

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

Подсистема локального хранения актуальной копии БДУ ФСТЭК (I) предназначена для построения СУБД с объектно-ориентированным проецированием (ORM) хранимых сущностей, характеризующих угрозы и уязвимости в формате открытого языка описания и оценки уязвимостей (OVAL), на сериализуемые файлы с выбранной XML-схемой. Модуль синхронизации с внешней БД сопоставляет (5) временные метки изменений данных внешнего хранилища БДУ

ФСТЭК (1) и метки в локальном хранилище. По результатам сопоставления принимается решение о запуске (4) механизма синхронизации. Модуль выгрузки XML-описаний угроз и уязвимостей из внешней базы подключается (2) к серверу БДУ и выполняет импорт данных (3) в локальную СУБД в требуемом формате.

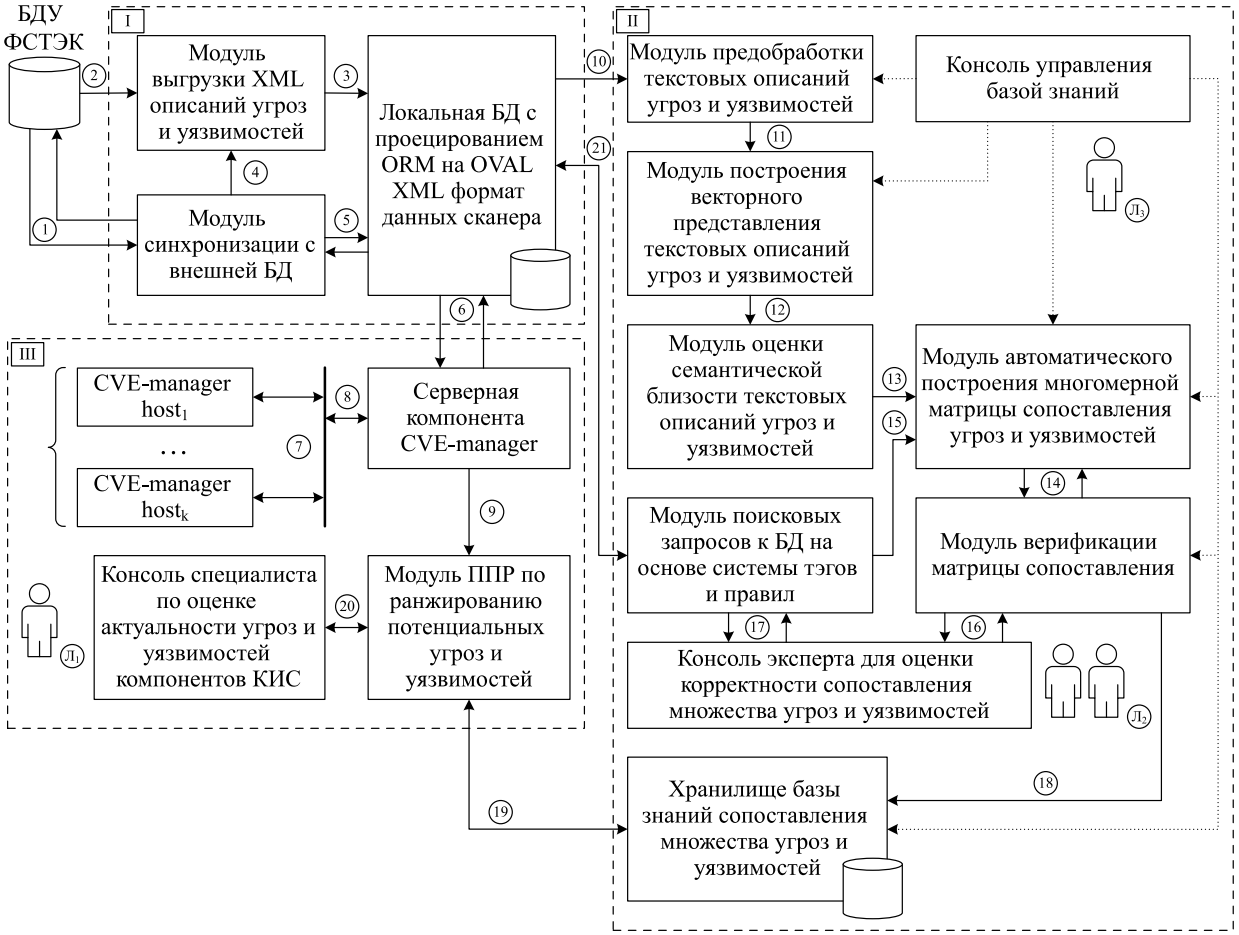


Рисунок 3.4 – Структурно-функциональная организация системы отбора и анализа актуальных угроз и уязвимостей на основе оценки семантической близости их текстовых описаний

Подсистема сопоставления угроз и уязвимостей на основе их текстового описания (II) предназначена для построения базы знаний, описывающей отображение множества уязвимостей на множество угроз.

БДУ, помимо формальных метрик, содержит текстовое описание уязвимости и угрозы, характеризующее особенности их проявления и возможности эксплуатации злоумышленником. Модуль предобработки текстовых описаний угроз и уязвимостей извлекает (10) данные из локального хранилища и выполняет цепочку подготовительных преобразований текстовых описаний (фильтрацию и нормализацию) сущностей для передачи (11) в модуль построения их формализованных векторных представлений. Модуль оценки семантической близости текстовых описаний использует (12) формализованные векторы признаков каждой сущности для попарной оценки сходства на основе косинус-метрики.

Далее, модуль автоматизированного построения многомерной матрицы сопоставления угроз и уязвимостей на основе оценок семантической близости формирует (13) матрицу отображения множества уязвимостей на множество угроз S.

Эксперты (Л2) с помощью консоли доступа выполняют оценку (16) корректности сопоставления множества угроз и уязвимостей и выполняют корректировку в случае необходимости. В процессе верификации (14) матрицы сопоставления эксперты опираются (17) на имеющийся механизм поисковых запросов к локальной БД на основе системы тегов и правил фильтрации, предусмотренных БДУ ФСТЭК (21, 15). Верифицированные сопоставления угроз и уязвимостей помещаются в хранилище базы знаний для последующего использования экспертами в ходе аудита ИБ корпоративной ИС. Специалист по знания (Л3) управляет работой модулей предобработки и векторизации текстовых описаний, а также следит за метриками качества базы знаний.

Подсистема оценки актуальных угроз и уязвимостей для корпоративной информационной системы (III) с помощью клиент-серверного сканера (CVE-manager) обеспечивается сбор (7, 8) данных об уязвимостях программного обеспечения рабочих станций и серверов ИС. Применяется связка ПО CVE-manager и ScanOVAL для ОС Linux и Windows, управляемое серверной компонентой, и взаимодействующее (6) с локальной БД. Результаты поиска уязвимостей с помощью сканеров безопасности представляются в виде XML документов с разметкой на языке OVAL. Применение графических интерфейсов работы с найденными уязвимостями ScanOVAL и WEB-интерфейс БДУ ФСТЭК позволяют выполнить фильтрацию найденных уязвимостей по 15 параметрам. Однако, ввиду значительного количества выявляемых уязвимостей на отдельных хостах (более 200 уязвимостей для системы с систематическим обновлением минимального набора прикладного ПО), ручная фильтрация даже наиболее критических по оценкам уязвимостей может занять длительное время. Существующие решения позволяют упростить поиск и сопоставление актуальных угроз и уязвимостей для конкретных версий ПО, но дальнейшая автоматизация процедуры подбора актуальных угроз и уязвимостей на основе данных интеллектуальной фильтрации и оценки семантической близости их текстовых описаний позволит масштабировать решение для крупных ИС. С помощью консоли специалист по ИБ (Л1) выполняет оценку (20) актуальных угроз и уязвимостей для отдельных узлов ИС, руководствуясь рекомендациями модуля поддержки принятия

решений по ранжированию и сопоставлению потенциальных угроз и уязвимостей, полученных (9) в результате сканирования ПО ИС, и механизмами интеллектуальной фильтрации (19) на основе извлекаемых из базы знаний (рисунок 3.5).

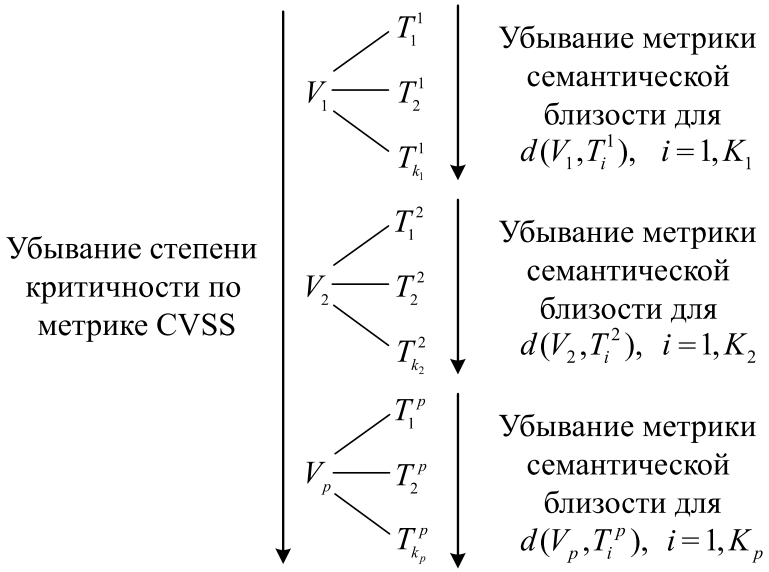


Рисунок 3.5 – Список актуальных уязвимостей, ранжированных по степени критичности, и сопоставленные с ними угрозы (в порядке убывания метрики семантической близости)

3.2.1 Исследование отношения «уязвимости – релевантные угрозы» на основе оценки семантической близости описаний

Доступная база уязвимостей содержит 27085 записей, база угроз – 217 записей. Из текстовых описаний объемом 740634 слова был сформирован словарь 12884 уникальных слов. После процедуры предобработки и нормализации построена модель Doc2Vec с помощью фреймворка Gensim. Размер формализованного вектора признаков выбран равным 100, количество эпох обучения модели равно 40. Параметры модели подбирались экспериментально.

В качестве иллюстрации работы системы рассмотрим выявленную хостовым сканером безопасности уязвимость BDU:2015-00285 «Уязвимость программного обеспечения Flash Player, позволяющая удаленному злоумышленнику нарушить конфиденциальность, целостность и доступность защищаемой информации». Данной уязвимости эксперт в ручном режиме поставил в соответствие угрозу УБИ.192 (таблица 3.6). Используя текстовое описание уязвимости, с помощью разработанного модуля автоматизированной системы осуществим выбор семантически близких по описанию угроз из БДУ ФСТЭК. На рис. 3.6 показаны

результаты подбора 10 релевантных угроз, отсортированных в порядке убывания метрики семантической близости.

Как видно из рисунка, угроза УБИ.192 попадает в данный перечень, что совпадает с результатом предварительного экспертного оценивания. Аналогичным образом, для выбранных в процессе экспертного анализа и сбора данных сканерами уязвимостей (поиск установленных версий ПО с имеющимися уязвимостями по БДУ) производится подбор соответствующих угроз. Финальная стадия анализа позволяет упростить работу эксперта, значительно сократив время на поиск и сопоставление уязвимостей и угроз.

Таблица 3.6 – Экспертное сопоставление угроз и уязвимостей из БДУ ФСТЭК

Угроза	Уязвимость	Воздействие/уровень опасности
УБИ.192 Угроза использования уязвимых версий программного обеспечения.	BDU:2015-00285 Уязвимость программного обеспечения Flash Player, позволяющая удаленному злоумышленнику нарушить конфиденциальность, целостность и доступность защищаемой информации	Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10)

Применяемые для префильтрации средства [101, 121] позволяют упростить поиск и сопоставление актуальных угроз и уязвимостей для конкретных версий ПО и сократить количество просматриваемых экспертом угроз для отдельной уязвимости с 200 до 4.

Рисунок 3.6 – Релевантные угрозы, отсортированные в порядке убывания нормированной метрики семантической близости (score) к данной уязвимости BDU:2015-00285

Сравнение процедуры анализа уязвимостей WEB-браузера Firefox с [101, 121] приведены в таблице 3.7.

Таблица 3.7 – Сравнение процедуры анализа уязвимостей

Параметр	Поиск по тегам	Система [101, 121]	Автоматизированная система на основе Text Mining
Ввод информации	Вручную, графический WEB-интерфейс БДУ	Формирование запроса оператором в графическом интерфейсе	Автоматизированная обработка результатов работы сканеров уязвимостей
Количество найденных уязвимостей	41	41	48
Количество сопоставленных угроз	2 (ручное сопоставление)	8 (задается на основе сформированной матрицы)	10 (задается пороговыми и количественными метриками, определяющими чувствительность фильтра на основе сформированной матрицы)
Затраченное время	Более 11 минут	20 с	< 5 с

Согласно оценке [121], время, затрачиваемое на сопоставление угроз и уязвимости «вручную» для полного списка, при этом составляет более 2 часов, применение же предлагаемых решений позволяет сократить время анализа до 20 секунд. Предлагаемая система для сопоставления на основе анализа текстовых описаний позволяет выполнить ранжирование оставшихся угроз по степени их семантической близости к конкретной уязвимости, тем самым дополнительно снижая когнитивную нагрузку на эксперта и уменьшая время анализа.

Таким образом, рассмотрена архитектура системы анализа критичных уязвимостей ПО с использованием технологии Text Mining, основанная на алгоритмах векторного представления слов и оценки семантической близости текстовых описаний уязвимостей, выявленных с помощью сканеров безопасности, и описаний релевантных угроз из БДУ ФСТЭК России. Программная реализация [104, 106] клиент-серверного прототипа данной системы и интеграция с модулями существующих решений позволяют:

– автоматизировать процесс сопоставления и ранжирования угроз ИБ для каждой выявленной уязвимости на рабочих станциях и серверах в составе корпоративной информационной системы;

– сократить время ручного анализа экспертом результатов работы сканеров за счет интеллектуальной фильтрации и ранжирования списка угроз;

– снизить когнитивную нагрузку на эксперта и повысить достоверность оценки степени критичности уязвимостей ПО за счет использования

дополнительной информации о фактически существующих зависимостях между выявленными уязвимостями и потенциальными угрозами;

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

3.3 Система оценки степени опасности уязвимостей

Разработана **структура системы [123] оценки опасности уязвимостей** на основе прогнозирования компонент метрики с помощью анализа текстового описания угроз и уязвимостей для повышения точности и оперативности оценки.

Структура предлагаемой системы для оценки степени опасности уязвимости CVSS 2.0/3.0 представлена на рисунке 3.7.

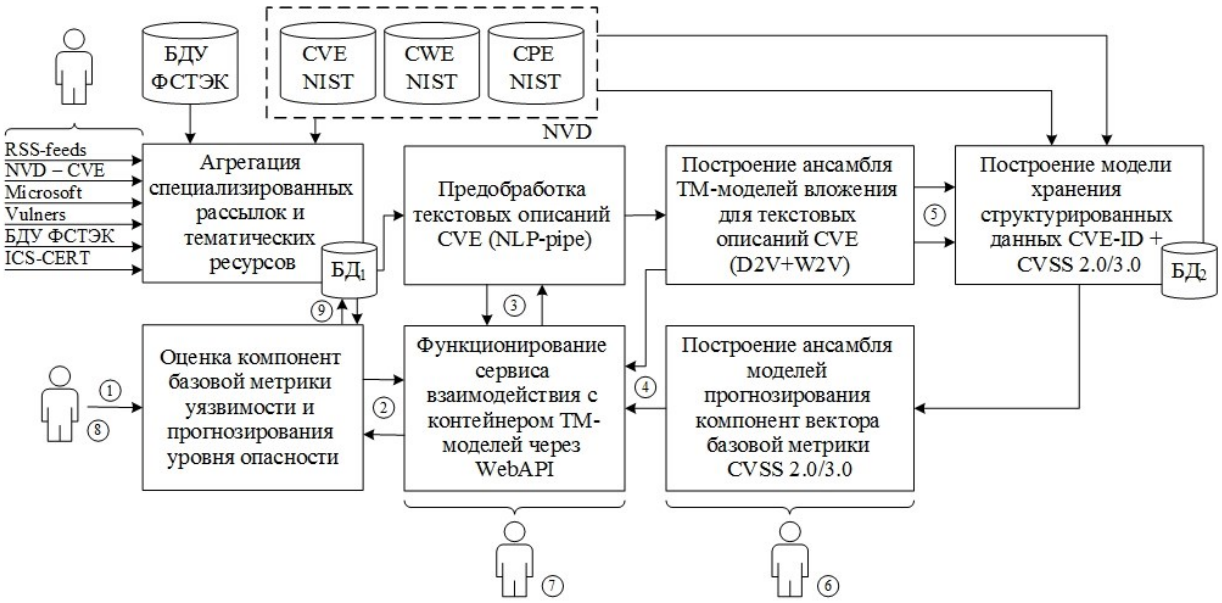


Рисунок 3.7 – Структура системы оценки степени опасности уязвимостей на основе интеллектуального анализа данных

Первый этап работы системы связан со сбором и агрегацией специализированных новостных рассылок и тематических ресурсов в виде слабоструктурированных текстовых данных для построения документоориентированной $БД_1$ (MongoDB) с привязкой записей к ключу CVE-ID из БДУ ФСТЭК и NVD (CVE, CWE (БД недостатков ПО, которые могут быть использованы злоумышленниками), CPE (формальный язык описания всех возможных продуктов, операционных систем и аппаратных устройств при описании уязвимостей)). Процесс сбора данных регулируется специалистами по информационной безопасности с применением Threat Intelligence.

Затем собранные текстовые данные подвергаются предобработке и нормализации: символьная фильтрация, токенизация, фильтрация на основе стоп-словарей, лемматизация – на основе технологии конвейеризации NLP-Pipe.

Далее строится ансамбль Text Mining моделей вложения на основе очищенных текстовых описаний уязвимостей с привязкой к ключу CVE-ID как взвешенная комбинация Doc2Vec и Word2Vec моделей. С помощью D2V и W2V моделей (5) формируется вектор вложений текстовых описаний для $БД_2$, предназначенной для хранения структурированных данных {CVE-ID, вектор CVSS 2.0/3.0, Text Embedded Vector}.

На следующем шаге конструируется ансамбль моделей для прогнозирования компонент вектора базовой метрики CVSS 2.0/3.0.

Подготовленные модели прогнозирования вектора CVSS 2.0/3.0 помещаются в контейнер (4) для размещения на сервере для обработки запросов от пользователей системы через WebAPI.

Второй этап предполагает обработку запросов (1) по оценке уровня опасностей выявленных уязвимостей, для которой отсутствует оценка CVSS и размеченный вектор базовой метрики от специалиста по информационной безопасности (8), проводящего аудит ИС. Выполняется передача (9 и 2) текстовых описаний уязвимости и/или CVE-ID в одну из баз уязвимостей, а также проводится подготовка (3) его нормализованного и предобработанного текстового описания.

Поддержка адекватного состояния и дообучение моделей прогнозирования осуществляется инженером по работе с моделями машинного обучения (machine learning, ML) (6). Функционирование контейнера ML-моделей на сервере и обработка WebAPI запросов обеспечивается инженером поддержки Web-сервиса (7).

3.3.1 Экспериментальная оценка степени опасности уязвимостей на основе технологий ИАД текстовых описаний БДУ ФСТЭК России

Для оценки BaseScore CVSS 2.0 рассмотрим два сценария:

– построение ансамбля предикторов для оценки отдельных значений компонент (AV, AC, Au, C, I, A) по формализованному текстовому описанию с последующим расчетом оценки уровня опасности (таблица 3.9);

– построение модели регрессии для непосредственной оценки результирующего значения по формализованному текстовому описанию.

Построение ансамбля предикторов выполнено для 75% доступных документов с формальным вектором признаков, сформированным с помощью D2V модели. Оптимизация гиперпараметров используемых моделей предикторов выполнена с помощью процедуры перебора по сетке (GridSearch) с применением перекрестной проверки с разбиением на 5 блоков. Параметры подбора приведены в таблице 3.8.

Таблица 3.8 – Параметры моделей предикторов

Классификатор	Параметры обучения		
	Число моделей	K-fold перекрестная проверка	Среднее время, мин
SGD (SVM) Классификатор на основе машины опорных векторов	576	5	35
SGD (LR) Классификатор на основе модели линейной регрессии	288	5	19,3
K-Neighbors Классификатор k ближайших соседей	12	5	3.9
RandomForest Классификатор на основе комитета случайных деревьев решений	60	5	26,3

Результаты работы каждого предиктора на обучающей и тестовой выборках (25% исходных документов) для всех компонент вектора базовой метрики приведены в таблице 3.9 и на рисунке 3.8.

Оценка классификаторов выполнена с помощью следующих метрик:

– Accuracy (точность) показывает долю правильных классификаций.

– Precision (точность) показывает долю объектов класса среди всех объектов, выделенных классификатором

– Recall (полнота) отражает долю найденных объектов класса от общего числа объектов класса.

– F_1 – среднее гармоническое Precision и Recall.

Таблица 3.9 – Результаты работы предикторов на обучающей и тестовой выборках

Компонент	Классификатор	Обучающая выборка				Тестовая выборка			
		F_1	Accuracy	Precision	Recall	F_1	Accuracy	Precision	Recall
AV	SGD (SVM)	0,948	0,958	0,939	0,958	0,948	0,958	0,939	0,958
	SGD (LR)	0,744	0,804	0,818	0,804	0,744	0,804	0,816	0,804
	KNeighbors	1,000	1,000	1,000	1,000	0,963	0,965	0,964	0,965
	RandomForest	1,000	1,000	1,000	1,000	0,948	0,953	0,955	0,953
AC	SGD (SVM)	0,588	0,645	0,590	0,645	0,580	0,640	0,581	0,640
	SGD (LR)	0,555	0,652	0,594	0,652	0,552	0,650	0,584	0,650
	KNeighbors	1,000	1,000	1,000	1,000	0,759	0,766	0,759	0,766
	RandomForest	1,000	1,000	1,000	1,000	0,737	0,764	0,778	0,764

Au	SGD (SVM)	0,786	0,838	0,779	0,838	0,782	0,836	0,770	0,836
	SGD (LR)	0,771	0,843	0,710	0,843	0,771	0,843	0,710	0,843
	KNeighbors	1,000	1,000	1,000	1,000	0,898	0,901	0,896	0,901
	RandomForest	0,988	0,989	0,989	0,989	0,872	0,889	0,881	0,889
C	SGD (SVM)	0,661	0,673	0,665	0,673	0,652	0,665	0,657	0,665
	SGD (LR)	0,506	0,581	0,606	0,581	0,495	0,571	0,582	0,571
	KNeighbors	1,000	1,000	1,000	1,000	0,770	0,773	0,771	0,773
	RandomForest	1,000	1,000	1,000	1,000	0,772	0,779	0,781	0,779
I	SGD (SVM)	0,700	0,707	0,698	0,707	0,694	0,701	0,692	0,701
	SGD (LR)	0,579	0,637	0,677	0,637	0,569	0,630	0,671	0,630
	KNeighbors	1,000	1,000	1,000	1,000	0,778	0,783	0,778	0,783
	RandomForest	1,000	1,000	1,000	1,000	0,773	0,782	0,779	0,782
A	SGD (SVM)	0,583	0,660	0,617	0,660	0,581	0,658	0,612	0,658
	SGD (LR)	0,508	0,608	0,562	0,608	0,516	0,615	0,583	0,615
	KNeighbors	1,000	1,000	1,000	1,000	0,780	0,787	0,780	0,787
	RandomForest	1,000	1,000	1,000	1,000	0,770	0,785	0,783	0,785

Второй сценарий подразумевает построение модели регрессии на основе ансамбля решающих деревьев (Random Forest) с оптимизацией гиперпараметров с помощью процедуры перебора по сетке (GridSearch) с применением перекрестной проверки с разбиением на 5 блоков. Результирующая модель ансамбля включает 500 решающих деревьев с максимальной глубиной 8.

Для обучающей выборки среднеквадратичная ошибка (Root Mean Square Error) составила 0,669, а для тестовой – 1,316.

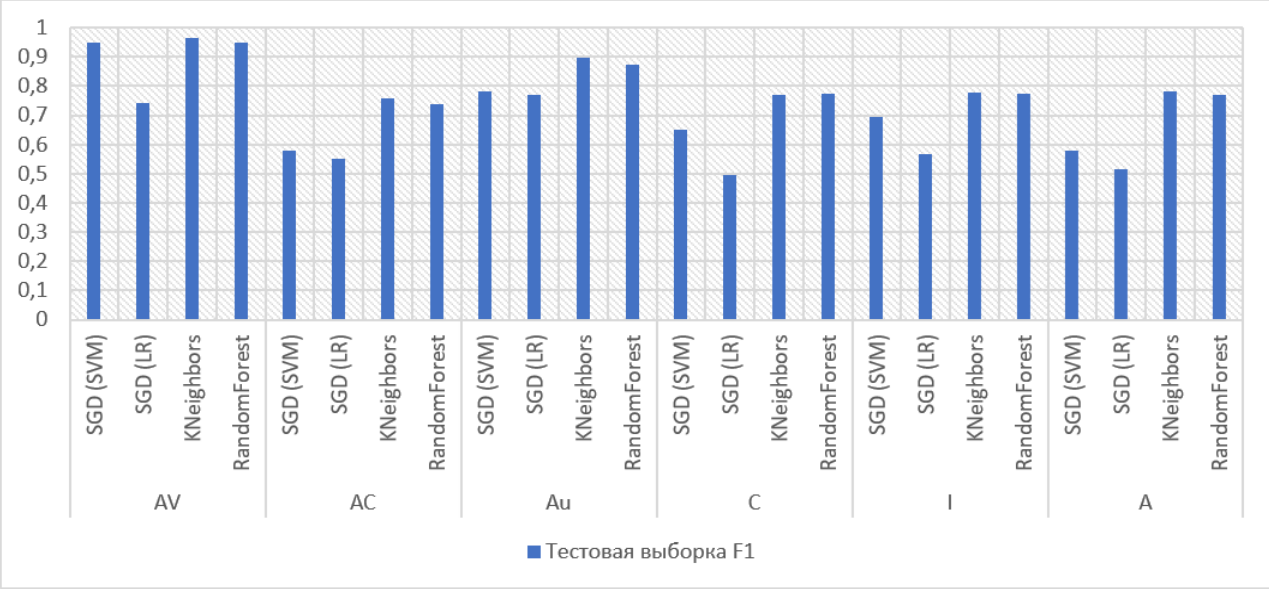


Рисунок 3.8 – Оценка F_1 меры для тестовой выборки по каждому классификатору и компоненту метрики

Прогноз оценки уровня опасности уязвимости для 50 примеров из обучающей выборки и 50 примеров тестовой выборки представлен на рисунке 3.9, где маркер «круг» – исходное значение, маркер «крест» – предсказанного, ось ординат – уровень опасности уязвимости.

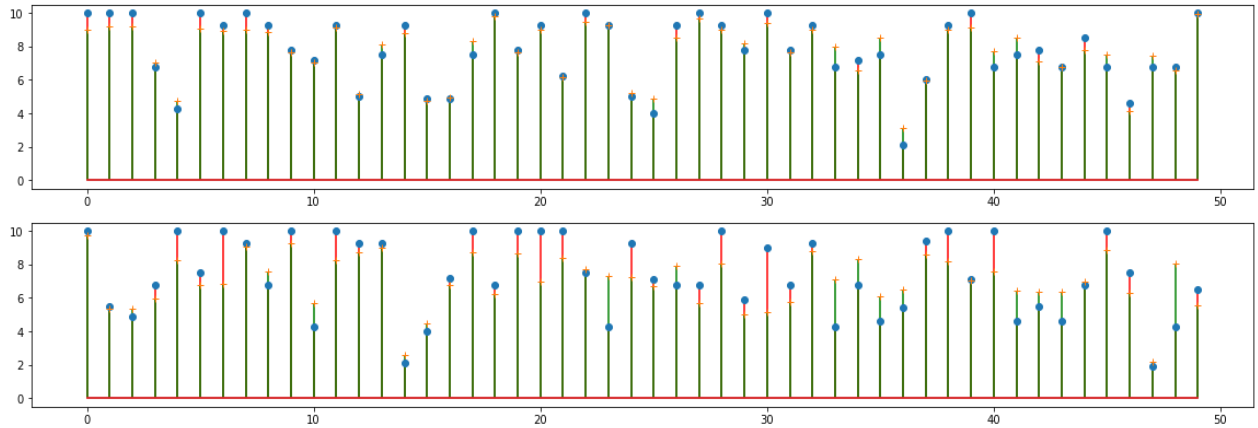


Рисунок 3.9 – Прогноз оценки уровня опасности уязвимости для 50 примеров из обучающей выборки (вверху) и 50 примеров тестовой выборки (внизу).

Анализ таблицы 3.9 показывает, что ансамбль предикторов позволяет получить оценку компонент вектора базовой метрики новых уязвимостей на уровне значения меры F_1 = 0,70-0,75 для тестовой выборки, что свидетельствует о хорошей обобщающей способности предлагаемого решения.

Модель регрессии на основе ансамбля решающих деревьев позволяет непосредственно оценивать уровень опасности уязвимости, но без определения компонент базовой метрики.

3.3.2 Экспериментальная оценка опасности уязвимостей на основе технологий интеллектуального анализа данных текстовых описаний NVD

Текстовые описания уязвимостей из базы NVD поступают в блок очистки, нормализации и предобработки с помощью NLP-pipe [287]. Формализация признаков текстовых описаний уязвимостей строится на основе нейросетевой модели векторного вложения для текстовых документов Doc2Vec (D2V) [228]. Нормализованные текстовые описания используются для построения и обучения D2V модели.

Корпус текстов для анализа построен из более чем 100000 агрегированных текстовых описаний уязвимостей из NVD. Структура конвейера NLP-Pipe для обработки данных представлена в таблице 3.10.

Таблица 3.10 – Структура конвейера NLP-Pipe

Этапы	Шаги	Действия	Инструменты
Предобработка	символьная фильтрация	Удаление нерелевантных символов, разворачивание сокращений, очистка от html-тегов	Набор из 40 регулярных выражений и библиотека Buitiful-Soup

	токенизация	Разбивка текста на токены с помощью предобученной для английского языка нейросетевой модели	spaCy + Gensim (SimpleTokenizer)
	фильтрация нерелевантных токенов	Удаление дат, цифр, чисел, ссылок, сокращений	Regular Expressions
Нормализация	лемматизация	Приведение слов в исходную форму с помощью предобученной нейросетевой модели	spaCy library
Постобработка	частеречная фильтрация	Остаются только существительные, глаголы, прилагательные, наречия, местоимения	spaCy library
	фильтрация на основе стоп-словарей	Фильтрация нерелевантных лемм с помощью составного стоп-словаря, включающего наиболее часто встречающиеся слова корпуса текстов	NLTK-english spaCy-english
	Формирование документа-строки	Объединение лемм в нормализованную строку-документ	

Для оценки BaseScore CVSSv2 рассмотрим два сценария:

- построение НС модели для оценки значений компонент метрики (AV, AC, Au, C, I, A) по формализованному текстовому описанию с последующим расчетом оценки уровня опасности;
- построение модели регрессии на основе комитета случайных деревьев для непосредственной оценки результирующего значения по формализованному текстовому описанию.

Параметры Doc2Vec модели Distributed memory (PV-DM) представлены в (таблица 3.11).

Таблица 3.11 – Параметры Distributed memory (PV-DM) Doc2Vec Model

Параметр	Значение
Dimension of feature vector	100
Analysis window size	5
The minimum frequency of occurrence of a word to be included in the model	2
Number of learning epochs	100

Построение НС моделей выполнено для 75% доступных документов с формальным вектором признаков, сформированным с помощью D2V модели. Оставшиеся 25% использованы для оценки обобщающей способности моделей.

Результаты работы НС моделей на обучающей и тестовой выборках (25% исходных документов) для всех компонент базовой метрики приведены в таблице 3.12 и рисунке 3.10

Таблица 3.12 – Результаты работы НС модели на обучающей и тестовой выборках

Компоненты	Значения компонент	Количество	Метрика	Train	Valid	Test
accessVector	NETWORK	123990	f1-score	0.967	0.955	0.956
	LOCAL	20832	accuracy	0.966	0.956	0.957
	ADJACENT_NETWORK	3591				
accessComplexity	LOW	86490	f1-score	0.880	0.848	0.839
	MEDIUM	57164	accuracy	0.888	0.857	0.848
	HIGH	4759				
confidentialityImpact	PARTIAL	72087	f1-score	0.913	0.841	0.837
	NONE	48060	accuracy	0.913	0.841	0.837
	COMPLETE	28266				
authentication	NONE	128022	f1-score	0.954	0.939	0.940
	SINGLE	20314	accuracy	0.956	0.942	0.943
	MULTIPLE	77				
integrityImpact	PARTIAL	77462	f1-score	0.932	0.864	0.861
	NONE	43560	accuracy	0.932	0.864	0.862
	COMPLETE	27391				
availabilityImpact	PARTIAL	62657	f1-score	0.881	0.827	0.828
	NONE	52982	accuracy	0.881	0.828	0.829
	COMPLETE	32774				

Второй сценарий подразумевает построение модели регрессии на основе ансамбля решающих деревьев (Random Forest) с оптимизацией гиперпараметров с помощью процедуры перебора по сетке (GridSearch) с применением перекрестной проверки и с разбиением на 5 блоков. Результирующая модель ансамбля включает 500 решающих деревьев с максимальной глубиной 8.

Для обучающей выборки RMSE составила 0.858, а для тестовой – 1.361.

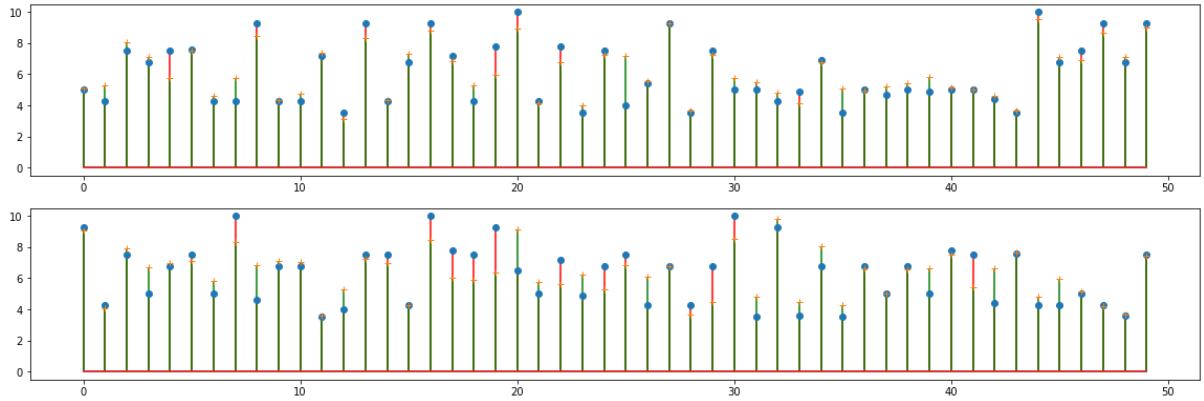


Рисунок 3.10 – Прогноз оценки уровня опасности уязвимости для 50 примеров из обучающей выборки (вверху) и 50 примеров тестовой выборки (внизу). Маркер «круг» – исходное значение, маркер «крест» – предсказанного. Ось абсцисс – уровень опасности уязвимости.

Проведены два эксперимента с описанием структуры классификаторов и регрессоров, разбиением на обучающую и тестовую выборки, с вычислением параметров точности, полноты, F_1 меры на тестовом и обучающем множестве.

Анализ таблицы 3.12 показывает, что НС модели позволяют получить оценку компонент базовой метрики новых уязвимостей на уровне $F_1 = 0.80\text{-}0.85$, что свидетельствует о хорошей обобщающей способности предлагаемого решения. Модель регрессии на основе ансамбля решающих деревьев позволяет непосредственно оценивать уровень опасности уязвимости, но без определения компонент базовой метрики. Значение RMSE среднеквадратической ошибки для обучающей выборки составила 0.858, а для тестовой – 1.361. Случайный контроль для примеров обучающей и тестовой выборки показал качественное соответствие оценки уровня опасности, формируемой моделью

Таким образом, предлагаемый подход основан на применении технологий интеллектуального анализа описаний уязвимостей на естественном языке. Отличительной особенностью является использование построение модели вложения слов и описаний уязвимостей и композиции классификаторов, выполняющих оценку компонент вектора метрики уязвимости согласно стандарту CVSS. Применение предлагаемого подхода позволит получить оценку метрики опасности (и ее компонент) зарегистрированной уязвимости на основе анализа семантической близости текстового описания к уже имеющимся в реестре записям.

Ансамбль нейросетевых моделей и регрессора на основе комитета случайных деревьев позволяет получить оценку компонент метрики опасности уязвимости CVSS на уровне $F_1 = 0.80\text{-}0.85$.

Практическая значимость обусловлена повышением эффективности (точности и оперативности) оценки метрик опасности уязвимостей с возможностью интеграции в систему аудита и инвентаризации для оперативного принятия мер по защите от новых уязвимостей.

3.4 Система построения и анализа семантической модели текстовых описаний угроз и уязвимостей объектов зоны объекта КИИ

Предложена **методика [29, 85] оценки актуальных угроз и уязвимостей программного обеспечения ИС объекта КИИ с использованием методов семантического анализа текстовых описаний угроз и уязвимостей.** 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.

Структура системы построения и анализа семантической модели текстовых описаний угроз и уязвимостей объектов зоны объекта КИИ представлена на рисунке 3.11.

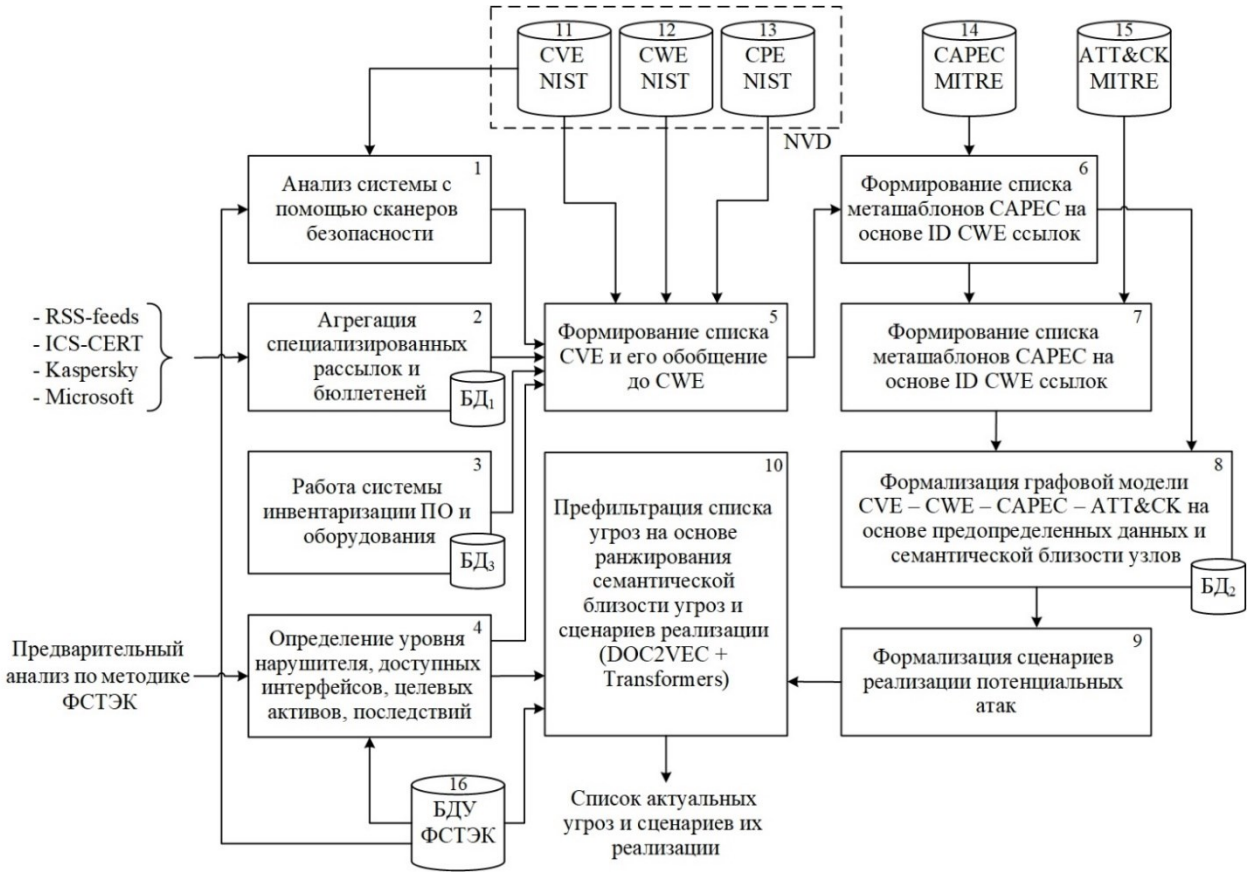


Рисунок 3.11 – Структура системы построения и анализа семантической модели текстовых описаний угроз и уязвимостей объектов зоны объекта КИИ

$БД_1$ – документированная база данных для агрегирования слабоструктурированных данных из внешних источников (MongoDB), $БД_2$ – графоориентированная база данных для хранения модели семантического описания сценариев реализации угроз.

Рассмотрим основные шаги предлагаемой методики:

Шаг 1. Семантический анализ агрегированного списка рассылок и бюллетеней. Для $БД_1$ формируется поисковый запрос, включающий описание основных узлов ИС, для построения списка семантически близких сообщений специализированных новостных рассылок. Из сформированного списка извлекаются индексы записей CVE и CWE. Поиск осуществляется как на основе оценки меры косинус-расстояния между вектором вложений, построенным с помощью

предобученных моделей Doc2Vec для русского и английского языка, так и на основе встроенного в $БД_1$ MongoDB языка запросов. Процедура предобработки и подготовки текстовых данных основана на построении конвейера NLP-pipe. Далее для формализации признаков строится нейросетевая модель векторного вложения для текстовых документов Distributed memory (PV-DM) [240] Doc2Vec.

Шаг 2. Анализ результатов работы сканеров безопасности. Формируется список выявленных уязвимостей для каждого компонента ИС в виде перечня CVE-ID и BDU-ID – идентификаторов выявленных уязвимостей.

Шаг 3. Фильтрация списка выявленных CVE на основе вектора доступа, сложности атаки, определенных в векторе базовой метрики CVSS для каждой уязвимости, и уровня нарушителя.

Шаг 4. Обобщение списка текстовых описаний CVE до текстовых описаний CWE.

Шаг 5. Последовательное выполнение запросов к локальным БД для формирования: списка меташаблонов CAPEC на основе списка CWE-ID, списка техник и тактик ATT&CK на основе списка ID CAPEC.

Шаг 6. Формализация графовой модели (на основе задания графа в виде списков вершин и ребер) в $БД_2$ Neo4j с расстановкой весовых коэффициентов на основе оценки меры семантической близости текстовых описаний с поддержкой реализации запросов на языке GraphQL.

Шаг 7. Обрезка графовой модели для удаления недостижимых вершин-листьев с повторной оценкой экспертом полученных техник, тактик и сценариев реализации атак (уточнение весового коэффициента и наличия ребра).

Шаг 8. Сопоставление текстовых описаний сценариев с базой угроз БДУ ФСТЭК с помощью модели Doc2Vec.

Шаг 9. Формализация семантической модели в виде иерархической нечеткой серой когнитивной карты (НСКК), позволяющей анализировать сценарии реализации атак с требуемым уровнем детализации за счет механизмов декомпозиции и укрупнения [11, 28], предложенной в [31].

Исходными данными для конструирования сценариев реализации атаки являются результаты работы экспертов по выявлению уязвимостей элементов ИС, а также потенциальных слабостей программного и аппаратного обеспечения. Наборы показателей системы оценки уязвимостей CVSS и базы данных угроз и уязвимостей позволяют формально описать сценарии эксплуатации

уязвимостей и автоматизировать построение цепочки возможных переходов между промежуточными узлами ИС.

В [31] рассматривается процедура «сворачивания» детализированной НСКК, раскрывающей содержание сценариев атак, до укрупненной НСКК уровня представления кибератаки. Каждая атака укрупняется до концепта НСКК с соответствующими весовыми коэффициентами, позволяющими оценить вероятность реализации атаки в каждом из возможных сценариев. Результирующая НСКК позволяет оценить уровень рисков ИБ при реализации воздействия нарушителя на промышленную систему. Наиболее детализированный уровень НСКК отражает ряд действий нарушителя на каждом этапе реализации угрозы, что позволяет получить развернутую итоговую оценку риска ИБ для целевых объектов ИС.

Под риском R_i понимается потенциальный ущерб, наносимый *i*-ому активу АСУ ТП предприятия (в относительных единицах) и приводящий к определенным согласно Методике киберфизическим последствиям. Предполагается, что значение риска ИБ определяется как установившееся значение состояния *i*-го целевого концепта.

Результирующая НСКК [316] оценки рисков нарушения кибербезопасности для целевых объектов ИС на основе выделенных сценариев реализации атак определяется в виде ориентированного графа.

3.1.2 Применение методики оценки актуальных угроз и уязвимостей ПО АСУ ТП с использованием методов семантического анализа текстовых описаний и когнитивного моделирования

Рассмотрим пример использования семантической модели анализа уязвимостей и актуальных угроз безопасности информации для фрагмента территориально-распределенной системы обустройства месторождения и транспорта товарной нефти, которая включает основные элементы: добыча нефти, сбор нефти, подготовка нефти, транспортировка товарной нефти.

Ввиду сложности анализируемого объекта, рассмотрим фрагмент базовой модели территориально распределенной системы – АСУ ТП пункта сдачи приема (ПСП) нефти (рисунок 3.12).

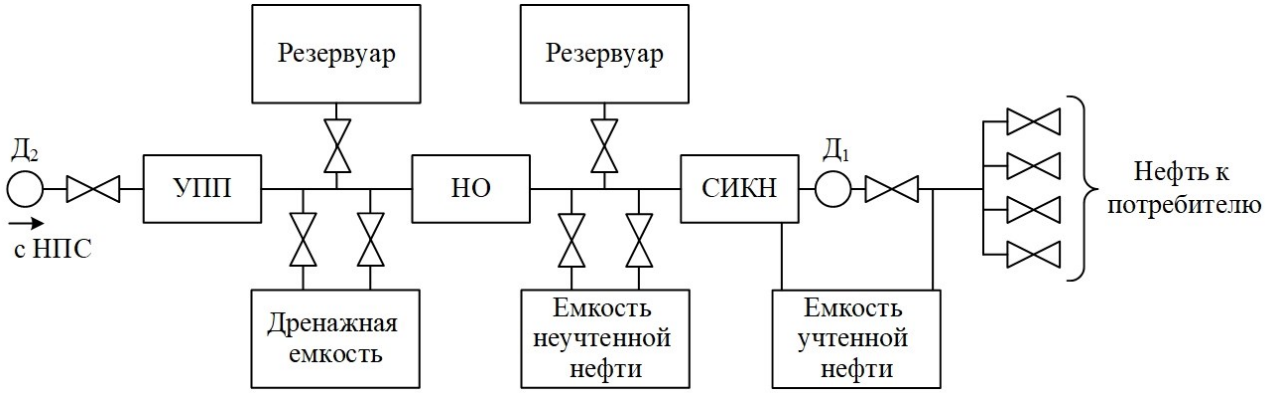


Рисунок 3.12 – Базовая модель АСУ ТП ПСП (Д1 – датчики СИКН; Д2 – датчики на входе НПС; УПП – установка подогрева продукта; НО – насосное оборудование; НПС – нефтеперекачивающая станция)

АСУ ТП ПСП в системе магистральных трубопроводов предназначена для автоматизации управления и оперативного контроля технологического процесса, включая сбор данных о технологических параметрах процесса: расход, уровень, температура, давление, плотность и влажность перекачиваемой нефти.

Подсистемы АСУ ТП ПСП согласно терминологии ГОСТ 62443 можно рассматривать как отдельные зоны безопасности, объединяемые по общим показателям риска, функциональным и/или техническим характеристикам, логическим или физическим границам, сетям передачи данных и т. д. На рисунке. 3.13 представлено зонирование по принципу единства выполняемых функций и требований к безопасности их реализации:

- Зона 1 – зона сервера СДКУ (система диспетчерского контроля и управления) SCADA;
- Зона 2 – зона критических устройств управления;
- Зона 3 – зона управления задвижками;
- Зона 4 – зона управления ТП ПСП;
- Зона 5 – зона управления системой измерения количества нефти (СИКН);
- Зона 6 – зона датчиков.

Выполним оценку актуальных угроз для Зоны 5 с помощью Методики [2].

В Зоне 5 с датчиков СИКН, установленных на двух трубопроводах, данные поступают на два контроллера Emerson Floboss S600+. С двух других датчиков, установленных на третьем и четвертом трубопроводе СИКН, данные поступают на контроллеры Allen Bradley 5561. Два АРМ (основной и резервный) хранят и отображают на мнемосхеме состояние и показатели четырех СИКН в составе

ПСП. Дополнительно в операторной установлен АРМ с данными по СИКН для принимающей стороны.

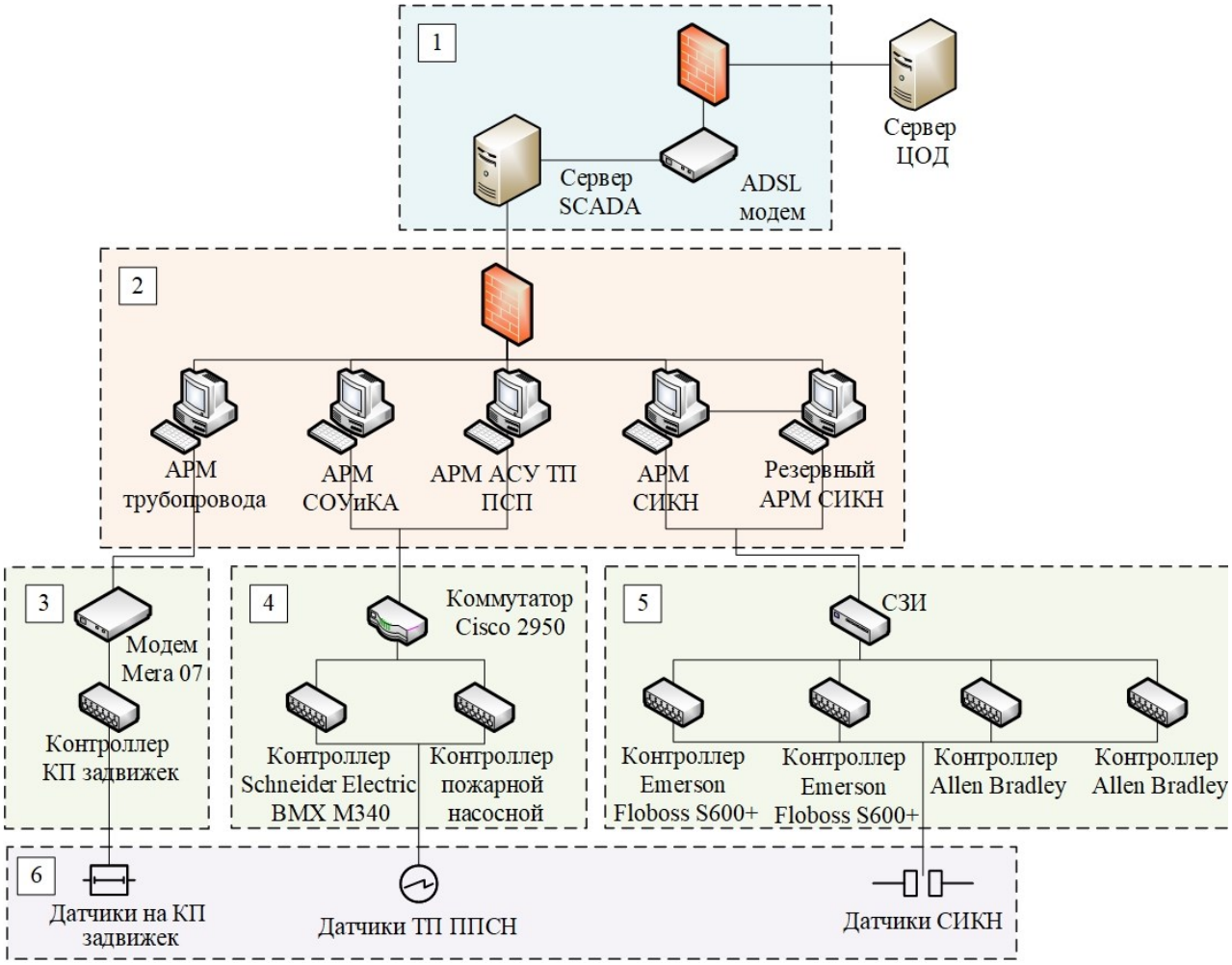


Рисунок 3.13 – Зональная модель объекта защиты

Промежуточные результаты этапов анализа согласно функциональной модели применения Методики представлены в таблице 3.13.

Таблица 3.13 – Промежуточные результаты реализации Методики

Этап	Определяемые параметры	Значения параметров
Определение негативных последствий	Виды рисков (ущерба) и типовые негативные последствия от реализации угроз безопасности информации	– нарушение штатного режима функционирования АСУ ТП (У2) – неспособность выполнять договорные обязательства (У2)
Определение объектов воздействия	Объекты воздействия	Программируемый логический контроллер (ПЛК) для управления насосными станциями
	Виды воздействия	Несанкционированная модификация (изменение) логики работы или уставок ПЛК, которая приводит к включению (или не отключению) насосной станции

Этап		Определяемые параметры	Значения параметров
			при закрытой аварийной задвижке в нефтепроводе (У3)
Оценка возможности реализации угроз и их актуальности	Определение цели реализации угроз безопасности информации нарушителями	Виды нарушителя	Авторизованные пользователи систем и сетей
		Категории нарушителя	Внутренний
		Возможные цели реализации угроз безопасности информации	Любопытство или желание самореализации Непреднамеренные, неосторожные или неквалифицированные действия
	Определение уровня возможностей нарушителей по реализации угроз безопасности информации	Уровень возможностей нарушителей	Нарушитель, обладающий базовыми возможностями
		Возможности нарушителей по реализации угроз безопасности информации	нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов
	Определения актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности	Доступные интерфейсы	Локальная вычислительная сеть Веб-интерфейс системы

Для детального моделирования сценариев эксплуатации уязвимостей и определения актуальных угроз воспользуемся предложенной методикой построения семантической модели текстовых описаний угроз и уязвимостей объектов АСУ ТП ПСП (рисунок 3.13), последовательно реализуем описанные ранее шаги предложенной методики:

Шаг 1. Семантический анализ агрегированного списка рассылок и бюллетеней. Поисковый запрос для $БД_1$ включает описание основных узлов Зоны 5 («промышленная сеть», «промышленный коммутатор», «программируемый логический контроллер»). Процедура предобработки и подготовки текстовых данных извлеченных из CVE, CPE и CWE, представлена в виде конвейера NLP-pipe.

Шаг 2-4. Формируется список выявленных сканерами безопасности уязвимостей для каждого компонента Зоны 5 в виде перечня CVE-ID и BDU-ID, выполняется его фильтрация и обобщение до текстовых описаний CWE.

Шаг 5. Список меташаблонов CAPEC, построенный на основе: списка CWE-ID, списка техник и тактик ATT&CK в виде графа приведен на рисунок 3.14.

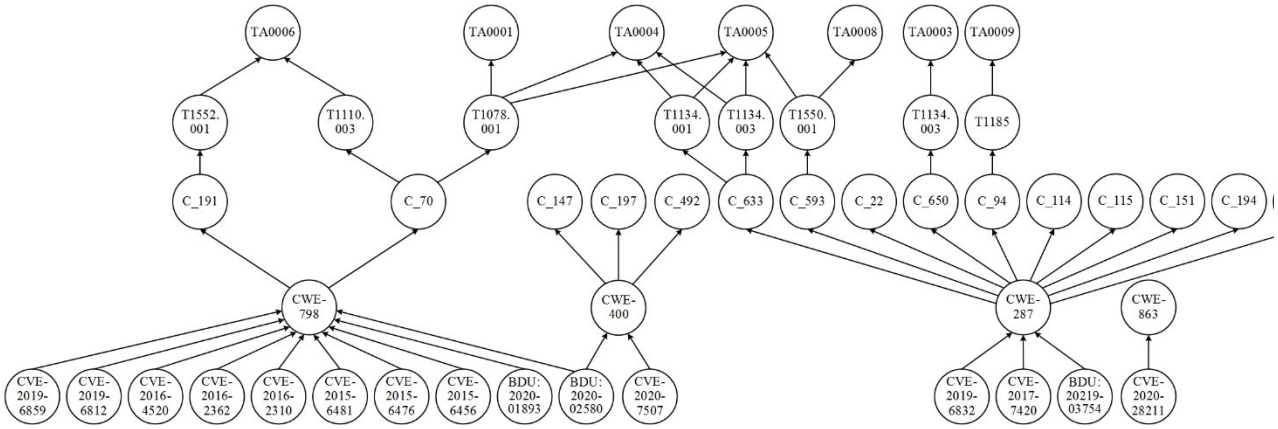


Рисунок 3.14 – Фрагмент графа с привязкой CVE-CWE-CAPEC-ATT&CK

Шаг 6-7. Формализация графовой модели в БД$_2$ Neo4j с расстановкой весовых коэффициентов на основе оценки меры семантической близости текстовых описаний с поддержкой реализации запросов на языке GraphQL (таблица 3.14).

Таблица 3.14 – Матрица связности узлов графовой модели CVE-CWE-CAPEC-ATT&CK по результатам анализа ссылочной модели и семантической близости текстовых описаний угроз и уязвимостей объектов

CWE ID	Название	CVE из NVD	CVE из BDU	CAPEC	ATT&CK Technic	ATT&CK Tactics
CWE-798	Use of Hard-coded Credentials (Использование жестко заданных учетных данных)	CVE-2019-6859, CVE-2019-6812, CVE-2016-4520, CVE-2016-2362, CVE-2016-2310, CVE-2015-6481, CVE-2015-6476, CVE-2015-6456.	BDU:2020-01893, BDU:2020-02580	CAPEC-191: Read Sensitive Constants Within an Executable	T 1552.001 Unsecured Credentials:Credentials in files	TA0006 Credential Access (Учетный доступ)
				CAPEC-70: Try Common or Default Usernames and Passwords	T 1078.001 Valid Accounts: Default Accounts (Действительные учетные записи: учетные записи по умолчанию)	TA0005 Defense Evasion, Persistence (Уклонение от защиты, настойчивость); TA0004 Privilege Escalation (Повышение привилегий); TA0001 Initial Access (Первоначальный доступ)
					T 1110.003 Brute Force: Password Spraying (Грубая сила: Распыление паролей)	TA0006 Credential Access (Учетный доступ)
CWE-287	Improper Authentication (Неправильная	CVE-2019-6832, CVE-2017-7420.	BDU:2019-03754	CAPEC-114, CAPEC-115, CAPEC-22,		

CWE ID	Название	CVE из NVD	CVE из BDU	CAPEC	ATT&CK Technic	ATT&CK Tactics
	аутентификация)			CAPEC-194, CAPEC-151		
				CAPEC-94	T1185 Man in the Browser (Человек в браузере)	TA0009 Collection (Сбор)
				CAPEC-593	T1550.001 Use Alternate Authentication Material:Application Access Token (Используйте альтернативный материал для аутентификации: токен доступа к приложению)	TA0005 Defense Evasion (Уклонение от защиты); TA0008 Lateral Movement (Боковое движение)
				CAPEC-633	T1134.001 Access Token Manipulation: Token Impersonation/ Theft (Манипулирование токеном доступа: выдача себя за другое лицо / кража токена)	TA0005 Defense Evasion (Уклонение от защиты); TA0004 Privilege Escalation (Повышение привилегий)
					T1134.003 Access Token Manipulation: Make and Impersonate Token (Манипуляции с токенами доступа: создание и выдача токена)	TA0005 Defense Evasion (Уклонение от защиты); TA0004 Privilege Escalation (Повышение привилегий)
				CAPEC-650	T1505.003 Server Software Component: Web Shell (Компонент серверного программного обеспечения: веб-оболочка)	TA0003 Persistence (Настойчивость)
				CAPEC-57		
CWE -863	Incorrect Authorization (Неправильная авторизация)	CVE-2020-28211				
CWE -400	Uncontrolled Resource Consumption (Неконтролируемое потребление ресурсов)	CVE-2020-7507	BDU:2020-02580	CAPEC-492, CAPEC-197, CAPEC-147		

Шаг 8-9. С учетом построенной графовой модели сценариев реализации угроз (тактический уровень моделирования угроз – таблица 3.13) и результатов анализа согласно Методике (стратегический уровень моделирования угроз – таблица 3.14), строятся актуальные способы эксплуатации уязвимостей и реализации угроз для элементов Зоны 5 АСУ ТП ПСП в виде НСКК. Итоговая цепочка действий нарушителя в виде укрупненной графовой модели (рисунок 3.15)

отражает возможные сценарии эксплуатации уязвимостей для реализации угроз безопасности информации в Зоне 5 АСУ ТП ПСП и позволяет получить оценку риска ИБ целевых концептов промышленной системы. Концепты для моделирования НСКК приведены в таблице 3.15. Для оценки риска ИБ используются определенные экспертами значения весов связей между концептами из таблицы 3.16.

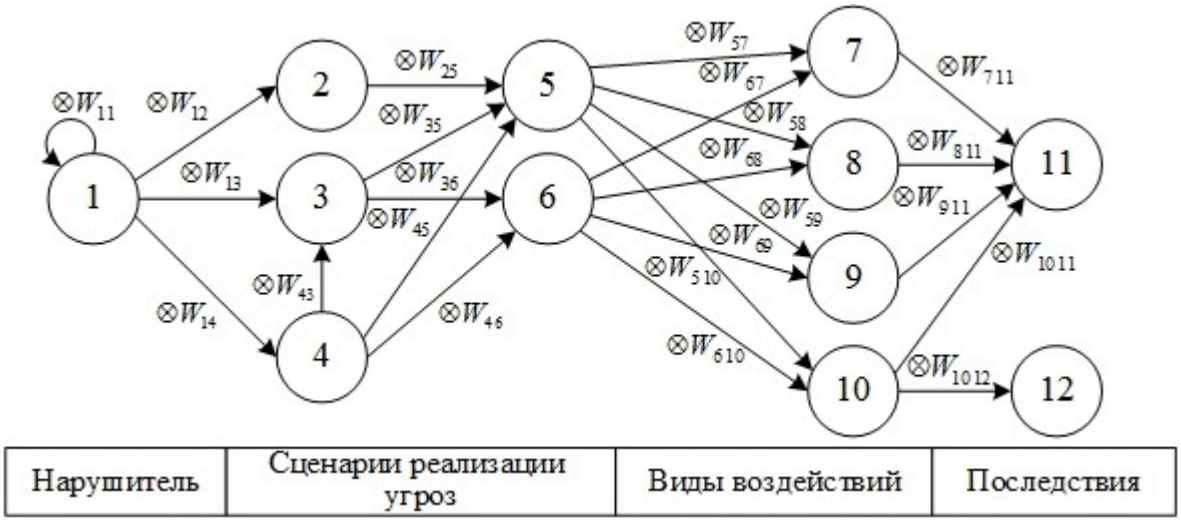


Рисунок 3.15 – Укрупненная графовая модель сценариев реализации угроз безопасности информации в Зоне 5 в виде НСКК

Таблица 3.15 – Концепты НСКК для моделирования актуальных способов реализации угроз

Концепт графовой модели	Характеристика	Группа концептов
C_1	Внутренний нарушитель с базовым потенциалом	
C_2	Подмена ответа сервера FTP резервного копирования конфигураций ПЛК (УБИ.034)	Реализация атак через эксплуатацию недостатков сетевых протоколов
C_3	Перехват учетной записи привилегированного пользователя на ПЛК (УБИ.034)	
C_4	Учетная запись с параметрами по умолчанию на ПЛК (УБИ0.30)	Реализация атак через эксплуатацию недостатков конфигурации или ПО ПЛК
C_5	Модификация прошивки ПЛК (УБИ.188)	Реализация атак через воздействие на управляющую программу ПЛК
C_6	Перезапись проекта ПЛК в режиме online (УБИ.179)	
C_7	Отказ в обслуживании оборудования	Виды воздействия
C_8	Потеря возможности мониторинга параметров СИКН	
C_9	Перевод СИКН и управляемых объектов в аварийное состояние	
C_{10}	Останов нефтетранспорта по магистральному нефтепроводу	

Концепт графовой модели	Характеристика	Группа концептов
C_{11}	Нарушение штатного режима функционирования АСУ ТП ПСП	Последствия
C_{12}	Неспособность компании выполнить договорные обязательства	

Таблица 3.16 – Веса связей НСКК оценки рисков ИБ реализации угроз безопасности информации для целевых концептов ИС

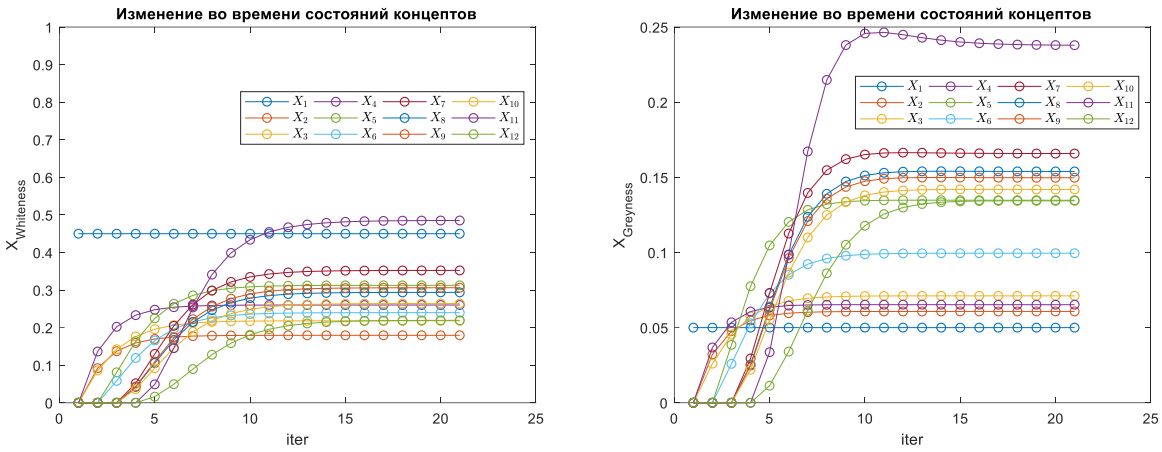
Вес связи	Диапазон	Вес связи	Диапазон
W_{11}	[0,4; 0,45]	W_{58}	[0,6; 0,85]
W_{12}	[0,3; 0,5]	W_{59}	[0,5; 0,65]
W_{13}	[0,3; 0,45]	$W_{5\,10}$	[0,3; 0,45]
W_{14}	[0,5; 0,7]	W_{67}	[0,6; 0,8]
W_{25}	[0,5; 0,7]	W_{68}	[0,25; 0,4]
W_{26}	[0,25; 0,4]	W_{69}	[0,5; 0,7]
W_{35}	[0,5; 0,75]	$W_{6\,10}$	[0,5; 0,75]
W_{36}	[0,5; 0,6]	$W_{7\,11}$	[0,35; 0,55]
W_{43}	[0,15; 0,25]	$W_{8\,11}$	[0,25; 0,45]
W_{45}	[0,25; 0,4]	$W_{9\,11}$	[0,5; 0,6]
W_{46}	[0,2; 0,3]	$W_{10\,11}$	[0,65; 0,85]
W_{57}	[0,6; 0,8]	$W_{10\,12}$	[0,7; 0,85]

Концепт C_1 выступает в качестве концепта-драйвера и представляет собой внутреннего нарушителя с базовым потенциалом при реализации угрозы, связанной с модификацией конфигураций ПЛК с целью нарушения технологического процесса, создания аварийной ситуации на промышленном объекте или состояния аварийной остановки.

Процесс изменения состояний концептов НСКК во времени показан на рис. 3.16, где по оси ординат расположены значения переменных состояния НСКК, а по оси абсцисс – итерации сходимости НСКК.

На графиках приведены центральные значения «серых» переменных состояния концептов (рисунок 3.16, а) и значения «серости» этих концептов (рисунок. 3.16, б). Из графиков видно, что состояния концептов стабилизировались за 8-10 итераций. Значения концептов НСКК, соответствующие оценкам рисков ИБ, связанных с нарушением штатного режима функционирования АСУ ТП ПСП, составило [0,2473; 0,7231], неспособности компании выполнить договорные обязательства – [0,0851; 0,3538]. Усредненные значения рисков ИБ в

рассматриваемых сценариях реализации угроз составили $X_{11}^{*}=0,4852$ и $X_{12}^{*}=0,2195$ соответственно.



а) б)

Рисунок 3.16 – Изменение во времени состояний концептов НСКК: (а) стабилизация «белого» значения концепта (б) стабилизация «серости» концепта

Отличительной особенностью является использование и ссылочной модели, и оценки семантической близости текстовых описаний из отечественных и зарубежных баз данных. Это позволяет снизить трудоемкость формирования перечня актуальных угроз и уязвимостей за счет применения технологий Text Mining для префильтрации несвязанных или недостижимых вершин при выполнении основных этапов анализа согласно Методике ФСТЭК России. Завершающий этап предлагаемой методики позволяет перейти к построению когнитивной модели оценки рисков ИБ для целевых объектов АСУ ТП, что позволяет получить детализированную оценку рисков ИБ и сделать более обоснованный выбор средств защиты информации за счет возможности моделирования различных сценариев реализации угрозы. Исходными данными для построения когнитивных карт являются не только экспертные оценки, но и формализованные и систематизированные данные из открытых баз данных угроз и уязвимостей, что существенно повышает обоснованность и полноту моделирования.

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

3.5 Пример оценки актуальных угроз и уязвимостей ПО АСУ ТП

В качестве объекта рассмотрим АСУ ТП транспорта товарной нефти (ТТН), интегрированную в комплексную систему оперативного контроля и управления в реальном масштабе времени, позволяющую передавать накапливаемые технологические данные о состоянии объекта в системы управления производственными процессами вышележащих уровней. Выделенный фрагмент [29] базовой архитектуры АСУ ТП ТТН на рисунке 3.17 включает в себя основные элементы АСУ ТП нефтеперекачивающих станций, телекоммуникационное оборудование и линии связи.

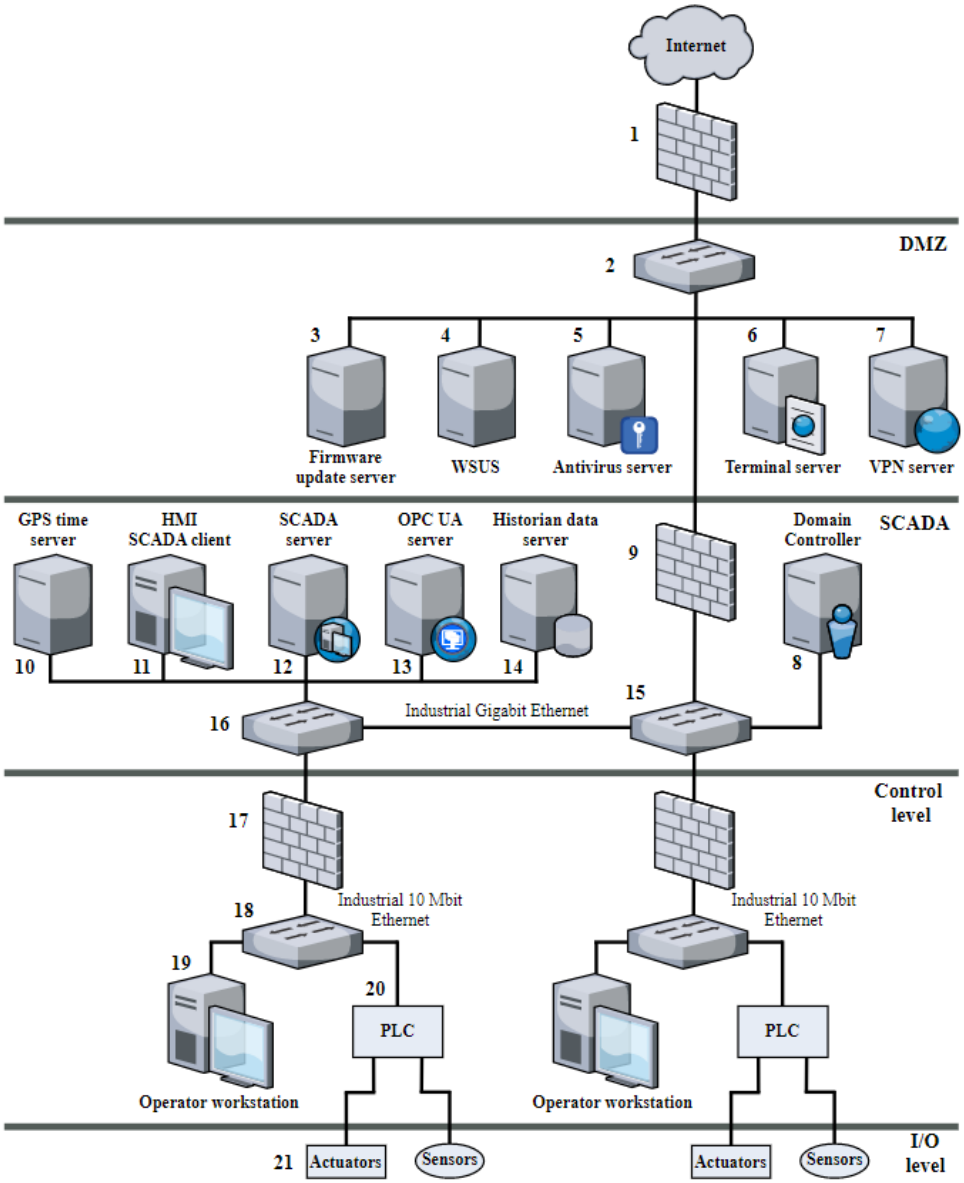


Рисунок 3.17 – Базовая архитектура АСУ ТП ТТН

Исходными данными являются результаты работы сканеров уязвимостей и базы данных угроз и уязвимостей, а также потенциальных слабостей программного и аппаратного обеспечения. Рассмотрим перечень уязвимостей (таблица 3.17) для целевых узлов – объектов воздействия злоумышленника – терминального сервера (6), сервера VPN (7) и программируемого логического контроллера (20). Столбец «Объект воздействия» содержит название и номер группы из перечня выделенных из описаний угроз. Оценка косинус-меры сходства приведена в порядке убывания значений для близких по описанию угроз.

Таблица 3.17 – Уязвимости компонентов (6, 7, 20) АСУ ТП ТТН

№	Уязвимость	Компонент системы	Объект воздействия	Семантически близкие угрозы	Оценка косинус-меры сходства
1	BDU:2019-04216: Уязвимость программного обеспечения OpenVPN, позволяющая нарушителю восстановить исходное сообщение	сервер VPN (7)	Сетевое оборудование (20) Сервер (19) системное и прикладное программное обеспечение (17)	Угроза некорректного использования функционала программного и аппаратного обеспечения (УБИ.063)	0,259
				Угроза использования уязвимых версий программного обеспечения (УБИ.192)	0,194
2	BDU:2020-04710: Уязвимость службы Remote Desktop Services, позволяющая нарушителю получить несанкционированный доступ к защищаемой информации	терминальный сервер (6)	Сетевое оборудование (20) Сервер (19) системное и прикладное программное обеспечение (17)	Угроза несанкционированного доступа к аутентификационной информации (УБИ.074)	0,274
3	BDU:2020-05232: Уязвимость службы удаленного рабочего стола, позволяющая нарушителю повысить свои привилегии				
4	BDU:2020-04773: Уязвимость службы Remote Desktop Services, позволяющая нарушителю вызвать отказ в обслуживании				
8	BDU:2019-02045: Уязвимость микропрограммного обеспечения ПЛК Modicon, связанная с нарушением доверительных границ, позволяющая нарушителю осуществить	ПЛК (20)	Микропрограммное обеспечение (8) Аппаратное обеспечение (1)	Модификация прошивки ПЛК (УБИ.188)	0,678

№	Уязвимость	Компонент системы	Объект воздействия	Семантически близкие угрозы	Оценка косинусмеры сходства
	несанкционированный доступ путем проведения атаки «грубой силы» по протоколу Modbus		Программное обеспечение автоматизированной системы управления технологическими процессами (17)		
9	BDU:2019-02042: Уязвимость микропрограммного обеспечения ПЛК Modicon, связанная с обходом аутентификации посредством спуфинга, позволяющая нарушителю повысить привилегии			Угроза использования информации идентификации /аутентификации, заданной по умолчанию (УБИ.030)	0,674
10	BDU:2019-02046: Уязвимость микропрограммного обеспечения ПЛК Modicon, связанная с ошибками контроля доступа, позволяющая нарушителю вызвать отказ в обслуживании или выполнить произвольный код			Угроза несанкционированного управления указателями (УБИ.095)	0,452
				Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров (УБИ.204)	0,395
				Угроза перебора всех настроек и параметров приложения (УБИ.109)	0,393

Анализ таблицы 3.17 показывает, что объемы просматриваемых экспертом данных при оценке опасности выявленных уязвимостей и релевантных им угроз нарушения ИБ с помощью префильтрации на основе технологий Text Mining удается сократить в 7-10 раз, тем самым повысив эффективность работы специалиста.

Таким, образом, предложена архитектура системы анализа уязвимостей ПО и угроз нарушения информационной безопасности с использованием технологии Text Mining, основанная на алгоритмах векторного представления слов и документов и оценки семантической близости текстовых описаний уязвимостей, выявленных с помощью сканеров безопасности, и описаний релевантных угроз из Банка данных угроз безопасности информации ФСТЭК России. В качестве связующего звена предложено использовать текстовое описание объектов воздействия злоумышленника.

Рассмотрен пример применения предложенного подхода для оценки уязвимостей прикладного ПО подсистемы АСУ ТП промышленного объекта нефтедобычи с последующим формирование списка релевантных угроз.

Применение предложенного подхода позволяет автоматизировать процесс сопоставления и ранжирования угроз ИБ для каждой выявленной уязвимости и в несколько раз сократить время ручного анализа экспертом результатов работы сканеров за счет интеллектуальной фильтрации и ранжирования списка угроз и объектов воздействия.

3.6 Выводы по главе

Предложен метод и алгоритм семантического анализа текстовых описаний угроз и уязвимостей, отличаются подходом к формализации слабоструктурированных текстовых описаний угроз и уязвимостей с помощью гетерогенных нейросетевых моделей вложений, что позволяет обеспечить выявления потенциальных угроз и уязвимостей с возможностью их приоритезации, а также автоматизировать основные этапы процедуры оценки рисков.

Предложена структура системы анализа критичных уязвимостей ПО с использованием технологии Text Mining, основанная на алгоритмах векторного представления слов и оценки семантической близости текстовых описаний уязвимостей, выявленных с помощью сканеров безопасности, и описаний релевантных угроз из БДУ ФСТЭК России. Программная реализация клиент-серверного прототипа данной системы и интеграция с модулями существующих решений позволяют:

– автоматизировать процесс сопоставления и ранжирования угроз ИБ для каждой выявленной уязвимости на рабочих станциях и серверах в составе корпоративной информационной системы;

– сократить время ручного анализа экспертом результатов работы сканеров за счет интеллектуальной фильтрации и ранжирования списка угроз;

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

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

Предложен подход к **оценке степени опасности уязвимостей** на основе прогнозирования метрики с помощью анализа текстового описания угроз и уязвимостей на основе применения технологий интеллектуального анализа описаний уязвимостей на естественном языке. Отличительной особенностью является использование построение модели вложения слов и описаний уязвимостей и композиции классификаторов, выполняющих оценку компонент вектора метрики уязвимости согласно стандарту CVSS. Применение предлагаемого подхода позволит получить оценку метрики опасности (и ее компонент) зарегистрированной уязвимости на основе анализа семантической близости текстового описания к уже имеющимся в реестре записям. Ансамбль нейросетевых моделей и регрессора на основе комитета случайных деревьев позволяет получить оценку компонент метрики опасности уязвимости CVSS на уровне $F_1 = 0.80\text{-}0.85$.

Практическая значимость обусловлена повышением эффективности (точности и оперативности) оценки метрик опасности уязвимостей с возможностью интеграции в систему аудита и инвентаризации для оперативного принятия мер по защите от новых уязвимостей.

Предложена методика оценки актуальных угроз и уязвимостей программного обеспечения объекта КИИ с использованием методов семантического анализа текстовых описаний угроз и уязвимостей. Отличительной особенностью является использование и ссылочной модели, и оценки семантической близости текстовых описаний из отечественных и зарубежных баз данных. Это позволяет снизить трудоемкость формирования перечня актуальных угроз и уязвимостей за счет применения технологий Text Mining для префильтрации несвязанных или недостижимых вершин при выполнении основных этапов анализа согласно Методике ФСТЭК России.

Глава 4. Разработка метода и алгоритмов комплексной оценки рисков ИБ объектов КИИ с использованием методов нечеткого когнитивного моделирования и машинного обучения

4.1 Общая схема построения нечеткой когнитивной модели оценки рисков ИБ объекта КИИ

Детальный пример анализа последствий от реализации вирусной атаки на некоторый информационный ресурс, располагаемый на рабочей станции (АРМ оператора) приведен в Приложении В. Анализ результатов, приведенных Приложении В, позволяет сделать выводы [27, 28, 30, 34, 40-43, 92, 126, 171, 180]:

1) использование НКК дает некоторую сравнительную базу для выбора вариантов построения системы защиты информации, исходя из приемлемого уровня обеспечения рисков ИБ. Так, вариант а-4 оказывается предпочтительнее вариантов а-1 ÷ а-3, поскольку он предлагает уделить одинаково серьезное внимание всем 3-м компонентам риска (парирование угрозы – ликвидация уязвимости – устранение последствий от реализации угрозы), что соответствует так называемому «принципу равнопрочности» защиты;

2) возможное разбиение полученных решений по уровням риска (например, $0,55 < R \le 0,65$ – высокий уровень; $0,45 < R \le 0,55$ – средний уровень; $0,35 < R \le 0,45$ – низкий уровень риска) является в значительной степени условным; столь малый разрыв между верхней и нижней границей риска объясняется, прежде всего, сжимающим характером сигмоидной функции (6), причем эффект сжатия проявляется тем сильнее, чем больше концептов располагается на пути от источника до целевого фактора;

3) приоритет в пользу выбора решений, соответствующих схеме НКК на рисунок В.2, а по сравнению со схемой НКК на рисунок В.2, б, обусловлен главным образом большим объемом ресурсов, выделенных на реализацию контрмер в 1-ом случае (переменная $X_4^* = 1$), в то время как во 2-ом случае максимальное значение объема ресурсов достигает лишь величины $X_4^* = 0,59$ для варианта б-4;

4) несмотря на то, что сигмоидная функция (6) представляет собой оператор сжатия, что гарантирует (в силу Утверждения 2) существование и устойчивость равновесного состояния НКК, условие (8) является достаточно жестким требованием по отношению к значениям весов НКК, что может послужить

серьезным ограничением при построении НКК большой размерности, содержащих большое число концептов и связей.

Реальные ситуации, возникающие на практике, требуют построения и исследования более сложных по своему составу НКК, включающих достаточно большое число концептов и связей. На рисунке 4.1 приведён пример такой НКК, характеризующей влияние некоторой совокупности угроз на возникновение рисков, связанных с нарушением конфиденциальности и целостности информации.

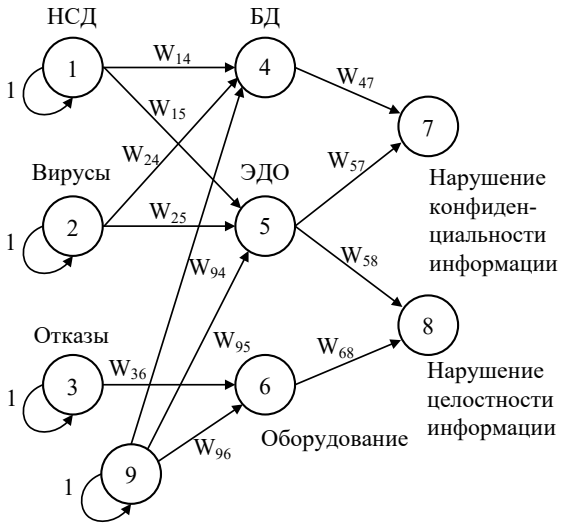


Рисунок 4.1 – НКК, характеризующая влияние совокупности угроз на возникновение рисков, связанных с нарушением конфиденциальности и целостности информации

Здесь: C_1, C_2 и C_3 – угрозы, связанные соответственно с попытками несанкционированного доступа (НСД) к информации, вирусной атакой и отказами оборудования; C_4, C_5 и C_6 – уязвимости, вызванные отсутствием надлежащей защиты базы данных (БД), электронного документооборота (ЭДО) и оборудования; C_7 и C_8 – ущерб (потери) от нарушения конфиденциальности и целостности информации; C_1 – контрмеры по защите информации. Пользуясь изложенной выше методикой, можно не только оценить возможные риски от воздействия угроз, но и выбрать правильную (рациональную) стратегию защиты информации.

Целью было показать те возможности и преимущества, которые предоставляет технология когнитивного моделирования для решения задачи оценки рисков ИБ. Особенностью применения данной технологии является акцент на выявление наиболее существенных факторов, оказывающих влияние на постановку задачи и получение необходимого результата, оценка существующих между ними причинно-следственных связей, возможность сравнительного анализа

различных вариантов принятия решений. Полученные при этом качественные модели в виде НКК особенно полезны на этапе предварительной оценки рисков информационной безопасности, при отсутствии достоверной статистики об имеющихся и потенциальных возможных инцидентов ИБ.

4.2 Оценка рисков ИБ объекта КИИ с помощью нечетких продукционных когнитивных карт

Под *нечеткой продукционной когнитивной картой* понимается ориентированный граф (орграф), задаваемый парой множеств:

$K = \{C, F\},$	(4.1)

где $C = \{C_i\}$, (i = 1, 2, …, n) – множество узлов (вершин) орграфа, называемых *концептами*; $F = \{F_{ij}\}$, (i, j = 1,2, …, n) – множество дуг – связей (отношений) между концептами; n – число концептов НПКК. Предполагается, что переменная состояния X_i каждого концепта C_i рассматривается как лингвистическая переменная, принимающая значения из некоторого 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 $X_i \in [-1,1]$. Различают два вида концептов: *уровни* (levels), которые представляют абсолютные значения состояния концепта в данный момент времени, и *вариации* (variations), которые представляют изменения состояния концепта по отношению к предыдущему моменту времени. Последнее важно для описания динамики поведения исследуемых систем. Для определения взаимного влияния концептов ($C_i \to C_j$) используются нечеткие продукционные правила, позволяющие представить предпосылки (условия) и заключения нечетких правил на основе нечетких множеств.

На рисунке 4.2 приведен пример задания нечетких правил для определения влияния концепта C_i на концепт C_j.

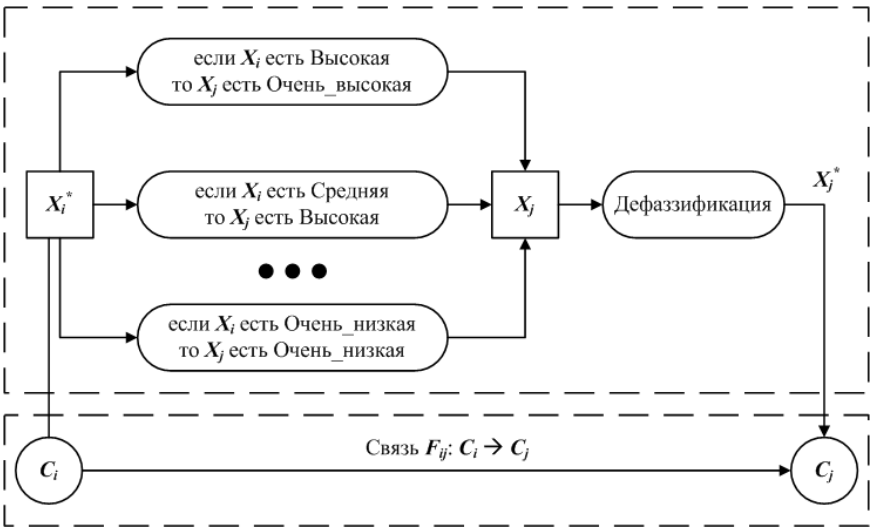


Рисунок 4.2 – Пример влияния концепта C_i на концепт C_j в НПКК

Предполагается, что переменные X_i и X_j, характеризующие состояния концептов C_i и C_j, могут принимать значения из терм-множества {Очень_высокая (*VH*), Высокая (*H*), Средняя (*M*), Низкая (*L*), Очень_низкая (*VL*)}, задаваемые с помощью соответствующих функций принадлежности. Для реализации процедуры нечеткого логического вывода (применительно к конкретному «четкому» значению входной переменной X_i^* и получению «четкого» значения переменной X_j^* на выходе) можно воспользоваться алгоритмом Мамдани [236]. Особенность реализации вычислительного процесса в данном случае состоит в выполнении последовательных преобразований (четкое значение X_i^* → фаззификация → нечеткий логический вывод → получение нечеткого множества для X_j → дефаззификация, вычисление четкого значения X_j^*) и т.д. для каждой последующей пары концептов $C_j \rightarrow C_{j+1} \rightarrow \cdots$ на пути следования в НПКК. На этапе дефаззификации (приведения к четкости) выходной переменной X_j используется метод взвешенного среднего:

$$X_j^* = \frac{\sum_{l=1}^{m} \alpha_l X_{jl}^o}{\sum_{l=1}^{m} \alpha_l} \qquad (4.2)$$

где X_j^* – дефаззифицированное значение переменной состояния концепта C_j; $X_{jl}^0, (l = 1,2,\dots,m)$ – центральные значения нечетких подмножеств (термов) переменной X_j; α_l – уровень активности l-го правила, соответствующий конкретному значению входной переменной X_i^*; m – число термов (подмножеств) лингвистической переменной X_j (в примере m = 5).

В общем случае, если на концепт C_j оказывают непосредственное влияние k предшествующих концептов $C_i, C_{i+1}, \dots, C_{i+k-1}$, то нечеткие продукционные правила принимают более сложный вид, например:

П$_1$: если X_i есть Высокая и X_{i+1} есть Высокая и … и X_{i+k-1} есть Высокая, то X_j есть Очень_высокая;

…

П$_N$: если X_i есть Очень_низкая и X_{i+1} есть Очень_низкая и … и X_{i+k-1} есть Очень_низкая, то X_j есть Очень_низкая;

Процедура нечеткого логического вывода здесь реализуется аналогично. Для выполнения операции логического «и» можно воспользоваться оператором MIN.

Основной недостаток НПКК – резкое возрастание числа продукционных правил при возрастании числа концептов. Так, в предыдущем примере для определения состояния одного концепта C_j (переменной X_j) при двух предшествующих взаимодействующих с ним концептах C_i, C_{i+1}, описываемых соответственно переменными состояния X_i и X_{i+1}, имеем: $k = 2, m = 5$, а общее число указанных выше правил равно $m^2 = 25$. Конечно, не все эти правила будут активными (т.е., $\alpha_l \neq 0$) для конкретных «четких» значений входов X_i^* и X_{i+1}^*, поступающих с выходов концептов C_i и C_{i+1}. Более того, всегда активизируются лишь четыре правила, остальные правила не срабатывают. Тем не менее, проблема высокой размерности базы правил НПКК остается, и, вообще говоря, для ее решения должны применяться специальные методы и способы [98].

4.2.1 Пример применения методики оценки рисков информационной безопасности с помощью НПКК

Допустим, что требуется оценить риск ИБ от возможного воздействия вирусной атаки на некоторый информационный ресурс, размещаемый на сервере, рассматривая в качестве уязвимости отсутствие обновлений антивирусного ПО.

Согласно трехфакторной формуле риска, представим соответствующую ей схему расчета в виде НПКК на рисунке 4.3. Здесь: C_1 – угроза, C_2 – уязвимость, C_3 – информационный ресурс, C_4 – реализация угрозы, C_5 – риск (потенциальный ущерб). Соответственно: X_1 – вероятность возникновения угрозы; X_2 – вероятность наличия уязвимости; X_3 – ценность (стоимость) информационного

ресурса; X_4 – вероятность успешной реализации угрозы; $X_5 = R$– уровень риска (величина ожидаемого потенциального ущерба).

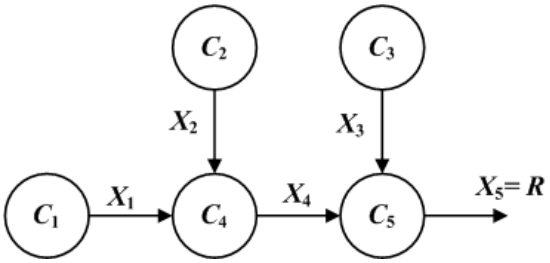


Рисунок 4.3 – Схема НПКК для оценки риска

Используя аппарат нечеткой логики, будем полагать, что каждая из указанных переменных состояния представляет собой лингвистическую переменную, принимающую одно из следующих значений: *L* – Low («Низкая (-ий)»); *M* – Medium («Средняя(-ий)»); *MH* – Medium High («Достаточно высокая (-ий)»); *H* – High («Высокая (-ий)»); *VH* – Very High («Очень высокая (-ий)»). Каждое из этих нечетких подмножеств задается, в свою очередь, собственной функцией принадлежности (рисунке 4.4).

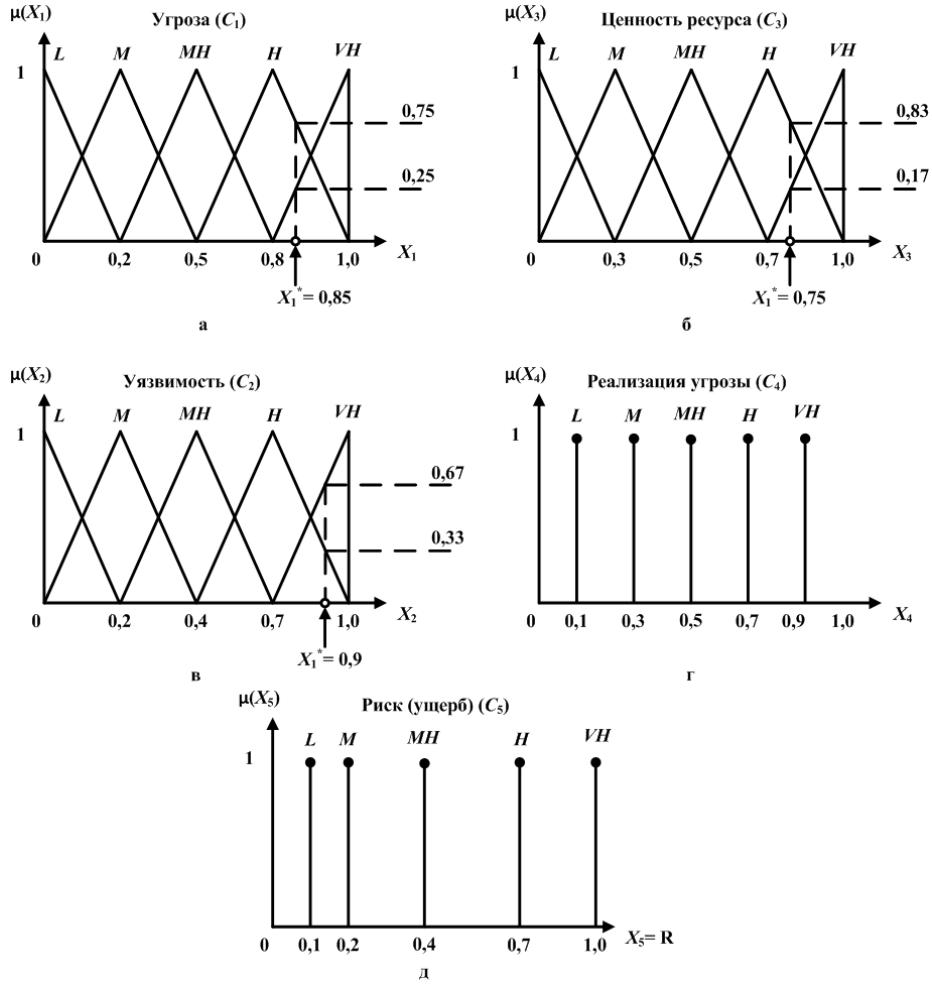


Рисунок 4.4 – Функции принадлежности нечетких множеств

Здесь функции принадлежности нечетких подмножеств НПКК $\mu(X_1), \mu(X_2), \mu(X_3)$ имеют треугольную форму, а функции принадлежности $\mu(X_4), \mu(X_5)$ являются столбчатыми (singletons).

Систему нечетких продукционных правил, описывающих состояние концептов C_4 и C_5, можно записать в виде:

Концепт C_4:

П$_1$: Если X_1 есть Низкая и X_2 есть Низкая, то X_4 есть Низкая;

…

П$_{25}$: Если X_1 есть Очень_высокая и X_2есть Очень_высокая, то X_4 есть Очень_высокая;

Концепт C_5:

П$_{26}$: Если X_3 есть Низкая и X_4 есть Низкая, то X_5 есть Низкая;

…

П$_{50}$: Если X_3 есть Очень_высокая и X_4 есть Очень_высокая, то X_5 есть Очень_высокая.

Всего имеем: 2 * 5 * 5 = 50 правил, которые удобно представить в виде так называемых матриц риска (или таблиц решений) [279]:

Табл. 1. Реализация угрозы C_4

X_1 \ X_2	L	M	MH	H	VH
VH	MH	H	H	H	VH
H	M	MH	H	H	H
MH	M	M	MH	MH	H
M	L	M	M	M	MH
L	L	L	L	M	M

Табл. 2. Риск (ущерб) C_5

X_3 \ X_4	L	M	MH	H	VH
VH	M	M	MH	H	VH
H	L	M	MH	H	H
MH	L	M	M	MH	MH
M	L	L	M	M	M
L	L	L	L	L	L

Рисунок 4.5 – Реализация угрозы и оценка риска

В клетках первой таблицы рисунка 4.5 записаны соответствующие значения (термы) переменной X_4, в клетках второй таблицы – значения (термы) переменной $X_5 = R$, т.е. уровня риска.

Допустим, что в конкретном рассматриваемом случае входные переменные НПКК (т.е. три базовых фактора риска) принимают значения: $X_1^* = 0{,}85$,

$X_2^* = 0{,}9$ $X_3^* = 0{,}75$. Обратившись к рисунку 4.5 и приведенным выше таблицам, видим, что переменные X_1, X_2, X_3, X_4 принимают только значения МН и Н, т.е. из 50 правил активными окажутся только 8 правил, соответствующих выделенным блокам из четырех соседних клеток в правом верхнем углу первой и второй таблиц. Таким образом, редуцированная система нечетких продукционных правил принимает вид:

1) если $X_1 = H$ и $X_2 = H$, то $X_4 = H$;
2) если $X_1 = H$ и $X_2 = VH$, то $X_4 = H$;
3) если $X_1 = VH$ и $X_2 = H$, то $X_4 = H$;
4) если $X_1 = VH$ и $X_2 = VH$, то $X_4 = VH$;

} концепт C_4

5) если $X_3 = H$ и $X_4 = H$, то $X_5 = H$;
6) если $X_3 = H$ и $X_4 = VH$, то $X_5 = H$;
7) если $X_3 = VH$ и $X_4 = H$, то $X_5 = H$;
8) если $X_3 = VH$ и $X_4 = VH$, то $X_5 = VH$.

} концепт C_5

Используя операции нечеткой логики [279] для заданных «четких» значений переменных X_1^*, X_2^*, X_3^*, получим значения уровней активностей данных правил:

$\alpha_1 = 0{,}33;\ \alpha_2 = 0{,}67;\ \alpha_3 = \alpha_4 = 0{,}25;\ \alpha_5 = 0{,}33;\ \alpha_6 = 0{,}67;$ $\alpha_7 = \alpha_8 = 0{,}17.$	(4.3)

Объединяя правила 1-4 и 5-8 с помощью логической связки ИЛИ (т.е. операции MAX), получаем функции принадлежности для переменных X_4 и X_5. (см. рисунок 4.6).

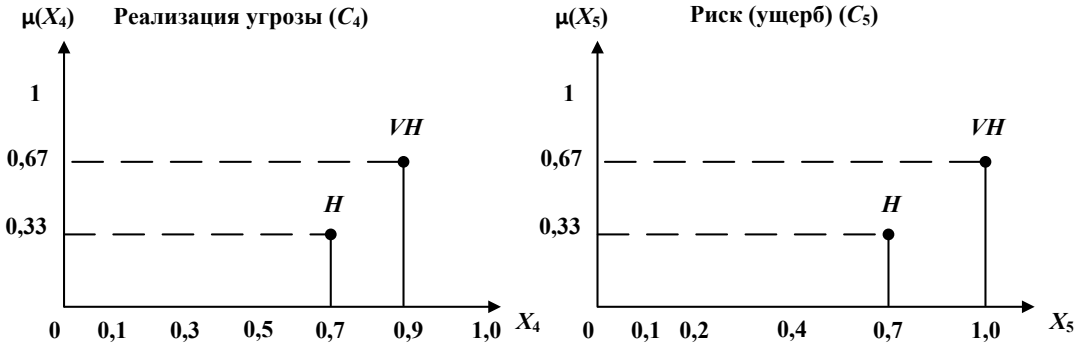


Рисунок 4.6 – Функции принадлежности нечетких переменных X_4 и X_5

Применяя формулу (4.2), вычисляем дефаззифицированные («четкие») значения переменных $X_4^* = 0{,}83$; $X_5^* = 0{,}9$. Следовательно, искомое значение уровня риска R, т.е. ожидаемого потенциального ущерба от действия угрозы, равно 90 %.

Допустим теперь, что за счет применения специальных мер по защите информации (контрмер) требуется снизить уровень риска R до среднего (M) или

низкого (L). С целью анализа эффективности различных способов управления риском воспользуемся НПКК, приведенной на рисунке 4.7.

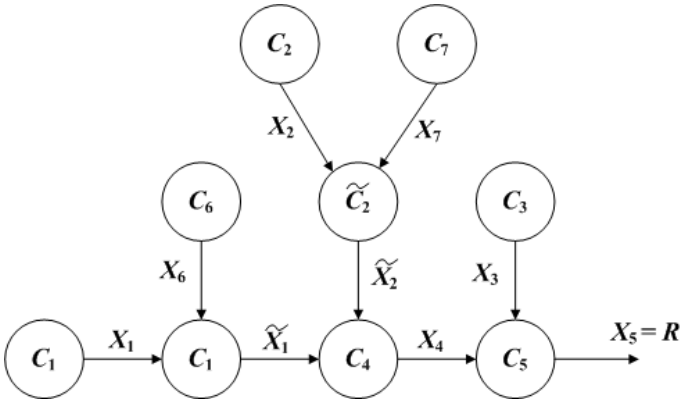


Рисунок 4.7 – Схема НПКК для оценки риска с учетом контрмер

Здесь: C_1, C_2, C_3 – соответственно угроза, уязвимость и информационный ресурс (как и в предыдущем, примере речь идет об оценке последствий от реализации вирусной атаки); 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. Соответственно в качестве переменных состояния концептов выступают: X_1 – вероятность возникновения угрозы; $\tilde{X}_1$ – вероятность скомпенсированной угрозы; $\tilde{X}_2$ – вероятность скомпенсированной уязвимости; X_3 – ценность (стоимость) информационного ресурса; X_4 – вероятность успешной реализации угрозы; $X_5 = R$ – уровень риска (величина ожидаемого потенциального ущерба); X_6 и X_7 – затраты на парирование угрозы и уязвимости.

То обстоятельство, что вновь введенные промежуточные концепты $\tilde{C}_1$ и $\tilde{C}_2$, как и концепты C_4 и C_5, являются «двухвходовыми», позволяет представить базу нечетких продукционных правил НПКК в виде совокупности 4-х раздельных таблиц, две из которых (приведенные выше) характеризуют изменение состояния концептов C_4 и C_5 в зависимости от состояния смежных концептов: $X_1 \times \widetilde{X_2} \to X_4$ и $X_3 \times X_4 \to X_5$.

Дополнительные две таблицы будут определять состояния новых концептов $\widetilde{C_1}$ и $\widetilde{C_2}$ с учетом добавленных в НПКК внешних управляющих факторов C_6 и C_7: $X_1 \times X_6 \to \widetilde{X_1}$ и $X_2 \times X_7 \to \widetilde{X_2}$ (см рисунок 4.8 – таблицы 3 и 4).

Табл. 3. Скомпенсированная угроза $\widetilde{C_1}$

X_1 \ X_6	L	M	MH	H	VH
VH	VH	H	MH	M	M
H	H	MH	MH	M	L
MH	MH	M	M	M	L
M	M	L	L	L	L
L	L	L	L	L	L

Табл. 4. Скомпенсированная уязвимость $\widetilde{C_2}$

X_2 \ X_7	L	M	MH	H	VH
VH	VH	H	MH	M	M
H	H	MH	MH	M	L
MH	MH	M	M	M	L
M	M	L	L	L	L
L	L	L	L	L	L

Рисунок 4.8 – Функции принадлежности нечетких переменных X_4 и X_5

Будем полагать, что функции принадлежности для нечетких переменных X_1, X_2, X_3, X_4, X_5 имеют тот же вид, что и на рис. 2. Для простоты принимаем, что функции принадлежности для переменных $\widetilde{X_1}$ и $\widetilde{X_2}$ имеют тот же вид, что и функции принадлежности переменных X_1 и X_2, а функции принадлежности для переменных X_6 и X_7 совпадают по внешнему виду с функцией принадлежности для переменной X_3 (по оси абсцисс на графике рисунке 4.9 в отложены нормированные значения переменной).

Проведем оценку риска с помощью НПКК, представленной на рисунке 4.7, используя следующие исходные данные: $X^*_1 = 0{,}85$; $X^*_2 = 0{,}9$; $X^*_3 = 0{,}75$ (как и в предыдущем примере); $X^*_6 = 0{,}9$; $X^*_7 = 0{,}85$ (управляющие факторы). Легко видеть, что, как и ранее, при реализации механизма нечеткого логического вывода задействуется лишь часть правил, приведенных в таблицах 1-4 рисунков 4.5 и 4.8, т.е. для расчетов можно воспользоваться схемой, представленной на рисунке 4.9.

Выполнив необходимые вычисления по схеме рисунок 4.10 в соответствии с алгоритмом Мамдани, используя при этом для реализации логических операций «и» и «или» операторы MIN и MAX, а при фаззификации – метод взвешенного среднего (3), получим «четкие» (дефаззифицированные) значения промежуточных и выходной переменных НПКК:

$\widetilde{X_1^*} = 0{,}13; \widetilde{X_2^*} = 0{,}16;\ X_4^* = 0{,}23;\ \ X_5^* = 0{,}26.$	(4.4)

Таким образом, уровень риска R в результате принятия специальных мер по защите информации снизился с 90% до 26%, т.е. в 3,5 раза.

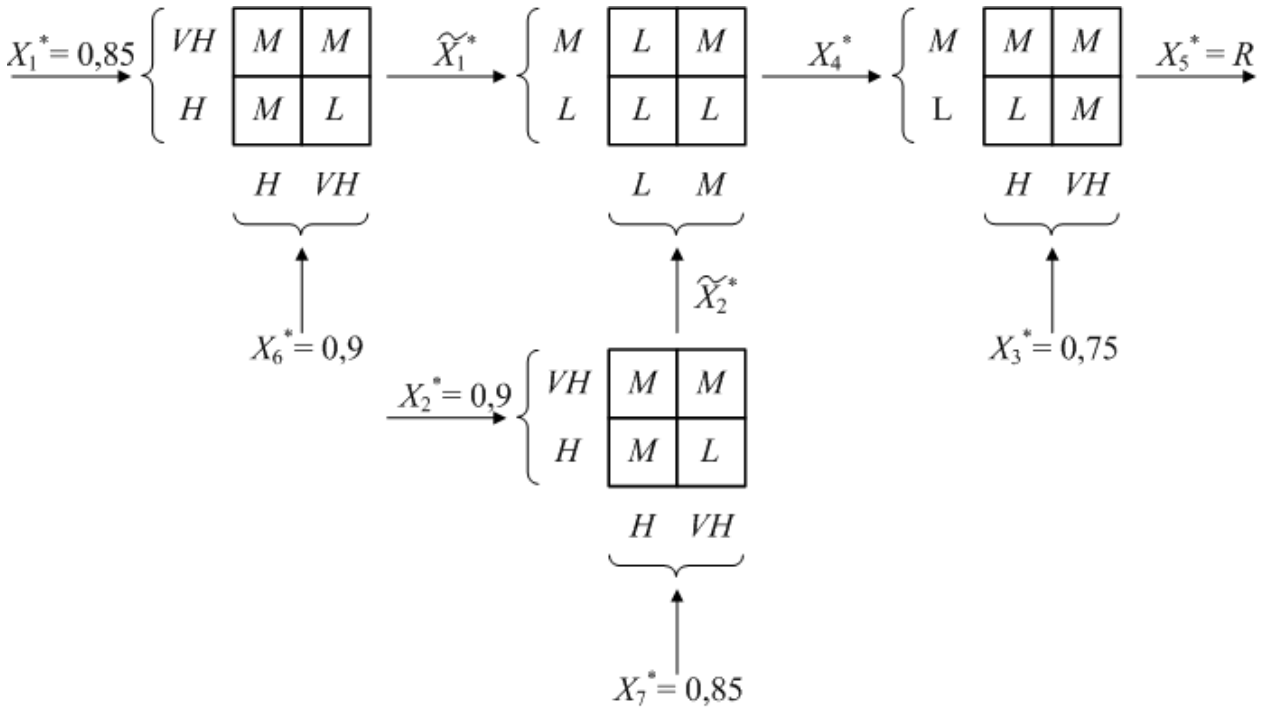


Рисунок 4.9 – Схема нечеткого логического вывода для оценки риска с учетом управляющих факторов

Аналогичным образом можно производить оценку риска для других исходных данных, отвечая на вопрос «Что будет, если…», рассматривая различные сценарии воздействия угроз и реализации защитных контрмер. Возможная постановка задачи – использование НПКК для выбора оптимального (рационального) способа защиты информации с учетом ограничений на величину риска и выделяемые ресурсы на реализацию контрмер.

К числу преимуществ предложенного подхода к оценке рисков, помимо наглядности и учета факторов неопределенности, относятся также гибкость и универсальность использования НПКК, заключающиеся в возможности расширения перечня учитываемых угроз, уязвимостей, защищаемых информационных ресурсов, а также категорий оценки рисков по видам ущерба от нарушения конфиденциальности, целостности и доступности информации.

4.3 Оценка рисков ИБ объекта КИИ с помощью серых и интуиционистских когнитивных карт

4.3.1 Оценка рисков ИБ объекта КИИ с помощью серых когнитивных карт

Пусть требуется оценить риски, связанные с нарушением конфиденциальности и целостности информации вследствие воздействия ряда угроз на

информационные ресурсы (активы). Пусть НСКК для рассматриваемой ситуации принимает вид, представленный на рис. 4.10.

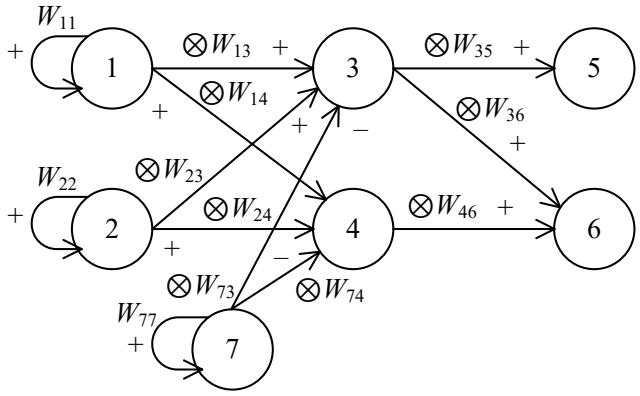


Рисунок 4.10 – Нечеткая серая когнитивная карта для оценки рисков ИБ

Здесь: 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.

Переменные состояния: $\otimes X_1$ – вероятность возникновения угрозы типа НСД за определенный период времени; $\otimes X_2$ – вероятность возникновения угрозы типа «Вредоносное программное воздействие/вирусы» за тот же период времени; $\otimes X_3$ – доля утраченных или искаженных записей в БД к их общему количеству; $\otimes X_4$ – доля времени, затрачиваемого на простои или восстановление нормальной работы ЭДО, по отношению к общему времени; $\otimes X_5$ – ущерб от нарушения конфиденциальности информации; $\otimes X_6$ – ущерб от нарушения целостности; $\otimes X_7$ – стоимость контрмер по защите информации. Связи между концептами $W_{13}, W_{14}, W_{23}, W_{24}, W_{35}, W_{36}, W_{46}$ считаются положительными, т.е. для пары концептов $C_i \to C_j$ увеличение переменной X_i приводит к увеличению переменной X_j; а связи W_{73}, W_{74} – отрицательными, т.е. увеличение переменной X_i приводит к уменьшению переменной X_j. Все переменные $\otimes X_1 \div \otimes X_7$ считаются нормированными; их значения принадлежат интервалу $[0,1]$.

Будем полагать, что при выборе серых значений весов $\otimes W_{ij}$ эксперт начинает с выбора «центров» соответствующих интервалов W_{ij}^0, ориентируясь на некоторую нечеткую шкалу, наподобие той, которая представлена в таблице 4.2.

Таблица 4.2 – Оценка силы связи между концептами

Лингвистическое значение силы связи	Числовой диапазон
Не влияет	0
Очень_слабая	(0; 0,15]
Слабая	(0,15; 0, 35]
Средняя	(0,35; 0,6]
Сильная	(0,6; 0,85]
Очень_сильная	(0,85; 1]

Следующим шагом, определяющим действия эксперта, будет выбор границ интервала $\left[\underline{W}_{ij}, \overline{W}_{ij}\right]$, определяющего серое значение силы связи $\otimes W_{ij}$. Это могут быть равноотстоящие от центрального значения W_{ij}^0 числа, например: $\otimes W_{ij} \in \left[W_{ij}^0 - \delta_{ij}, W_{ij}^0 + \delta_{ij}\right]$, где $\pm\delta_{ij}$ – разброс оценки относительно центра W_{ij}^0, но возможны и другие варианты.

Допустим, что эксперт оценил значения весов связей НСКК (рисунок 4.12) следующим образом (таблица 4.3).

Таблица 4.3 – Значения весов связей НСКК

Вес связи	Значение веса связи	Серость (разброс оценки)
W_{13}	[0,65; 0,85]	0,1
W_{14}	[0,6; 0,75]	0,075
W_{23}	[0,6; 0,8]	0,1
W_{24}	[0,5; 0,7]	0,075
W_{35}	[0,6; 0,8]	0,1
W_{36}	[0,7; 0,85]	0,075
W_{46}	[0,5; 0,7]	0,1
W_{73}	[-0,6; -0,4]	0,1
W_{74}	[-0,6; -0,3]	0,15

Здесь в отдельном столбце приведены значения уровня «серости» (greyness) соответствующих «серых» чисел, определяемого как отношение размаха серого числа к общей длине диапазона его изменения [-1, 1]:

$$\Phi\left(\otimes W_{ij}\right) = \left|\overline{W}_{ij} - \underline{W}_{ij}\right|/2 \qquad (4.5)$$

Заметим, что концепты C_1, C_2, C_7 на рисунке 4.10 имеют собственные циклы положительной обратной связи с весами $W_{11} = W_{22} = W_{77} = 1$. Это указывает на то, что данные концепты выступают в качестве независимых источников входных сигналов НСКК, отражающих воздействия на смежные концепты со стороны внешней среды (концепты-*драйверы*).

Примем в качестве функции активации $f(\cdot)$ концептов C_3, C_4, C_5, C_6 двухполярную сигмоиду. Проверка выполнения условия устойчивости для данных, приведенных в таблице 4.3, показывает, что

$\left(\sum_{i,j=3}^{6} \overline{W}_{ij}^{2}\right)^{\frac{1}{2}} = \sqrt{2{,}98} < 2,$	

т.е. установившиеся состояния НСКК для рассмотренных ниже сценариев будут устойчивы. Значения весов связей, выходящих из драйверов, т.е. концептов C_1, C_2 и C_7, в данном случае не учитываются.

Переходя непосредственно к расчетной части моделирования с помощью НСКК, рассмотрим следующие сценарии моделирования.

A) *Угроза «Несанкционированный доступ» при отсутствии дополнительных мер защиты (контрмер)*, что соответствует начальным условиям:

$\otimes X(0) = ([0{,}8; 1], [0; 0], [0; 0], [0; 0], [0; 0], [0; 0], [0; 0]);$	(4.6)

B) *Угроза «Вредоносное программное воздействие» при отсутствии дополнительных контрмер*, что соответствует начальным условиям:

$\otimes X(0) = ([0; 0], [0{,}8; 1], [0; 0], [0; 0], [0; 0], [0; 0], [0; 0]);$	(4.7)

C) *Угроза «Несанкционированный доступ» при использовании дополнительных контрмер*, что соответствует начальным условиям:

$\otimes X(0) = ([0{,}8; 1], [0; 0], [0; 0], [0; 0], [0; 0], [0; 0], [0{,}8; 1]);$	(4.8)

D) *Угроза «Вредоносное программное воздействие» при использовании дополнительных контрмер*, что соответствует начальным условиям:

$\otimes X(0) = ([0; 0], [0{,}8; 1], [0; 0], [0; 0], [0; 0], [0; 0], [0{,}8; 1]);$	(4.9)

В качестве указанных контрмер могут выступать, например, межсетевые экраны, системы обнаружения атак, антивирусные программы и т.п.

Нетрудно видеть, что для сценария A расчетная схема моделирования существенно упрощается и принимает следующий вид (рисунок 4.11).

Учитывая монотонный характер зависимостей $X_5 = f_1(X_1, X_3)$ и $X_6 = f_2(X_1, X_3, X_4)$, можно отдельно произвести оценку сначала верхней границы переменной $\otimes X_5$ и переменной $\otimes X_6$:

$$\overline{X}_5 = f_1(\overline{X}_1, \overline{X}_3);\ \ \overline{X}_6 = f_2(\overline{X}_1, \overline{X}_3, \overline{X}_4),$$

а затем – аналогично оценку нижней границы $\otimes X_5$ и $\otimes X_6$:

$$\underline{X}_5 = f_1(\underline{X}_1, \underline{X}_3);\ \ \underline{X}_6 = f_2(\underline{X}_1, \underline{X}_3, \underline{X}_4).$$

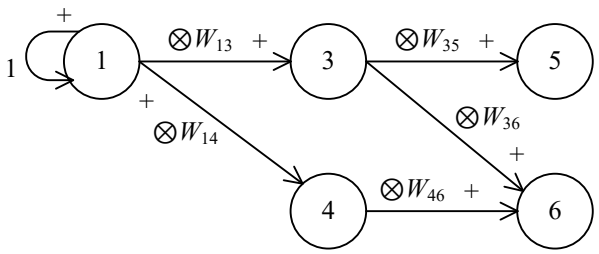
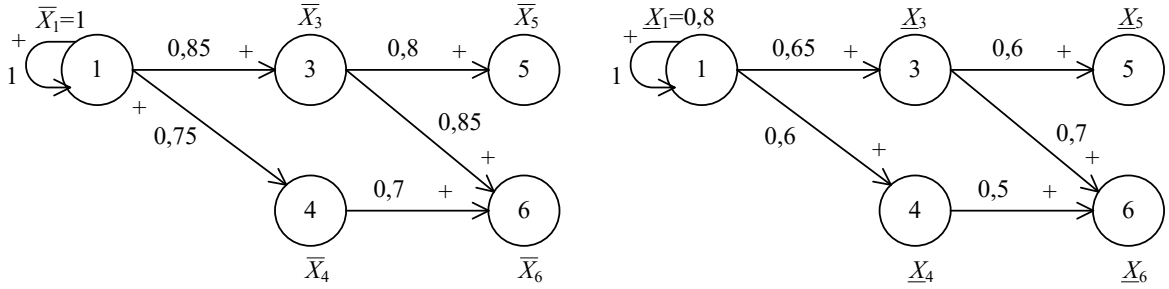


Рисунок 4.11 – Схема оценки рисков с помощью НСКК

Для исходных данных, приведенных в таблице 4.3, соответствующие схемы НКК для оценки верхней и нижней границ $\otimes X_5$ и $\otimes X_6$ принимают вид, представленный на рисунок 4.12.



а) б)

Рисунок 4.12 – Схемы НКК для оценки верхней и нижней границы рисков ИБ

Далее, используя уравнения (3), можно рассчитать значения $\overline{X}_i(k)$ и $\underline{X}_i(k)$, определяющие изменение верхних и нижних границ переменных состояния концептов $X_i(k)$ во времени $(k = 1,2, \dots)$. Выполнив соответствующие расчеты для схем НКК, на рисунке 4.12, а-б, для начальных условий (4.6) получим данные, представленные в таблицах 4.4 и 4.5.

Таблица 4.4 – Верхние границы оценок состояния

$\overline{X}_i$ \ k	1	2	3	4	5	6	7	8
$\overline{X}_3$	0,40	0,55	0,60	0,62	0,63	0,63	0,63	0,63
$\overline{X}_4$	0,36	0,50	0,55	0,57	0,58	0,58	0,58	0,58
$\overline{X}_5$	0	0,16	0,21	0,33	0,39	0,42	0,43	0,43
$\overline{X}_6$	0	0,29	0,50	0,60	0,64	0,66	0,66	0,66

Таблица 4.5 – Нижние границы оценок состояния

$\underline{X}_i$ \ k	1	2	3	4	5	6	7	8

$\underline{X_3}$	0,25	0,37	0,42	0,44	0,45	0,45	0,45	0,45
$\underline{X_4}$	0,24	0,34	0,39	0,41	0,42	0,42	0,42	0,42
$\underline{X_5}$	0	0,07	0,14	0,19	0,22	0,24	0,25	0,25
$\underline{X_6}$	0	0,15	0,28	0,37	0,41	0,44	0,45	0,45

Как видно из таблиц, переменные состояния $\overline{X_i}(k)$ и $\underline{X_i}(k)$ за 7-8 тактов достигают своих установившихся значений, что является следствием выполнения условий устойчивости. В частности, для схемы на рисунке 4.12, а имеем: $\left(\sum_{i,j=3}^{6} \overline{W}_{ij}^{2}\right)^{\frac{1}{2}} = \sqrt{1{,}85} = 1{,}36 < 2$, т.е. условие устойчивости выполняется. Таким образом, серый вектор состояния НСКК $\otimes X(k)$ сходится к установившемуся значению

$$\otimes X^*|_A =$$

$$([0{,}8; 1], [0; 0], [0{,}45; 0{,}63], [0{,}42; 0{,}58], [0{,}25; 0{,}43], [0{,}45; 0{,}66]),$$

а искомые оценки рисков ИБ вследствие нарушения конфиденциальности и целостности информации будут определяться серыми числами:

$$\otimes X_5^*|_A \in [0{,}25; 0{,}43];\ \otimes X_6^*|_A \in [0{,}45; 0{,}66]. \quad (4.10)$$

Значения «серости» для указанных установившихся значений переменных состояния:

$$\Phi_1^*|_A = 0{,}2;\ \Phi_2^*|_A = 0;\ \Phi_3^*|_A = 0{,}18;\ \Phi_4^*|_A = 0{,}16;\ \Phi_5^*|_A = 0{,}18;\ \Phi_6^*|_A = 0{,}21.$$

Следуя аналогичной процедуре, можно произвести оценку диапазонов изменения рисков ИБ для сценария B (схема НСКК на рисунке 4.13, а), сценария C (схема НСКК на рисунке 4.13, б) и сценария D (схема НСКК на рисунке 4.13, в).

После выполнения соответствующих расчетов с помощью уравнений (3) для начальных условий (4.6)-(4.9), получаем:

для сценария B (рисунок 4.13, а):

$$\otimes X_5^*|_{\mathrm{B}} \in [0{,}23; 0{,}42];\ \otimes X_6^*|_{\mathrm{B}} \in [0{,}41; 0{,}65]; \quad (4.14)$$

для сценария C (рисунок 4.13, б):

$$\otimes X_5^*|_{\mathrm{C}} \in [0{,}1; 0{,}17];\ \otimes X_6^*|_{\mathrm{C}} \in [0{,}22; 0{,}28]; \quad (4.15)$$

для сценария D (рисунок 4.13, в):

$$\otimes X_5^*|_D \in [0{,}09; 0{,}15];\ \otimes X_6^*|_D \in [0{,}17; 0{,}22]. \quad (4.16)$$

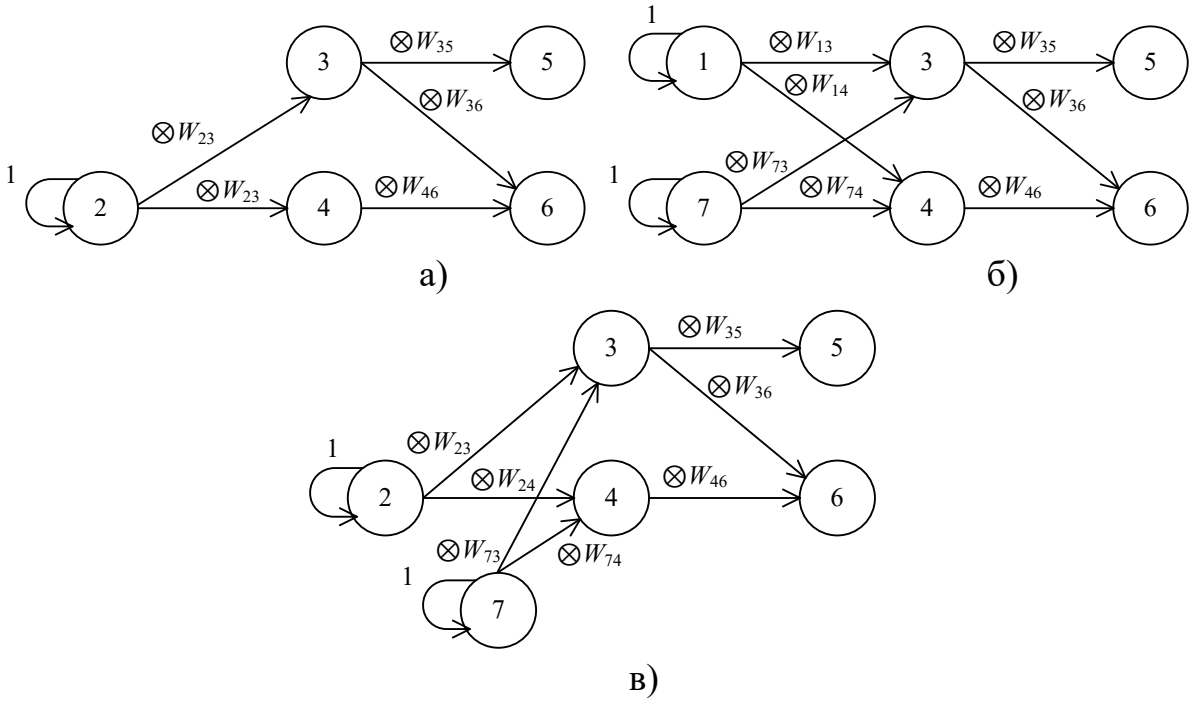


Рисунок 4.13 – Схемы НСКК для оценки рисков ИБ

С целью большей наглядности представим полученные результаты в виде диаграмм (рис. 5, а-б), где по оси абсцисс отложены значения чисел $\otimes X_5$ и $\otimes X_6$, а по оси ординат – указания на соответствующий сценарий (вариант) моделирования.

Нарушение конфиденциальности

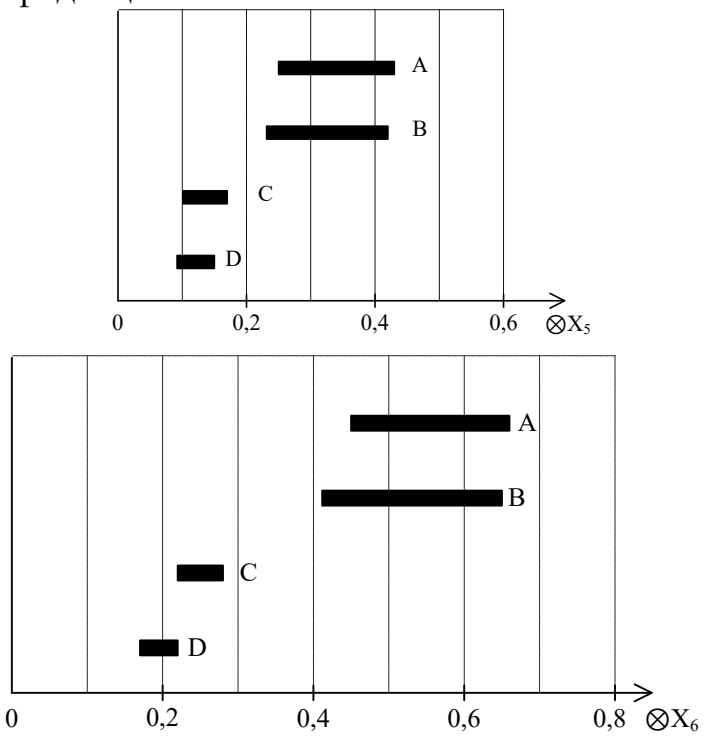


Рисунок 4.14 – Диаграммы значений рисков ИБ для различных сценариев

Как видно из рисунков, обе рассмотренные угрозы («НСД» и «Вредоносное программное воздействие») при отсутствии дополнительных контрмер по защите информации (сценарии A и B) приводят к значительным рискам, причем ущерб от нарушения целостности информации ($\otimes X_6$) превышает ущерб от нарушения ее конфиденциальности ($\otimes X_5$). Применение дополнительных контрмер позволяет в (2-2,5) раза снизить соответствующие риски. Диапазон интервальных оценок («серость» чисел $\otimes X_5$ и $\otimes X_6$) при переходе от стратегии A и B к стратегиям C и D при этом уменьшается примерно в той же пропорции, т.е. в (2,5-3) раза, что и абсолютные значения верхней и нижней границ этих чисел.

В целом, на основе полученных результатов можно сделать следующие общие выводы:

1) применение НСКК позволяет перейти от «точечных» оценок мнений экспертов (что обычно подвергается сомнению) к более мягким интервальным оценкам исходных данных, и как следствие, к получению интервальных оценок конечных результатов, что является, с одной стороны, более достоверным, а с другой стороны, предоставляет ЛПР больший материал для принятия окончательного решения с учетом его опыта и предпочтений;

2) рассмотренные выше интервальные оценки в представлении исходных данных могут, вообще говоря, отражать не «осторожность» конкретного эксперта в оценке силы взаимосвязей между концептами, а разброс мнений группы экспертов, имеющих свое собственное представление об изучаемой проблеме;

3) являясь расширением классических НКК Б. Коско, НСКК сохраняют наглядность, интерпретируемость и способность к обучению на реальных данных, т.е. общепризнанные преимущества технологий когнитивного моделирования сложных, плохо формализуемых систем;

Проанализированы основные этапы реализации соответствующей процедуры когнитивного моделирования.

Отмечаются несомненные преимущества применения НСКК для решения задачи оценки информационных рисков, связанных с получением более достоверных оценок исходных данных и предоставлением лицу, принимающему решения, больше степеней свободы для принятия окончательного и более обоснованного решения по существу изучаемого вопроса.

4.4 Методика декомпозиции вложенных НКК

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

Рассмотрена **методика анализа рисков ИБ с использованием построения вложенных нечетких когнитивных карт** на примере задачи обеспечения целостности телеметрической информации (ТМИ) в промышленной автоматизированной системе сбора, хранения и обработки информации о состоянии авиационных бортовых систем. В качестве объекта защиты будем рассматривать автоматизированную информационную систему (АИС) сбора, хранения и обработки телеметрической информации предприятия-изготовителя изделий авиационной техники.

4.4.1 Нечеткие когнитивные карты и принцип вложения

В качестве базового подхода к построению вложенных НКК можно воспользоваться предложенной в [316] теорией декомпозиции больших НКК. Согласно этой теории, процедура когнитивного моделирования начинается с построения подробной (развернутой) НКК исследуемой системы, которая принимается в качестве исходной. Затем производится разбиение множества вершин (концептов) данной НКК на ряд отдельных блоков в соответствии с отношением эквивалентности. Каждый из этих блоков содержит локальную информацию о взаимодействиях и внутренних зависимостях между концептами в пределах данного блока. Рассматривая полученные блоки в качестве вершин укрупненной (обобщенной) НКК (авторы [316] назвали Quotient Fuzzy Cognitive Map), получим новое блочное представление НКК.

На рисунке 4.15 показан пример подобной декомпозиции НКК (слева – исходная НКК, состоящая из 6 индивидуальных блоков (частных НКК), определенным образом связанных между собой; справа – укрупненная НКК, каждая из вершин которой отражает множество вершин соответствующей частной НКК.

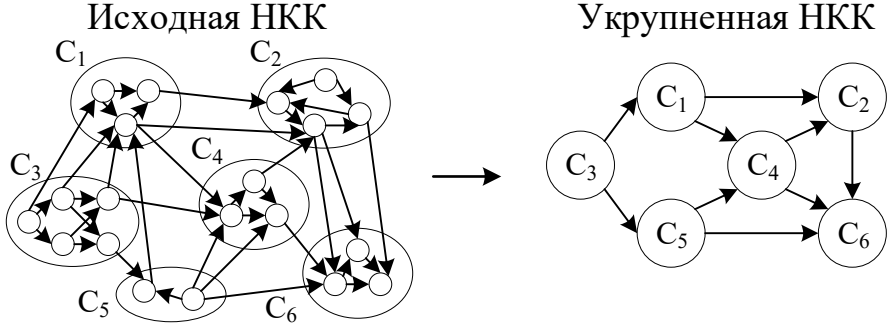


Рисунок 4.15 – Пример декомпозиции НКК

В отличие от описанной выше процедуры преобразования НКК [316] путем ее «сворачивания» (т.е. от частного к общему), наоборот, будем строить вложенную НКК путем ее «развертывания», детализации (от общего к частному). Будем полагать, что рассматриваемая вложенная НКК строится в классе НСКК, предложенных в 2010 г. Хосе Салмероном [274].

4.4.2 Методика анализа рисков ИБ с помощью вложенных нечетких серых когнитивных карт

Рассмотрим методику анализа рисков ИБ распределенной системы с использованием вложенных нечетких когнитивных карт на следующем примере. В качестве объекта защиты будем рассматривать АИС сбора, хранения и обработки ТМИ предприятия-изготовителя (ПИ) изделий авиационной техники. Текущая информация о параметрах состояния бортовых систем собирается в течение всего периода их эксплуатации наземными службами технического обслуживания. Детальный анализ этой информации позволяет в последующем принимать правильные управленческие и конструкторские решения о дальнейшей эксплуатации и модификации бортовых систем летательного аппарата. Поэтому задача обеспечения целостности ТМИ в условиях воздействия на нее внешних и внутренних угроз имеет важное значение.

Обобщенная структура перспективной территориально распределенной АИС сбора, хранения и обработки ТМИ на станциях технического обслуживания приведена в Приложении Г.

Используя в качестве инструмента моделирования аппарат НСКК, обратимся к задаче анализа рисков, связанных с обеспечением целостности ТМИ в рассмотренной выше АИС с учетом воздействия на систему внешних и внутренних угроз. Укрупненная НСКК для оценки рисков АИС, выступающая в данном

случае как когнитивная модель АИС начального приближения (нулевой уровень декомпозиции), представлена на рисунке 4.16.

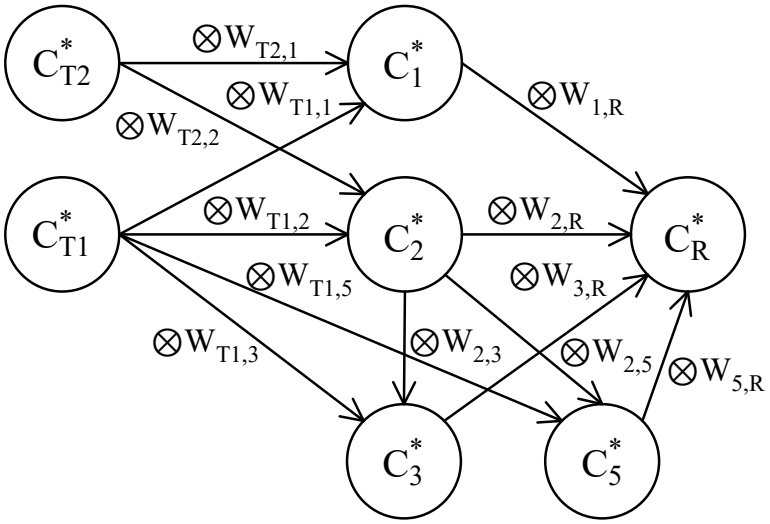


Рисунок 4.16 – Укрупненная (исходная) НСКК для оценки рисков АИС

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

Таблица 4.7 Список концептов укрупненной НСКК

Концепт	Наименование концепта
$C_{T_1}^*$	Внутренняя угроза целостности ТМИ (вследствие сбоев или ошибочных действий персонала)
$C_{T_2}^*$	Внешняя угроза целостности ТМИ (вследствие попытки несанкционированного доступа извне к информации)
C_1^*	Модификация данных ТМИ в Зоне 1
C_2^*	Модификация данных ТМИ в Зоне 2
C_3^*	Модификация данных ТМИ в Зоне 3
C_5^*	Модификация данных ТМИ в Зоне 5
C_R^*	Риск (потенциальный ущерб), вызванный нарушением целостности ТМИ в АИС

Выбор серых значений весов связей $\otimes W_{ij}$ для НСКК на рисунке Г.1 должен производиться экспертом с учетом его опыта и субъективных оценок вероятностей использования уязвимостей АИС, что на практике весьма затруднительно. Учитывая, что каждое из указанных событий представляет собой сложное событие, состоящее из цепочки следующих друг за другом элементарных событий, целесообразно декомпозировать изображенную на рисунке Г.1 НСКК, представив ее в виде набора вложенных НСКК для отдельных концептов (т.е. зон безопасности, содержащих целевые объекты атаки на ТМИ через соответствующие уязвимости АИС).

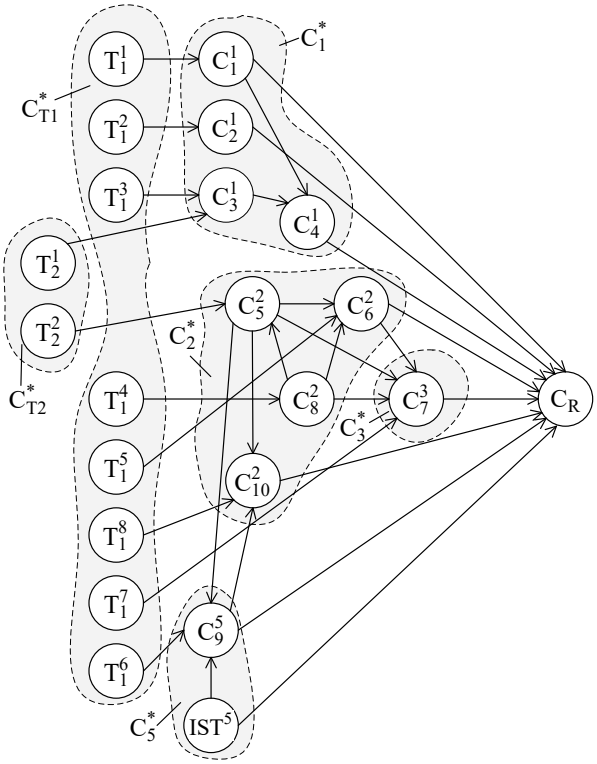


Рисунок 4.17 – Первый уровень декомпозиции НСКК для оценки рисков АИС

Первый уровень декомпозиции исходной (укрупненной) НСКК представлен на рисунке 4.17. Здесь используются следующие обозначения: верхний индекс (маркер «q») концепта C_p^q указывает на его принадлежность к концепту C_q^* укрупненной НСКК; нижний индекс (p) – номер концепта в НСКК первого уровня декомпозиции.

Таблица 4.8 – Список концептов первого уровня декомпозиции НСКК

Концепт	Наименование концепта	Родительский концепт
$T_1^1, \dots, T_1^8$	Внутренние угрозы целостности ТМИ (т.е. точки потенциальной реализации угрозы нарушения целостности ТМИ внутренним субъектом)	T_1^*
T_2^1, T_2^2	Внешние угрозы целостности ТМИ (декомпозиция концепта T_2^*)	T_2^*
C_1^1	Доступ к данным ТМИ в клиент-серверной SCADA web-base до внесения в БД оперативного хранилища ТМИ	C_1^* (Зона 1)
C_2^1	Доступ к БД оперативного хранения данных ТМИ	
C_3^1	Доступ к сетевому оборудованию	
C_4^1	Доступ к модулю Web-сервера отправки данных ТМИ в долгосрочное хранилище ПИ	
C_5^2	Доступ к сетевой инфраструктуре	C_2^* (Зона 2)
C_6^2	Доступ к модулю Web-клиента, реализующего прием ТМИ на ПИ с удаленных станций обслуживания	
C_8^2	Несанкционированный доступ к рабочей станции ядра КИС ПИ	
C_{10}^2	Доступ к серверу отчетов о состоянии оборудования, формируемых для пользователей Зоны 4	

C_7^3	Получение доступа к ТМИ в долгосрочном хранилище	C_3^* (Зона 3)
C_9^5	Доступ к серверу управления вычислительным кластером Зоны 5	C_5^* (Зона 5)
IST^5	Модуль контроля целостности ТМИ	

На рисунке 4.18 представлен второй уровень декомпозиции для концепта C_1^*, позволяющий уточнить воздействие угроз на рассматриваемый концепт.

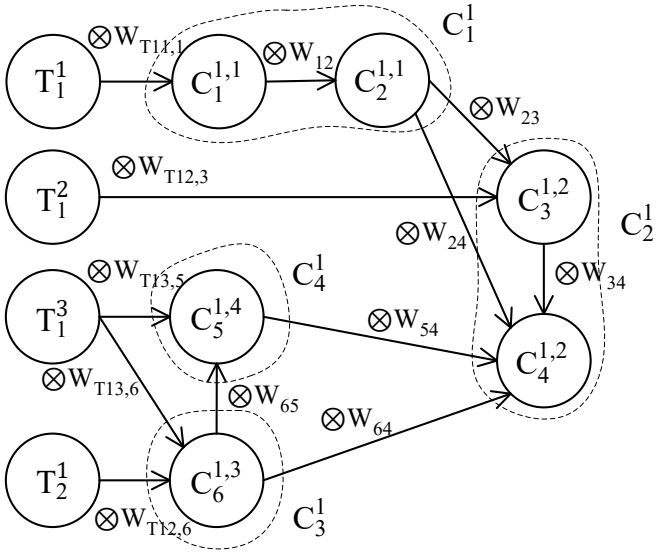


Рисунок 4.18 – Второй уровень декомпозиции НСКК для оценки рисков АИС в зоне 1

На схеме используются следующие обозначения концептов $C_r^{q,p}$ второго уровня декомпозиции НСКК: верхний индекс (маркер «q») – номер концепта (родительский концепт нулевого уровня декомпозиции) укрупненной НСКК, в состав которого входит данный элемент; индекс p – номер родительского концепта первого уровня декомпозиции; нижний индекс (r) – номер концепта текущего уровня. Список концептов второго уровня декомпозиции НСКК для зоны 1 приведен в таблице 4.9.

Таблица 4.9 – Список концептов второго уровня декомпозиции НСКК для зоны 1

Концепт	Наименование концепта	Родительский концепт
$C_1^{1,1}$	Доступ к HMI client SCADA	C_1^1
$C_2^{1,1}$	Доступ к оперативным данным ТМИ на client-server части SCADA до внесения в оперативное хранилище	
$C_3^{1,2}$	Доступ к клиенту для взаимодействия с сервером OPC UA	C_2^1
$C_4^{1,2}$	Доступ к БД хранения оперативных данных ТМИ	

Дальнейшая декомпозиция второго уровня позволяет перейти к еще более детальной НСКК, позволяющей учитывать влияние отдельных уязвимостей на потенциальное нарушение целостности ТМИ в промежуточных элементах обработки информации.

Так, для концепта $C_1^{1,1}$, характеризующего возможность запуска в браузере клиентской части SCADA системы на основе Web-технологий (зона 1), соответствующая декомпозиция может быть представлена в виде НСКК на рисунке 4.19.

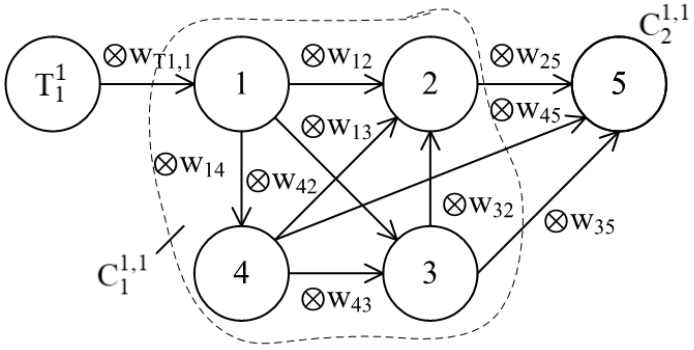


Рисунок 4.19 – Третий уровень декомпозиции – концепт $C_1^{1,1}$

Здесь цифрами 1÷5 обозначены следующие концепты:

1 – эксплуатация уязвимости системы авторизации ОС;

2 – эксплуатация уязвимости Web-клиента SCADA;

3 – эксплуатация уязвимости браузера ОС для запуска клиентской части SCADA;

4 – эксплуатация уязвимости доступа к памяти ОС;

5 – эксплуатация уязвимости системы авторизации OPC UA клиента.

Аналогичным образом можно провести декомпозицию других концептов исходной НСКК для второго уровня декомпозиции Зоны 1, представленной на рисунке 4.18 (см. рисунки 4.20-4.21). Соответствующая НСКК, раскрывающая содержание концепта C_2 (Зона 2), приведена на рисунке 4.20.

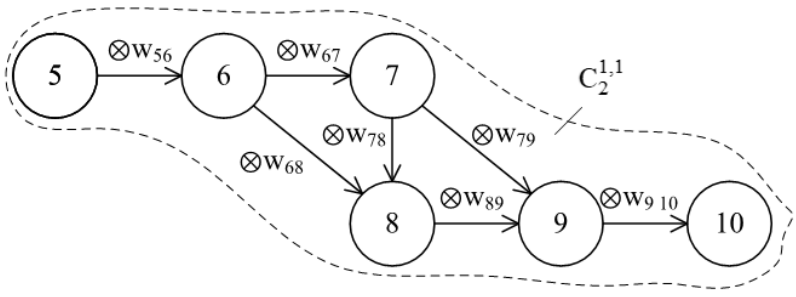


Рисунок 4.20 – Декомпозиция концепта $C_2^{1,1}$ НСКК для оценки рисков АИС Зоны 1

Таблица 4.10 – Список концептов третьего уровня декомпозиции Зоны 1

Концепт	Название концепта	Родительский концепт

6	эксплуатация уязвимости системы авторизации основного пользователя ОС	$C_2^{1,1}$
7	эксплуатация уязвимости доступа к памяти ОС	
8	эксплуатация уязвимости виртуальной машины Java	
9	эксплуатация уязвимости системного ПО сервера приложений для запуска серверного Web-приложения SCADA системы	
10	целевой концепт доступа к оперативным данным ТМИ, которые могут быть модифицированы до внесения в БД на узлах SCADA client-server type	

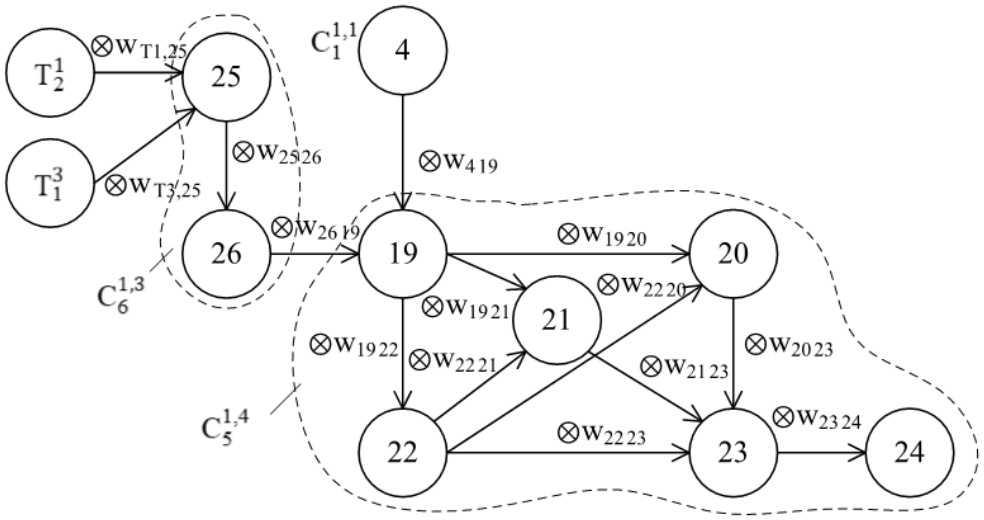


Рисунок 4.21 – Декомпозиция концептов $C_6^{1,3}$ и $C_5^{1,4}$ второго уровня декомпозиции НСКК

Таблица 4.11 – Список концептов третьего уровня декомпозиции Зоны 1

Концепт	Название концепта	Родительский концепт
19	Эксплуатация уязвимости системы авторизации основного пользователя ОС	$C_5^{1,4}$
20	Эксплуатация уязвимости системного ПО, реализующего работу связки сервера веб-приложений Apache, СУБД MySQL, среды исполнения PHP для поддержки интерактивных Web-страниц	
21	Эксплуатация уязвимости доступа к памяти ОС	
22	Эксплуатация уязвимости доступа к памяти виртуальной машины Java	
23	Эксплуатация уязвимости ПО сервера приложений	
24	Целевой концепт несанкционированного запуск модуля доступа к БД оперативного хранения ТМИ на станциях обслуживания ЛА	
25	Эксплуатация уязвимости системы авторизации основного пользователя ОС	$C_6^{1,3}$
26	эксплуатация уязвимости доступа к памяти ОС	

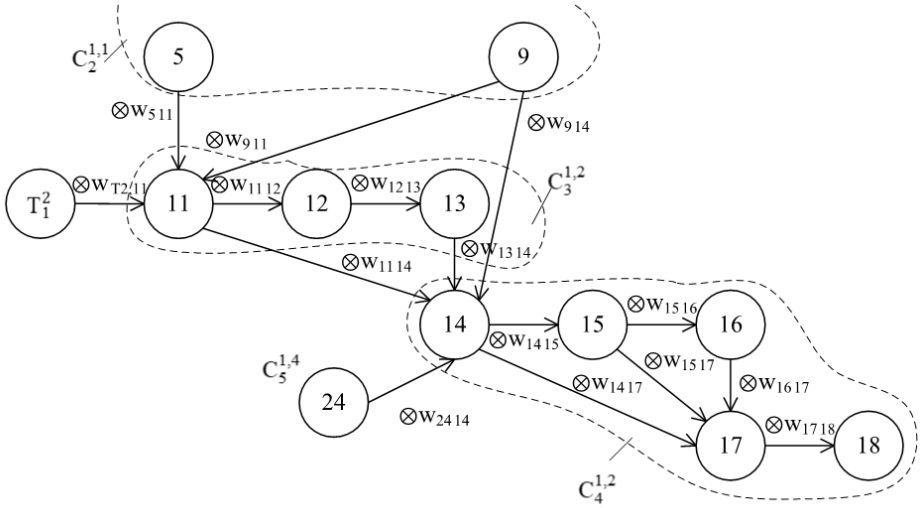


Рисунок 4.22 – Декомпозиция концептов $C_3^{1,2}$ и $C_4^{1,2}$ НСКК для оценки рисков АИС

Таблица 4.12 – Список концептов третьего уровня декомпозиции Зоны 1

Концепт	Название концепта	Родительский концепт
14	Эксплуатация уязвимости системы авторизации основного пользователя ОС	$C_4^{1,2}$
15	Эксплуатация уязвимости доступа к памяти ОС	
16	Эксплуатация уязвимости системы авторизации основного пользователя СУБД	
17	Эксплуатация уязвимости доступа к памяти СУБД	
18	целевой концепт несанкционированной модификация оперативных данных ТМИ, хранимых в БД	
11	Эксплуатация уязвимости системы авторизации клиентской части ПО OPC Client UA	$C_3^{1,2}$
12	Эксплуатация уязвимости системы авторизации основного пользователя ОС	
13	Эксплуатация уязвимости доступа к памяти ОС	

В основе предложенного подхода используется построение укрупненной НСКК для оценки рисков автоматизированной информационной системы, с последующей ее декомпозицией на ряд вложенных когнитивных карт следующих уровней детализации. Особенности построения данной процедуры рассмотрены на примере задачи обеспечения целостности ТМИ в промышленной автоматизированной системе сбора, хранения и обработки информации о состоянии авиационных бортовых систем. Использование НСКК позволяет при этом получить более достоверные оценки факторов риска с учетом возможного разброса фактически располагаемых данных и мнений экспертов.

4.4.3 Методика построения многослойных нечетких когнитивных карт

Общую идею построения многослойной НКК можно пояснить рисунком 4.23.

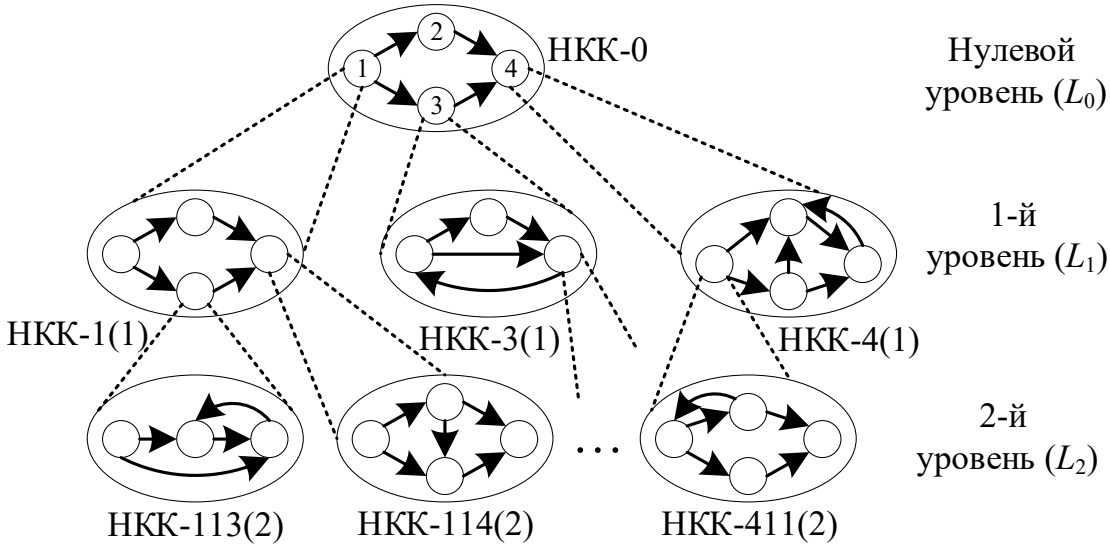


Рисунок 4.23– Архитектура многослойной НКК

Здесь НКК-0 – исходная (укрупненная) НКК, соответствующая нулевому (концептуальному) уровню представления исследуемой проблемы; 1, 2, 3, 4 – базовые концепты, образующие исходную НКК-0; НКК-1(1), НКК-3(1), НКК-4(1) – нечеткие когнитивные карты первого уровня декомпозиции исходной нечеткой когнитивной карты НКК-0, раскрывающие содержание (внутреннюю структуру) своих «родительских» концептов 1, 3, 4; НКК-113(2), НКК-114(2), НКК-411(2) – нечеткие когнитивные карты 2-го уровня декомпозиции, раскрывающие (детализирующие) содержание концептов НКК-1(1), НКК-4(1) и т.д. Таким образом, верхний слой (нулевой уровень декомпозиции) НКК-0 отвечает за предоставление глобальной информации об исследуемой проблеме, тогда как последующие, нижележащие слои НКК (1-й, 2-й и т.д. уровни) обеспечивают дополнительную, локальную информацию о взаимодействиях и внутренних зависимостях, характеризующих поведение концептов вышележащего уровня («родительских» концептов).

Согласно [247], разбиение НКК на слои (уровни) производится экспертом или группой экспертов таким образом, что каждый слой (L_i) описывает определенный аспект понимания, глубины изучения проблемы и, следовательно, число слоев (d) многослойной НКК будет определяться числом принимаемых во внимание аспектов. В общем виде, многослойная НКК представляет собой многослойный ориентированный граф G, определяемый кортежем множеств

$G = \{V_M, E_M, V, L\}$	(4.17)

где V_M – множество вершин графа (концептов НКК), участвующих в формировании слоев в соответствии с принятым способом декомпозиции НКК; E_M – множество дуг, связывающих вершины графа (концепты НКК), входящие в V_M; V – множество всех вершин (концептов НКК); L – множество слоев НКК.

В свою очередь, множества L, V_M, E_M определяются с помощью следующих отношений:

$L = \{L_a\}_{a=0}^{d-1} = L_0 \times L_1 \times \ldots \times L_{d-1};$ $V_M \subseteq V \times L_0 \times L_1 \times \ldots \times L_{d-1};$ $E_M \subseteq V_M \times V_M.$	(4.18)

Общее количество концептов, входящих в многослойную НКК, равно $D = \sum_{a=0}^{d-1}|L_a|$, где $|L_a|$ – число концептов, принадлежащих слою L_a.

Ключевым вопросом построения многослойных НКК является разбиение исходной (укрупненной) НКК на слои, а также изучение взаимодействия между концептами как внутри слоя, так и между слоями. Рассмотрим подробнее методику построения многослойных НКК для анализа рисков ИБ.

1. *Нулевой уровень декомпозиции (слой L_0) НКК*

Составляется исходная (укрупненная) НКК-0, которая включает в себя в качестве концептов наиболее значимые (существенные) факторы рисков ИБ с указанием выявленных экспертами взаимосвязей между этими концептами.

В качестве рекомендаций общего характера при реализации данного этапа можно воспользоваться информацией, приведенной в [76, 77]. Оценка силы связей НКК-0 при этом является предварительной (приближенной), уточнение силы связей между концептами откладывается до следующего этапа построения НКК.

2. *Первый уровень декомпозиции (слой L_1) НКК*

На данном этапе производится «раскрытие» всех или части концептов, входящих в состав укрупненной нечеткой когнитивной карты НКК-0. Рассмотрим, как это делается, на следующем примере. Допустим, что некоторый концепт C_1, принадлежащий НКК-0, реализует причинно-следственную (каузальную) связь ЕСЛИ A_1 И A_2, ТО F (рисунок 4.24, а). Здесь A_1, A_2 и F – события, которые могут произойти с определенной степени вероятности (уверенности). Будем полагать, что вероятности наступления указанных событий определяются параметрами X_1, X_2, X_3 (переменными состояния), принадлежащими интервалу $[0,1]$. Предположим теперь, что мы рассматриваем отношение $(A_1 \text{ И } A_2) \rightarrow F$ как сложное событие, которое можно представить в виде цепочки последовательных

элементарных событий: $A_1 \to B_1$; $A_2 \to B_2$; $(B_1$ И $B_2) \to D_1$; $B_2 \to D_2$; $(D_1$ И $D_2) \to F$. Тогда родительский концепт C_1 замещается частной НКК, состоящей из 5 концептов C_1^1, C_1^2, C_1^3, C_1^4, C_1^5 (см. рисунок 4.24, б).

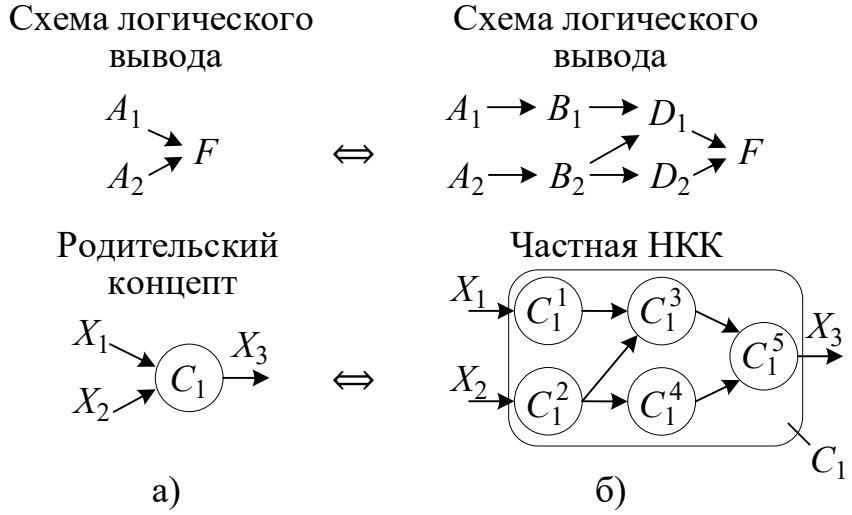


Рисунок 4.24– Общая схема декомпозиции: а – родительский концепт C_1; б – частная НКК

В основе данного преобразования лежит отношение эквивалентности, согласно которому родительский концепт и замещающая его частная НКК считаются эквивалентными, если они имеют одинаковые входы и выходы, реализуют эквивалентные (т.е. взаимно преобразуемые) схемы логического вывода и одинаково интерпретируемы (хотя и с разной глубиной понимания) в рамках общей (укрупненной) НКК исследуемой проблемы.

На этом же этапе уточняются значения весов связей между концептами (уже применительно к частным НКК) с учетом дополнительной информации, полученной от экспертов.

3. *Следующие уровни декомпозиции (слои L_2, L_3, ...) НКК*

Аналогично, любой из концептов частных НКК, построенных на предыдущем уровне декомпозиции, может быть, в свою очередь, развернут (детализирован), что в итоге даст возможность еще более глубокого анализа всех аспектов изучаемой проблемной области за счет включения в рассмотрение дополнительных нижележащих слоев L_2, L_3 и т.д. Соответственно, пересматриваются (уточняются) значения весов связей между концептами НКК.

4. *Моделирование поведения (динамики) полного набора нечетких когнитивных карт*

Для каждой НКК (начиная с частных НКК нижних уровней декомпозиции L_1, L_2, … и заканчивая укрупненной НКК самого верхнего уровня L_0) производится расчет динамики изменения состояния концептов.

После выполнения всех расчетов для частных (локальных) НКК, расположенных на нижних слоях НКК, производится агрегирование полученных результатов моделирования на верхнем уровне НКК (слой L_0), с вычислением интегральных показателей оценки рисков.

4. *Сценарное моделирование с использованием НКК*

Завершающим этапом когнитивного моделирования является этап сценарного моделирования, на котором производится анализ различных вариантов воздействия факторов риска ИБ с оценкой ожидаемых последствий, выбор возможных контрмер для снижения уровня рисков, формирование рекомендаций ЛПР.

Преимуществом данного класса когнитивных моделей является, помимо их наглядности, возможность последовательного раскрытия неопределенности на каждом последующем (нижележащем) слое нечеткой когнитивной карты, с привлечением дополнительной информации от экспертов о содержании базовых концептов (факторов риска). Кроме того, использование данного класса нечетких когнитивных моделей обеспечивает возможность учета разброса мнений экспертов о взаимном влиянии концептов и, как следствие, обеспечить больше степеней свободы лицу, принимающему решение на основании результатов моделирования.

4.5 Сценарный подход к моделированию сложных многошаговых целенаправленных кибератак с использованием базы меташаблонов атак

Предложен **сценарный подход [31, 44] к моделированию сложных многошаговых целенаправленных кибератак с использованием базы меташаблонов атак САРЕС и БДУ ФСТЭК** с дальнейшей формализацией в виде иерархической НКК для возможности анализа с требуемым уровнем детализации и количественной оценки рисков ИБ. 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.

4.5.1 Моделирование вектора кибератак на основе композиции меташаблонов

В качестве примера промышленного объекта для моделирования вектора кибератак рассмотрим АСУ ТП транспорта товарной нефти (ТТН), интегрированную в комплексную систему оперативного контроля и управления в реальном масштабе времени, позволяющую передавать накапливаемые технологические данные о состоянии объекта в системы управления производственными процессами вышележащих уровней.

В соответствии с ГОСТ Р 62443, выделим фрагмент базовой архитектуры АСУ ТП ТТН, включающий в себя основные элементы АСУ нефтеперекачивающих станций, телекоммуникационное оборудование и линии связи (рисунок 3.17). Наиболее опасным с точки зрения возможных последствий сценарием развития кибератаки при этом является ситуация, когда в результате несанкционированного доступа злоумышленник получает возможность управления ключевым оборудованием предприятия: становится возможным изменить транспортные потоки, спровоцировать аварии, вызвать чрезвычайные ситуации и т.д. Поэтому проанализируем угрозу перехвата управления АСУ ТП (УБИ.183 в БДУ ФСТЭК), которая заключается в возможности осуществления злоумышленником несанкционированного доступа к информационной инфраструктуре за счет получения права управления входящей в ее состав АСУ ТП путем эксплуатации уязвимостей ее программного обеспечения или слабостей технологических протоколов передачи данных. Возможные последствия:

– остановка работы насосного оборудования нефтеперекачивающих станций;

– нарушение целостности накапливаемых данных учета принятой нефти.

Процесс моделирования атаки внешнего злоумышленника на АСУ ТП ТТН на основе традиционного подхода с использованием графовых моделей рассмотрен в Приложении Д.

4.5.2 Моделирование вектора кибератак в базисе нечетких когнитивных карт

Рассмотрим дальнейшую формализацию графа атак в виде иерархической нечеткой когнитивной карты, позволяющей анализировать векторы атак с требуемым уровнем детализации за счет механизмов декомпозиции и укрупнения. Процедура преобразования НКК путем ее «сворачивания» (т.е. перехода от частного к общему), и, наоборот, построения вложенной НКК путем ее «развертывания», детализации (от общего к частному) описаны в [204, 311].

В данной случае рассмотрим процедуру «сворачивания» детализированной НКК, раскрывающей содержание вектора атак, до укрупненной НКК уровня представления кибератаки. Процесс сворачивания действий злоумышленника на хосте 7 экспертного графа атак (рисунок Д.1) отображен на рисунке 4.25, где $ВЗ_1$ – концепт-драйвер, характеризующий активного внешнего злоумышленника, а численные обозначения приведены для концептов, соответствующих элементам графа атак подробного меташаблона с привязкой к системе индексации базы шаблонов CAPEC.

Алгоритм построения укрупненной НКК для сформированного вектора атаки включает следующие шаги:

1. Композиция сценарного уровня моделирования атаки (рисунке 4.25, I)
2. Наиболее детализированный уровень графа атаки получен на основе анализа матрицы переходов детальных меташаблонов. Вершины графа атак соответствуют концептам НКК, а веса связей – вероятностям переходов, полученным на основе оценок опасности уязвимостей CVSS.
3. Построение укрупненной НКК для представления модели атаки (рисунке 4.25, II). Если предыдущий детализированный уровень НКК отражал ряд действий злоумышленника на каждом этапе реализации атаки, то данный уровень позволяет свернуть данные действия до описания последовательности этапов развития атаки на основе формализованных меташаблонов, т.е. отображает сценарий реализации кибератаки.
4. Построение НКК для свернутого представления варианта отдельной атаки (рисунке 4.25, III). Каждая атака укрупняется до концепта НКК с соответствующими весовыми коэффициентами, позволяющими оценить вероятность реализации атаки в каждом из возможных сценариев.

5. Построение НКК для моделирования набора возможных атак на выделенные целевые концепты с оценкой вероятности реализации и значимости возможных последствий (рисунке 4.26).
6. Результирующая НКК, позволяющая оценить уровень рисков ИБ при реализации воздействия злоумышленника на АСУ ТП.

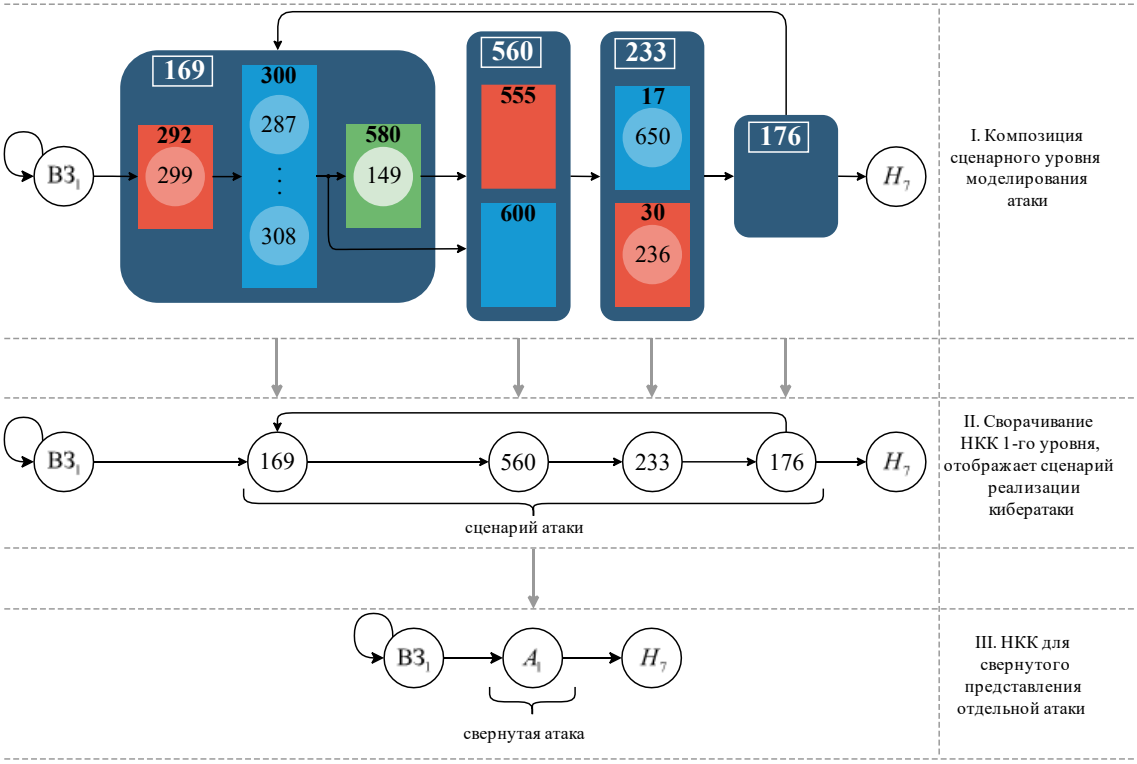


Рисунок 4.25 – Этапы построения укрупненной НКК для формализации детального графа атаки

На рисунке 4.26 развернута цепочка действий злоумышленника (фрагмент Cyber Kill Chain) при реализации атаки на граничные элементы системы (хосты 7 и 1) с последующими переходами к внутренним хостам сети (3, 6 и далее – 14 и 20), достижимость которых определяется из матрицы переходов графа физической и логической топологий сети с учетом наличия уязвимостей для реализации переходов между промежуточными узлами. Целевыми концептами являются хосты 14 и 20, соответствующие серверу промежуточного хранения исторических данных и ПЛК. Соответствующими последствиями реализации атаки являются концепты $П_I$ и $П_{II}$, описанные ранее.

Множество маршрутов из начальной вершины НКК в конечную отражает множество сценариев, т.е. последовательность перемещений злоумышленника между элементами системы.

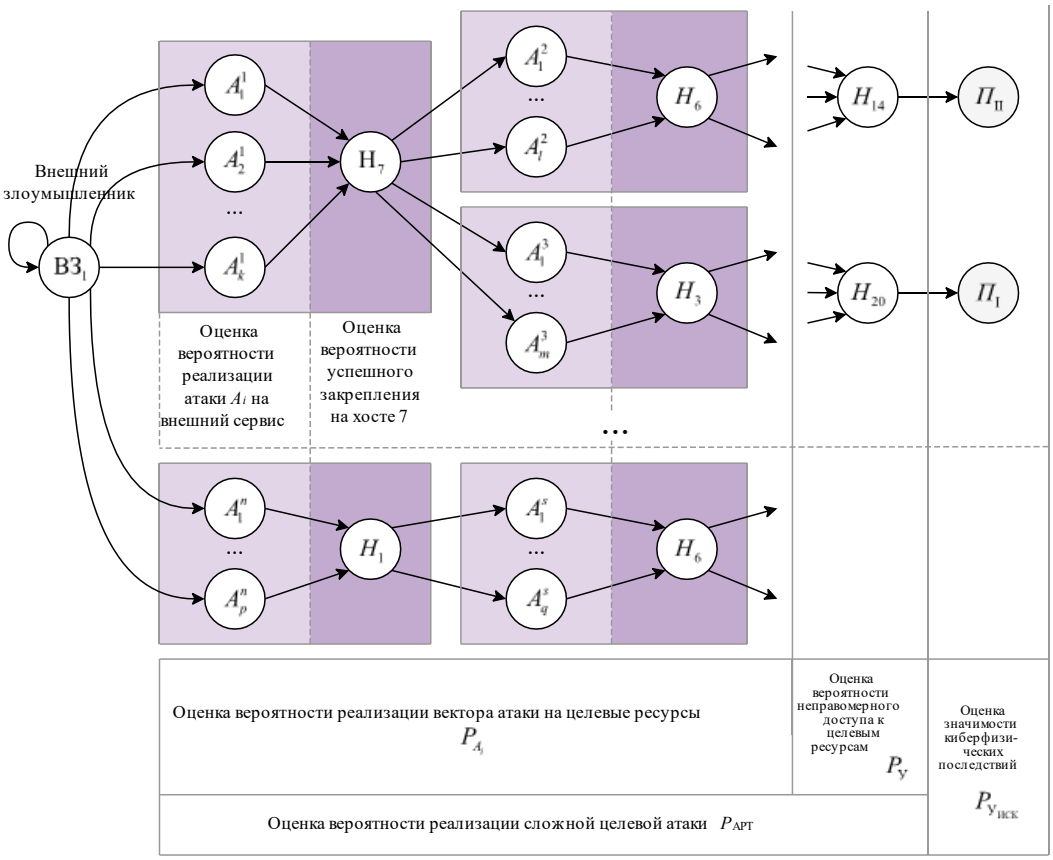


Рисунок 4.26 – НКК для моделирования набора атак на выделенные целевые концепты

Поскольку сценарий характеризуется наличием уязвимостей на всем пути злоумышленника до цели, а также метриками CVSS этих уязвимостей, то на основании НКК, моделирующей все возможные атаки на ресурсы рассматриваемой системы, формируются [102, 111]:

– оценка вероятности реализации атаки на внешний сервис, как первый шаг нарушителя, нацеленный на проникновении в систему предприятия;

– оценка вероятности успешного закрепления на узле;

– оценка реализации каждого этапа кибератаки в отдельности;

– оценка реализации вектора атаки на целевой ресурс, определяющая возможность реализации воздействий злоумышленника на информационную инфраструктуру предприятия для достижения целевого ресурса;

– оценка вероятности неправомерного доступа к целевому ресурсу, что говорит о успешности реализации конкретного сценария реализации кибератаки;

– оценка вероятности реализации сложной целенаправленной кибератаки;

– оценка значимости последствий, на основании которых эксперт может сделать выводы о критичности последствий реализации кибератаки.

4.5.3 Пример моделирования вектора кибератак на основе меташаблонов CAPEC с количественной оценкой риска ИБ

Согласно предложенному алгоритму, строится НКК (рисунок 4.27, I), соответствующая детализированному уровню графа атаки (рисунок 4.27, I). На основе детализированной НКК с учетом оценок взаимовлияния и установившегося состояния концептов строится НКК (рисунок 4.27, II, где A_j^i – концепт, состояние которого соответствует оценке вероятности реализации сценария атаки злоумышленника, закрепившегося на i-узле сети, на j-узел) для свернутого представления варианта отдельной атаки внешнего злоумышленника на VPN-сервер базовой архитектуры сети (хост 7).

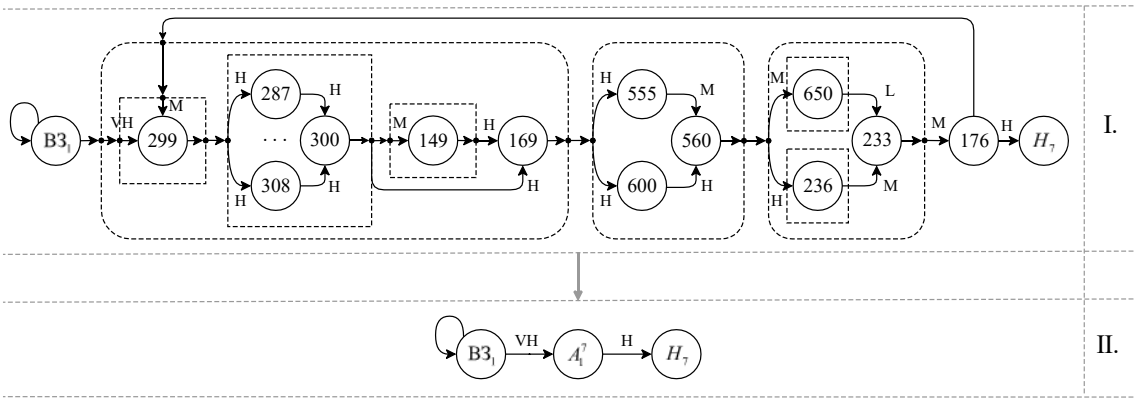


Рисунок 4.27 – НКК, моделирующая атаку на хост 7

Следующим шагом является построение НКК (рисунок 4.28) для моделирования набора возможных атак на выделенные целевые концепты базовой архитектуры с оценкой вероятности реализации и значимости возможных последствий.

С учетом определенных на предыдущем шаге установившихся значений концептов A_j^i рассчитываются оценки рисков ИБ остановки работы насосного оборудования (C_{Π_I}) и нарушения целостности исторических данных ($C_{\Pi_{II}}$) (таблица 4.13). При анализе максимального потока в ориентированном графе НКК из вершины $ВЗ_1$ в целевые вершины C_{Π_I} и $C_{\Pi_{II}}$) с помощью алгоритма Форда-Фалкерсона можно выделить [36] наиболее критичные узлы сети (C_9, C_{18}, C_{19}, C_5, C_{20}), закрепление на которых позволяет злоумышленнику реализовать атаки, приводящие к наиболее значительным последствиям. Следовательно, для выделенных узлов рассмотрим применение соответствующих дополнительных средств защиты информации (концепты $C_{СЗИ_1}$, $C_{СЗИ_2}$, $C_{СЗИ_3}$, $C_{СЗИ_4}$, $C_{СЗИ_5}$).

Интервальные значения соответствующих целевых концептов C_{Π_I} (рисунок 4.29, а) и $C_{\Pi_{II}}$ (рисунок 4.29, б) при реализации каждого из сценариев позволяют оценить эффективность применяемых СЗИ.

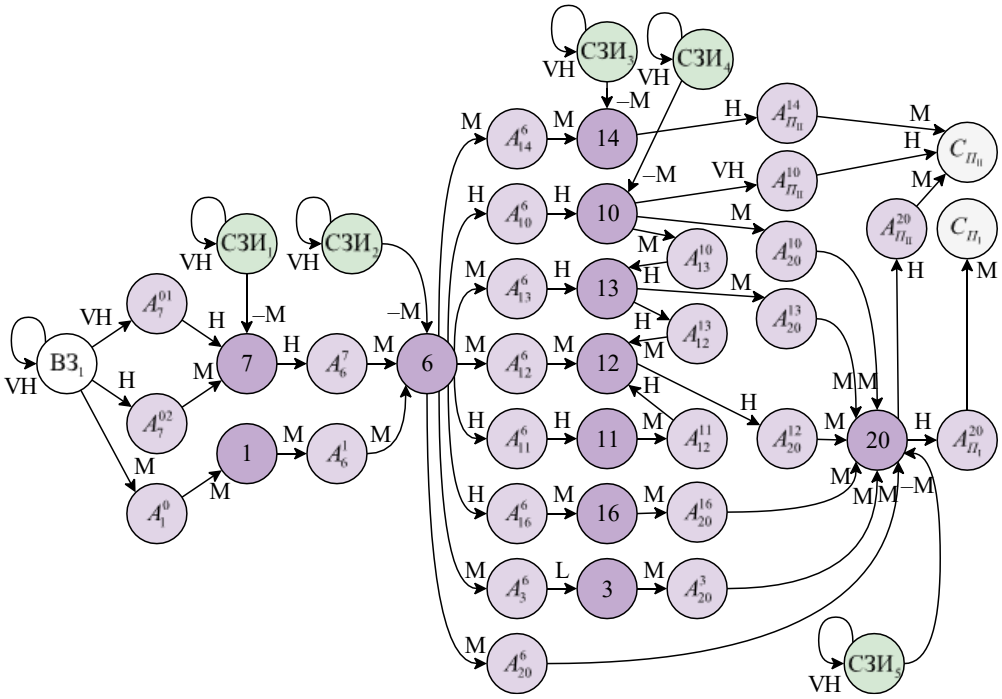
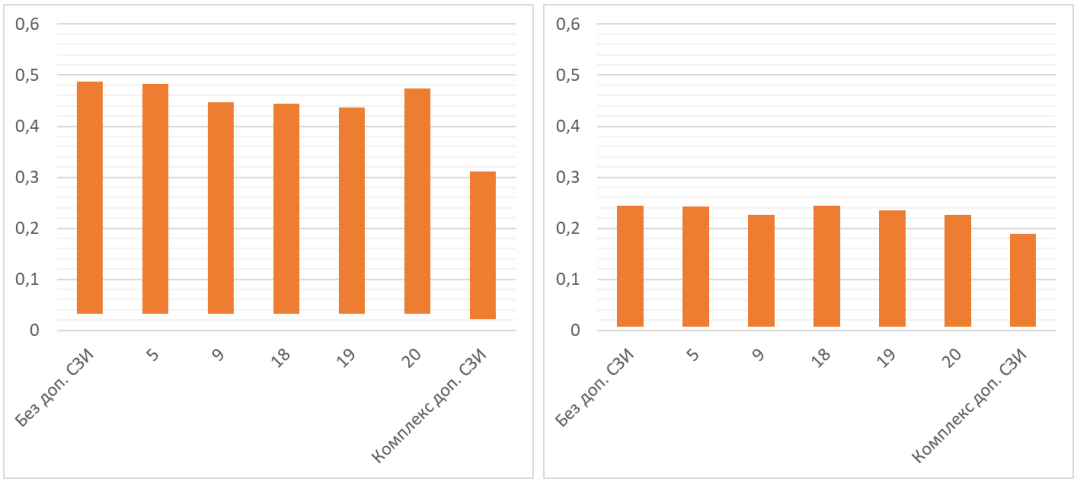


Рисунок 4.28 – НКК, моделирующая возможные атаки на выделенные целевые концепты базовой архитектуры

$C_{ВЗ_1}$ – внешний злоумышленник, реализующий атаку на компоненты АСУ ТП; C_{Π_I} – остановка работы насосного оборудования; $C_{\Pi_{II}}$ – нарушение целостности исторических данных.



а) б)

Рисунок 4.29 – Интервальные значения целевых концептов C_{Π_I}(а) и $C_{\Pi_{II}}$(б) при моделировании сценариев реализации сложной атаки внешнего злоумышленника на целевые ресурсы: без дополнительных СЗИ, дополнительные СЗИ применяются для ключевых узлов базовой архитектуры сети (C_5, C_9, C_{18}, C_{19}, C_{20}), применяется комплекс доп. СЗИ

Таблица 4.13 – Оценка рисков ИБ

Сценарий	Остановка работы насосного оборудования ($C_{П_I}$)	Нарушение целостности исторических данных ($C_{П_{II}}$)
Без применения дополнительных СЗИ	[0,0073; 0,2366]	[0,0323; 0,4544]
СЗИ для узла C_5	[0,0073; 0,2352]	[0,0323; 0,4511]
СЗИ для узла C_9	[0,0072; 0,2192]	[0,0322; 0,4545]
СЗИ для узла C_{18}	[0,0073; 0,2366]	[0,0317; 0,4120]
СЗИ для узла C_{19}	[0,0072; 0,2286]	[0,0322; 0,4045]
СЗИ для узла C_{20}	[0,0073; 0,2189]	[0,0323; 0,4414]
Применение комплекса СЗИ для узлов C_5, C_9, C_{18}, C_{19}, C_{20}	[0,0071; 0,1818]	[0,0223; 0,2883]

Показатели риска ИБ для ключевых ресурсов снизились в среднем на 15-20 %, что свидетельствует об эффективности рекомендуемых мер нейтрализации кибератак.

Автоматизированное моделирование набора возможных атак на компоненты базовой архитектуры АСУ ТП ТТН позволяет извлечь информацию о слабых местах ИС, наиболее опасных уязвимостях и потенциальных слабостях компонент системы, выявить наиболее успешные сценарии реализации атак и оценить их последствия для предприятия. Исходными данными для построения когнитивных карт становятся не только экспертные оценки (граф атак), но и формализованные и систематизированные шаблоны из международных баз знаний, что существенно повышает обоснованность и полноту сценарного моделирования. Применение данного подхода позволит получить подробную оценку рисков кибербезопасности и, как следствие, обеспечить более обоснованный выбор средств для реализации стратегии многоуровневой эшелонированной защиты.

Традиционно используется построение вектора в виде графа атак, однако пошаговое описание реализации кибератаки на АСУ ТП вызывает трудности с масштабируемостью графа атак и затруднения у экспертов в процессе его практического анализа. Кроме того, неполнота и противоречивость исходных данных затрудняет оценку вероятностных переходов при анализе вектора атак. Построение НКК для моделирования набора всех возможных атак и их сценариев реализации облегчает специалистам анализ защищенности и позволяет на этапе архитектурного проектирования ИС заложить основные средства и инструменты защиты. В результате анализа вектора кибератак эксперт может определить все возможные сценарии реализации с учетом используемых уязвимостей, оценить уровень опасности реализации каждого сценария в отдельности и кибератаки в целом.

4.6 Меры повышения интерпретируемости НКК

Одной из первоочередных задач при построении и применении нечетких когнитивных моделей является проблема их интерпретируемости, т. е. прозрачности, понятности в терминах, доступных ЛПР по результатам моделирования.

Первым шагом на пути решения данной проблемы является структурно-топологический анализ НКК, предложенной экспертами, позволяющий выявить наиболее структурно-значимые элементы в составе НКК, а также относительно независимые подсистемы НКК, играющие ключевую роль в поведении исследуемой системы.

Другая группа методов связана с обработкой результатов опроса экспертов относительно характера взаимного влияния концептов, причем результатом подобной процедуры может быть как агрегация мнений экспертов, так и переход к описанию НКК в виде интервально-значной (серой, интуиционистской) НКК, поведение которой описывается уравнениями интервальной математики.

И наконец, на этапе сценарного моделирования с помощью НКК, повышение интерпретируемости полученных результатов достигается путем повышения вариативности (разнообразия) используемых сценариев. При этом оценивается влияние как отдельных факторов риска, так и комбинации этих факторов, в том числе путем расширения состава моделируемой НКК за счет включения в нее дополнительных факторов, направленных на снижение рисков ИБ. Залогом успешной реализации перечисленных мер является автоматизация основных этапов когнитивного моделирования с использованием проблемно-ориентированных диалоговых средств моделирования НКК.

На этапе определения структуры НКК – первым необходимым шагом является оценка структурно-топологических свойств полученной НКК. При этом можно воспользоваться, например, следующими показателями структурной сложности НКК [76, 361]:

а) *плотность* (density) НКК – коэффициент, показывающий степень связности изображающего ее графа:

$$D = \frac{L}{n(n-1)} \qquad (4.19)$$

где L – общее число связей в НКК; n – число концептов НКК;

б) *центральность* (centrality) концепта C_i – характеризует степень взаимодействия i-го концепта НКК с его соседями:

– *исходящая центральность* – подсчитывается как сумма сил связей W_{ij}, выходящих из рассматриваемого концепта C_i:

$$od_i = \sum_{k=1}^{n} W_{ik} \quad (4.20)$$

– *входящая центральность* – подсчитывается как сумма сил связей W_{ij}, входящих в рассматриваемый концепт:

$$id_i = \sum_{k=1}^{n} W_{ki} \quad (4.21)$$

– *общая центральность* концепта (или степень вершины графа):

$$td_i = od_i + id_i \quad (4.22)$$

Следующий конструктивный шаг в изучении полученной НКК – ее декомпозиция на относительно независимые подсистемы (блоки, модули), объединяющие в своем составе группы из числа смежных, наиболее тесно взаимодействующих между собой концептов НКК.

Эффективной мерой повышения интерпретируемости модели НКК является *редукция* (упрощение) НКК, т. е. уменьшение количества концептов НКК за счет объединения близких по содержанию концептов, а также удаления из НКК наименее значимых концептов.

На этапе определения весов связей НКК важное значение имеет работа с экспертами, грамотное построение процедуры оценивания весов связей, внимательное отношение к мнению каждого эксперта (хотя разброс мнений и оценок экспертов является неизбежным и в определенной степени даже желательным).

Существуют различные подходы к обработке результатов опроса экспертов:

а) приведение полученного множества оценок экспертов к «точечным» значениям весов связей.

При этом могут использоваться как стандартные методы экспертных оценок [100], так и адаптированные к решению данной задачи метод планирования экспериментов [229], метод объединения (merging) ориентированных графов [241, 213], оптимизация структуры и значений весов НКК с помощью генетического алгоритма [269];

б) учет разброса оценок экспертов посредством описания силы связей между концептами в рамках различных модификаций НКК:

– представление весов связей с помощью нечетких терм-множеств;

– представление весов связей с помощью интервальных чисел;

– описание силы связей с помощью нечетких продукционных правил.

Применение данного подхода к оценке рисков ИБ позволяет получить в конечном итоге количественную оценку факторов риска в виде некоторых диапазонов значений риска (нижняя граница – «оптимистическая» оценка риска, верхняя граница – «пессимистическая» оценка), что дает ЛПР аргументы для более взвешенного принятия решений по управлению рисками.

На этапе сценарного моделирования проводится серия вычислительных экспериментов с полученной НКК с целью получения ответов на следующие ключевые вопросы:

– каковы ожидаемые риски нарушения ИБ?

– какие из учитываемых факторов риска являются определяющими и какую долю они вносят в совокупную оценку значения риска?

– какие управляющие факторы являются наиболее эффективными с учетом полученных оценок риска, насколько их применение позволит минимизировать (или удержать в заданных пределах) оценки ожидаемых рисков?

Естественно, что выполнению указанной серии экспериментов должен предшествовать тщательно спланированный выбор сценариев моделирования. На данном этапе важно правильно оценивать адекватность выбранной для моделирования НКК, используя для этого различные метрики (критерии сравнительного анализа) НКК. В работе [315] предложено использовать для этих целей три группы метрик: а) основанные на анализе контента; б) основанные на анализе показателей структурной сложности НКК; в) основанные на анализе динамики поведения НКК. Последнее означает, что результаты расчета переменных состояния НКК несут в себе определенную информацию о характере изменения состояния НКК во времени («быстро», «медленно»), что также должно учитываться при прогнозировании значений рисков ИБ.

Когнитивное моделирование требует для своей реализации, как правило, значительных ресурсов времени в силу необходимости рассмотрения и сравнения различных вариантов решения поставленной задачи. Выход из создавшейся ситуации – автоматизация основных этапов моделирования с применением специально разработанных для этих целей пакетов программ.

4.7 Выводы по главе

Показаны возможности и преимущества, которые предоставляет технология когнитивного моделирования (и в частности, аппарат нечетких когнитивных карт) для решения задачи анализа и управления информационными рисками. Особенностью применения данной технологии является акцент на выявление наиболее существенных факторов, оказывающих влияние на постановку задачи и получение необходимого результата, оценка существующих между ними причинно-следственных связей, возможность сравнительного анализа различных вариантов принятия решений. Полученные при этом качественные модели в виде НКК особенно полезны на этапе предварительной оценки рисков информационной безопасности, при отсутствии достоверной статистики об имеющихся и потенциальных возможных инцидентов ИБ.

Рассмотрены особенности применения одного из перспективных классов когнитивных моделей – нечетких продукционных когнитивных карт (НПКК) для решения задачи оценки рисков информационной безопасности. В основе построения данных моделей используется описание взаимодействия между концептами, образующими НПКК, с помощью системы нечетких правил (продукций), отражающих знания и опыт экспертов в данной предметной области.

На конкретном примере реализации вирусной атаки на информационный ресурс рассмотрены основные этапы исполнения алгоритма нечеткого логического вывода Мамдани – фаззификация исходных данных, работа с правилами, дефаззификация (приведение к четкости).

К числу преимуществ предложенного подхода к оценке рисков, помимо наглядности и учета факторов неопределенности, относятся также гибкость и универсальность использования НПКК, заключающиеся в возможности расширения перечня учитываемых угроз, уязвимостей, защищаемых информационных ресурсов, а также категорий оценки рисков по видам ущерба от нарушения конфиденциальности, целостности и доступности информации.

Рассмотрена процедура оценки рисков обеспечения кибербезопасности промышленной сети АСУ ТП нефтедобывающего предприятия с использованием когнитивного моделирования на основе классических, серых и интуиционистских НКК и их ансамбля. Реализованы основные стадии анализа и моделирования объекта защиты, согласно ГОСТ 62443: построен фрагмент референсной модели архитектуры АСУ ТП месторождения, включающий основные элементы

АСУ кустовых площадок. Рассмотрено применение предложенной методики для оценки рисков обеспечения целостности телеметрической информации в промышленной сети и непрерывности технологического процесса. Применение ансамбля нечетких когнитивных карт позволяет учесть неопределенность мнений экспертов в оценке риска ИБ по сравнению с оценками, получаемыми отдельными НКК. Таким образом, предложенная методика позволяет получить качественную и количественную оценку показателей риска с учетом совокупности объективных и субъективных факторов неопределенности.

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

Рассмотрена **методика анализа рисков ИБ с использованием построения вложенных нечетких когнитивных карт** на примере задачи обеспечения целостности телеметрической информации (ТМИ) в промышленной автоматизированной системе сбора, хранения и обработки информации о состоянии авиационных бортовых систем. В качестве объекта защиты будем рассматривать автоматизированную информационную систему (АИС) сбора, хранения и обработки телеметрической информации предприятия-изготовителя изделий авиационной техники.

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

«сворачивания» детализированной нечеткой когнитивной карты вектора атаки показан на примере угрозы перехвата управления автоматизированной системы управления технологическими процессами нефтедобывающего предприятия с оценкой вероятности реализации с учетом уровня опасности эксплуатируемых уязвимостей. Разработаны основные программные модули системы. Проведены вычислительные эксперименты с целью оценки эффективности ее применения. Показано, что в результате анализа вектора кибератак в нечетком когнитивном базисе эксперт может ранжировать возможные сценарии реализации с учетом используемых уязвимостей, оценить уровень опасности реализации каждого сценария в отдельности и кибератаки в целом.

Одной из первоочередных задач при построении и применении нечетких когнитивных моделей является проблема их интерпретируемости, т. е. прозрачности, понятности в терминах, доступных ЛПР по результатам моделирования. Первым шагом на пути решения данной проблемы является структурно-топологический анализ НКК, предложенной экспертами, позволяющий выявить наиболее структурно-значимые элементы в составе НКК, а также относительно независимые подсистемы НКК, играющие ключевую роль в поведении исследуемой системы. Другая группа методов связана с обработкой результатов опроса экспертов относительно характера взаимного влияния концептов, причем результатом подобной процедуры может быть как агрегация мнений экспертов, так и переход к описанию НКК в виде интервально-значной (серой, интуиционистской) НКК, поведение которой описывается уравнениями интервальной математики. И наконец, на этапе сценарного моделирования с помощью НКК, повышение интерпретируемости полученных результатов достигается путем повышения вариативности (разнообразия) используемых сценариев. При этом оценивается влияние как отдельных факторов риска, так и комбинации этих факторов, в том числе путем расширения состава моделируемой НКК за счет включения в нее дополнительных факторов, направленных на снижение рисков ИБ. Залогом успешной реализации перечисленных мер является автоматизация основных этапов когнитивного моделирования с использованием проблемно-ориентированных диалоговых средств моделирования НКК.

Глава 5. 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) [66, 68, 103, 110, 112, 115-117, 122, 125, 135, 145, 153, 156].

5.1 Система и способы мониторинга целостности телеметрической информации

5.1.1 Способ мониторинга целостности телеметрической информации на основе алгоритмов интеллектуального анализа ТВР

Способ мониторинга целостности данных, получаемых с эксплуатируемой САУ ГТД ЛА, основан на применении алгоритмов адаптивной сегментации ТВР с использованием таких характеристик сигналов, как: амплитуда, форма волны (морфологии), длительность, распределение энергии, частотное содержание и т.д., с последующей идентификацией фрагментов ТВР и сопоставлением их с отдельными событиями. Блок принятия решений о наличии вмешательства злоумышленника и внесении модификации в контент сообщения при передаче информации с борта ЛА на ПИ обеспечивает обработку ТВР, генерируемых САУ ГТД на эксплуатируемом ЛА, а именно определяет режим работы САУ ГТД (установившийся или переходный) и производит сравнение этих данных с данными, генерируемыми моделью на предприятии-изготовителе.

Структурная схема способа мониторинга целостности параметров САУ ГТД летательного аппарата прототипа представлена на рисунке 5.1.

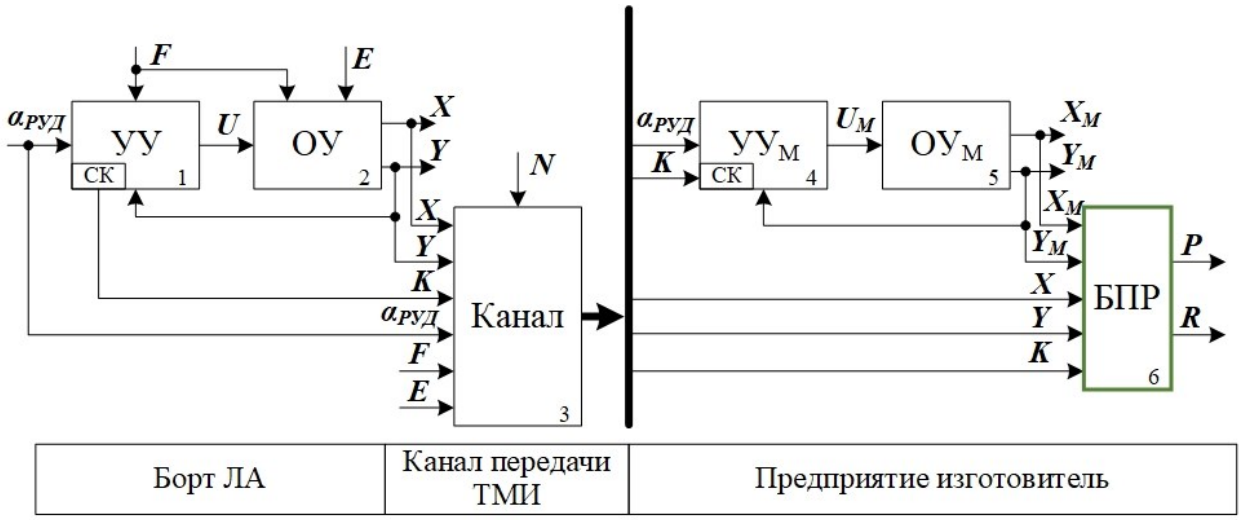


Рисунок 5.1 – Структурная схема способа мониторинга целостности параметров САУ ГТД летательного аппарата

Таблица 5.1 – Основные обозначения структурной схемы способа мониторинга целостности

№	Обозначение параметра	Параметр	Примечания
1	*F*	свойства внешней среды, такие как параметры атмосферного воздуха: температуру за бортом ЛА, давление и прочее	Вектор
2	*E*	дополнительные эксплуатационные факторы	Вектор
3	*Y*	параметры регулирования, такие как: частоты вращения роторов, давление воздуха за компрессором, температура газа за турбиной и т.д.	Вектор
4	*X*	характеристики САУ ГТД: тяга, скорость ее изменения, удельный расход топлива и прочее	Вектор
5	*U*	вектор управляющих воздействий, формируемый устройством управления	Вектор
6	*K*	сигнал о состоянии САУ ГТД (исправна К=1/неисправна К=0)	Сигнал
7	$\alpha_{РУД}$	положение рычага управления ГТД	Сигнал
8	*N*	воздействие внешних факторов и шума на канал	Вектор
9	Y_M	параметры регулирования на выходе модели объекта управления (аналог *Y*) на предприятии изготовителе	Вектор
10	X_M	характеристики модели ГТД (аналог *X*)	Вектор
11	U_M	вектор управляющих воздействий, формируемый моделью устройства управления (аналог U_M)	Вектор

В систему управления ГТД поступает векторы ***F*** и ***E***. Исходящими из объекта управления 2 в составе системы управления на борту ЛА являются векторы ***Y*** и ***X***. В объект управления 2 поступает вектор управляющих воздействий ***U***,

формируемый устройством управления 1. Система контроля САУ ГТД формирует сигнал (***K***) о ее состоянии.

Векторы ***X, Y, K, F, E*** и $\boldsymbol{\alpha}_{\text{РУД}}$ передаются через канал передачи данных 3 на предприятие-изготовитель для использования в модели САУ ГТД: блоки 4 и 5. Канал подвергается воздействию внешних факторов и шуму (***N***).

Возникновение отказа на борту ЛА – особый случай. При передаче данных с борта ЛА на предприятие-изготовитель, включающих подобный сигнал, предприятие–изготовитель связывается с органами ОрВД для исключения возможности подделки такого сигнала злоумышленником

В случае, если на предприятие-изготовитель пришли данные, говорящие о нормальной работе САУ ГТД (К=1), однако злоумышленник модифицировал сигнал системы контроля, и неисправности были, сравнение ТВР и оценка параметров согласованности выявит нарушение целостности.

Векторы $\boldsymbol{X}$, $\boldsymbol{Y}$, $\boldsymbol{Y_M}$, $\boldsymbol{X_M}$ передаются в блок принятия решения 6 (БПР), где выполняется оценка их согласованности, а также проверяется состояние сигнала системы контроля (***K***), после чего принимается решение (***R***) о том, было ли совершено воздействие на систему злоумышленником, произошел отказ оборудования или работа продолжается в штатном режиме и оценка вероятности правильности принятого решения (***P***).

Способ мониторинга целостности данных, получаемых с борта ЛА, включает следующие основные шаги:

1. выделяется набор параметров САУ ГТД для анализа согласованности данных ТМИ, полученных с модели, и данных, полученных с борта ЛА;
2. выделяется скользящее окно для анализа многомерных векторов X, Y, $\boldsymbol{Y_M}, \boldsymbol{X_M}, \boldsymbol{X_M^W}, \boldsymbol{X_R^W}$ – наборы ТВР, сгенерированные моделью и полученные с ЛА, помещенные в одно временное окно;
3. строится многомерный технологический временной ряд (мТВР) P^W – параметры согласованности ТВР для каждого из окон анализа W_S;
4. определяется режим работы САУ ГТД U_H (установившийся или переходный) в выделенном временном окне;
5. выполняется расчет параметров согласованности ТВР, полученных с борта ЛА, и ТВР, генерируемых моделью;
6. по вычисленным параметрам согласованности определяется тип рассогласования ТВР;

7. на основе типа динамики САУ ГТД, типа рассогласования ВР и сигнала системы контроля принимается решение о целостности данных, полученных с ЛА;

Контроль целостности ТМИ базируется на анализе согласованности поведения параметров, полученных с помощью модели сложного технического изделия, и принимаемых с бортовых систем летательного аппарата. Выходом системы мониторинга является решение о наличии вмешательства злоумышленника и внесении модификации в контент сообщения при передаче информации с борта ЛА на ПИ и оценка вероятности событий нарушения целостности данных.

Структурная схема системы, реализующей способ мониторинга целостности данных, полученных из модели САУ ГТД и летательного аппарата, представлена на рисунке 5.2 и содержит в себе следующие блоки:

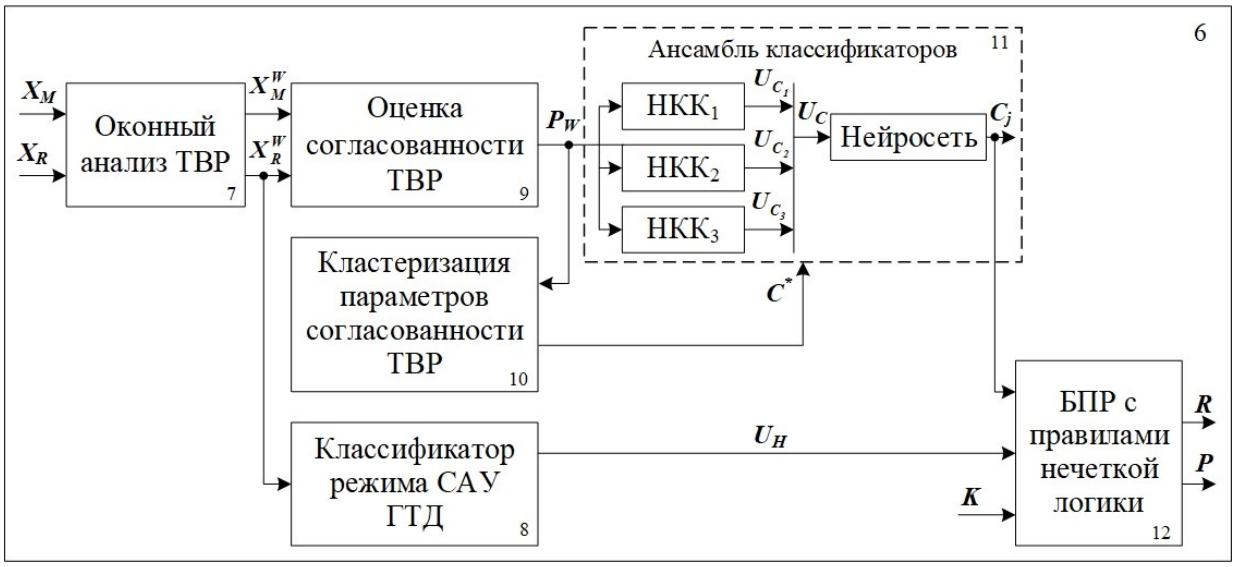


Рисунок 5.2 – Структурная схема системы, реализующей способ мониторинга целостности данных, полученных из модели САУ ГТД и летательного аппарата

Здесь X_M – вектор параметров состояния ГТД, полученных на основе модели (ТВР); X_R – вектор параметров состояния ГТД, полученных с борта ЛА (ТВР); X_M^W, X_R^W – набор отсчетов соответствующих ТВР, попавших в окно анализа; F_R^W – контактный вектор признаков состояния ГТД, полученный из многомерного технологического временного ряда (ТВР); P^W – вектор параметров согласованности ТВР X_M^W и X_R^W в окне анализа; $\{H_R^*\}$ – множество выделенных кластеров состояния ГТД; $\{H_R\}$ – сформированные классы состояния ГТД; U_H – вектор оценки вероятности принадлежности текущего набора отсчетов ТВР в окне

анализа к одному из выбранных классов состояния; $\{C_q^*\}$ – множество выделенных кластеров согласованности ТВР; $\{C_q\}$ – множество сформированных классов типов согласованности; U_C – вектор оценки вероятности принадлежности текущего вектора признаков согласованности любого из классов C_q; S_{CCS} – сигнал системы контроля; 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.

Блок оконного анализа ТВР (7) с помощью скользящего окна длиной W_S с шагом S формирует из исходных многомерных ТВР X_M и X набор матриц X_M^W, X_R^W признаков для определения текущего типа динамики САУ ГТД и дальнейшего анализа согласованности ТВР. Размер скользящего временного окна равен 100 временным отсчетам и подобран экспериментально.

Блок (8) реализует классификатор состояний модели САУ ГТД. На выходе блока формируется решение о том, в каком состоянии находится модель САУ ГТД: установившемся или переходном. Подробная схема блока (8) представлена на рисунок 5.3.

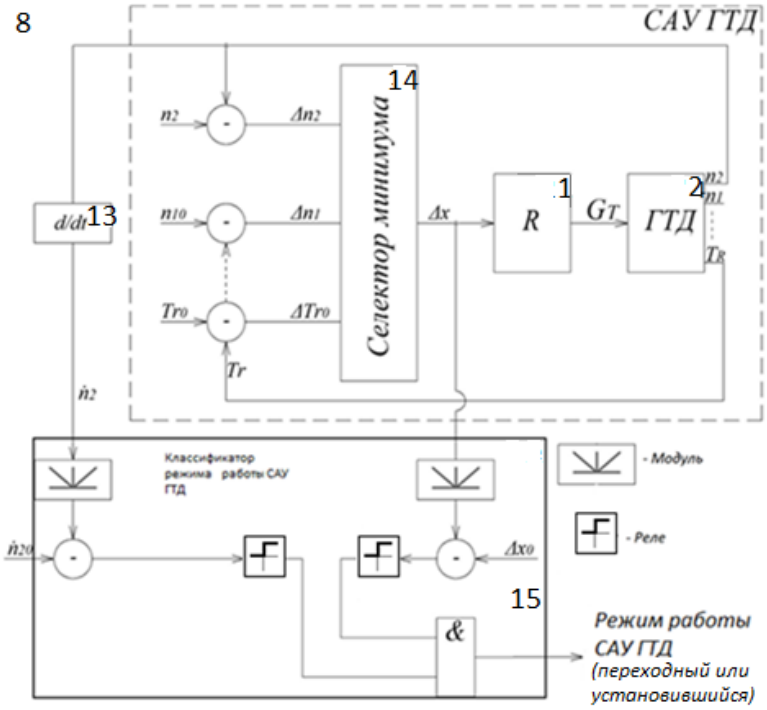


Рисунок 5.3 – Классификатор состояний модели САУ ГТД

Обозначения на рисунке 5.3 следующие:

n_1 – частота вращения ротора низкого давления

n_2 – частота вращения ротора высокого давления

$T_г$ – температура газа за турбиной

n_{10} – уставочное значение частоты вращения ротора низкого давления

n_{20} – уставочное значение частоты вращения ротора высокого давления

$T_{г0}$ – уставочное значение температуры газа за турбиной

Δn_1– разность между уставочным и действительным значениями частоты вращения ротора низкого давления

Δn_2 – разность между уставочным и действительным значениями частоты вращения ротора высокого давления

$\Delta T_г$ – разность между уставочным и действительным значениями температуры газа за турбиной

G_t – расход топлива

Δx – выход сектора минимума

$\dot{n}_2$ – производная частоты вращения ротора высокого давления

На вход классификатора 15 поступают производная частоты вращения 13 ротора высокого давления и сигнал с выхода селектора минимального значения 14 рассогласований управляемых параметров двигателя 2, являющегося элементом САУ ГТД [59], вычисляют абсолютные значения этих величин и сравнивают их с пороговыми значениями. Режим считается установившимся, если выполняется следующее условие:

$\{\lvert\Delta x\rvert \le x_0\} \wedge \{\lvert\dot{n}_2\rvert \le \dot{n}_{20}\}$	

где Δx – это выход сектора минимума,

$x_0 = 0{,}2\%$ от регулируемого в настоящий момент параметра,

$\dot{n}_2$ –это производная частоты вращения ротора высокого давления,

$\dot{n}_{20} = (0{,}05 - 0.1\%)\ \mathrm{n}_{2\ max}$ в секунду.

Если условие не выполняется, то режим САУ ГТД считается переходным. В случае, если в выбранном временном окне встречается и переходный, и установившийся, считают, что в данном окне САУ ГТД находится в переходном состоянии.

Блок (9) выполняет построение вектора P^W оценок согласованности многомерных ТВР в текущем окне анализа X_M^W, X_R^W с помощью набора метрик, указанных в таблице 5.2.

Таблица 5.2 – Метрики оценки согласованности многомерных ТВР в текущем окне анализа

№	Название метрики согласованности	Коэффициент	Параметры
1	Коэффициент корреляции	$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x}) \cdot (y_i - \bar{y})}{(n-1) \cdot S_x \cdot S_y}$	*X, Y* – две сравниваемые подпоследовательности ТВР равной длины, *n* – длина подпоследовательностей, $\overline{x}$, $\overline{y}$ – выборочные средние, S_x и S_y выборочные среднеквадратичные отклонения
2	Коэффициент детерминации	$R^2 = r_{xy}^2$	определяется по значению коэффициента корреляции
3	Средняя абсолютная ошибка, %	$MAPE = \frac{1}{n}\sum_{i=1}^{n}\frac{\lvert x_i - y_i \rvert}{x_i} \cdot 100\%$	
4	Евклидово расстояние	$x_{i\text{н}} = \frac{x_i - \bar{x}}{S_x}$, $y_{i\text{н}} = \frac{y_i - \bar{y}}{S_y}$ $d_E = \sqrt{\sum (x_{i\text{н}} - y_{i\text{н}})^2}$	$\overline{x}$, $\overline{y}$ – выборочные средние величин, S_x и S_y выборочные среднеквадратичные отклонения величин, $x_н$ и $y_н$ – нормированные величины

Данный вектор оценок согласованности позволяет делать вывод о текущем типе согласованности параметров модели и реального САУ ГТД для последующего принятия решения о возможных причинах выявленных расхождений в блоке принятия решений.

Блок (10) предназначен для автоматической классификации параметров согласованности ТВР X_M^W, X_R^W. В результате формируется совокупность кластеров $\{C*\}$ типов согласованности методом k-средних (k – means)/

В ходе анализа согласованности ТВР было выделено 7 кластеров, после чего была выполнена автоматическая классификация типов согласованности.

Блок (11) позволяет выполнить построение гетерогенного ансамбля нейронечетких классификаторов (ННК) типов согласованности на имеющихся данных $\boldsymbol{P^W}$.

Результирующий блок (12) основан на адаптивной нейро-нечеткой сети реализует принятие решения $\boldsymbol{R}$ о текущем состоянии системы и позволяет произвести оценку вероятности правильности принятого решения $\boldsymbol{P}$ о наличии одного из состояний согласованности данных модели и САУ ГТД: «Отказ САУ ГТД», «Нормальная работа», «Нарушение целостности».

5.1.2 Способ мониторинга целостности телеметрической информации на основе алгоритмов адаптивной сегментации ТВР

Способ мониторинга целостности данных, получаемых с эксплуатируемой САУ ГТД ЛА, основан на применении методов интеллектуального анализа многомерных технологических временных рядов параметров, характеризующих состояние ГТД, с использованием алгоритма адаптивного скользящего окна и оценки параметров согласованности ТВР. Блок принятия решений о состоянии канала передачи с борта ЛА на ПИ обеспечивает обработку ТВР, генерируемых САУ ГТД на эксплуатируемом ЛА, и производит сравнение этих данных с данными, генерируемыми моделью на ПИ.

Способ мониторинга целостности данных, получаемых с борта ЛА, включает следующие основные шаги:

1. формируется набор параметров САУ ГТД для анализа согласованности данных ТМИ, полученных с модели, и данных, полученных с борта ЛА;
2. формируется подпоследовательность многомерных параметров X, Y, $\boldsymbol{Y_M}$, $\boldsymbol{X_M}$, $\boldsymbol{X_M^W}$, $\boldsymbol{X_R^W}$ – наборы ТВР, созданные с помощью модели и полученные с борта ЛА – с помощью адаптивного скользящее окно длины W_S переменной длины;
3. выполняется расчет параметров согласованности одной, двух и трех пар ТВР (полученных с борта ЛА и генерируемых моделью) для каждой подпоследовательности, попадающей в скользящее окно анализа W_S;
4. строится многомерный технологический временной ряд (мТВР) P^W – параметры согласованности одной, двух и трех пар ТВР для каждой подпоследовательности, попадающей в скользящее окно анализа W_S;
5. на основе параметров согласованности ТВР и сигнала системы контроля принимается решение о целостности данных, полученных с ЛА;

Контроль целостности ТМИ базируется на анализе согласованности поведения параметров, полученных с помощью модели сложного технического изделия, и принимаемых с бортовых систем летательного аппарата. Выходом системы мониторинга является оценка вероятности событий нарушения целостности данных.

Структурная схема системы, реализующей способ мониторинга целостности данных, полученных из модели САУ ГТД и летательного аппарата, представлена на рисунке 5.4 и содержит в себе следующие блоки:

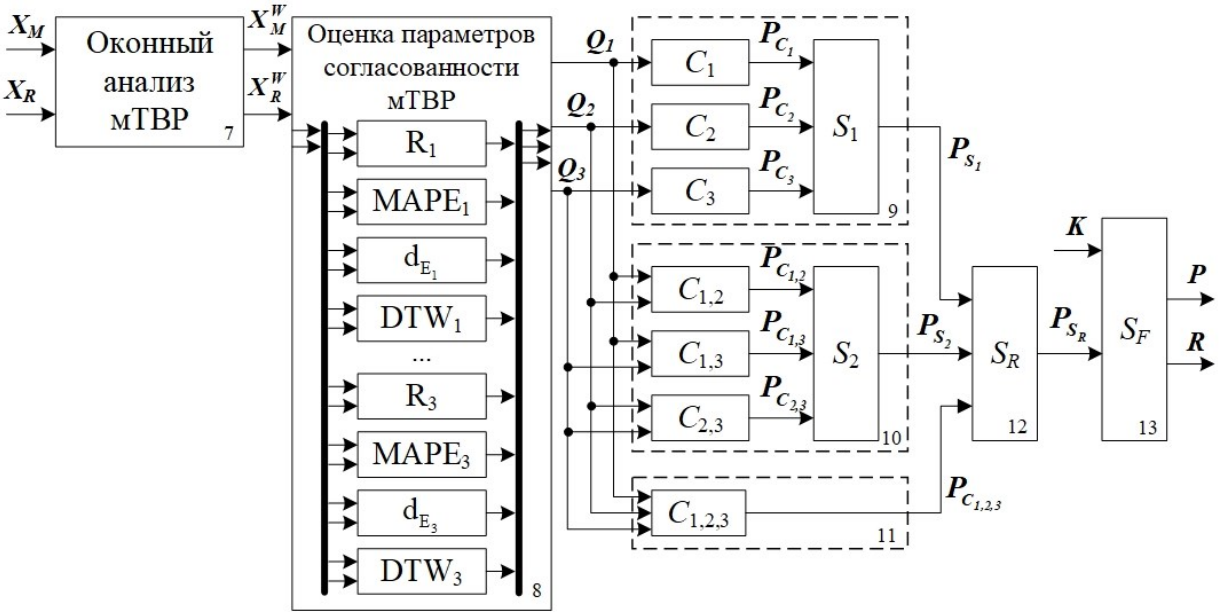


Рисунок 5.4 – Структурная схема системы, реализующей способ мониторинга целостности данных, полученных с помощью модели САУ ГТД и с борта ЛА

Блок оконного анализа ТВР (7) с помощью адаптивного скользящего окна длиной W_S с шагом S формирует из исходных многомерных ТВР X_M и X_R набор матриц X_M^W, X_R^W признаков для дальнейшего анализа согласованности ТВР. Размер скользящего окна анализа варьируется в диапазоне от 50 до 250 отсчетов и подбирается на этапе оптимизации параметров моделей-классификаторов блоков (9)-(12) экспериментально.

Блок (8) выполняет построение вектора P^W оценок согласованности трех пар ТВР в текущем окне анализа X_M^W, X_R^W с помощью набора метрик, указанных в таблице 5.2. Дополнительно вводится метрика, определяющая коэффициент оптимального пути трансформации временной шкалы, приведенная в таблице 5.3.

Таблица 5.3 – Метрики оценки согласованности многомерных ТВР в текущем окне анализа

№	Название метрики согласованности	Коэффициент	Параметры
1	Оптимальный путь трансформации временной шкалы	$DTW(X,Y) = \min_k \left\{ \frac{\sum_{k=1}^{K} d(w_k)}{K} \right\}$	d – матрица расстояний, $d(x_i, y_j) = (x_i - y_j)^2$ D – матрица трансформации $D_{i,j} = d_{i,j} + \min(D_{i-1,j}, D_{i-1,j-1}, D_{i,j-1})$

			W – путь трансформации (последовательность смежных элементов матрицы трансформации) длиной $n \le K < 2n$, $w_k = (i,j)_k, d(w_k) = d(x_i, y_j) = (x_i - y_j)^2$

Расширенный вектор оценок согласованности пары ТВМ используется для последующего принятия решения о возможных причинах выявленных расхождений в блоке принятия решений. Выход блока (8) включает трехкомпонентный вектор Q_1, Q_2, Q_3 – оценки согласованности для каждой из трех пар анализируемых ТВР.

Блоки (9), (10) и (11) предназначены для классификации параметров согласованности одной, двух и трех пар ТВР X_M^W, X_R^W. Блок (9) включает три независимых бинарных классификатора (C_1, C_2, C_3) на основе многослойных полносвязных нейронных сетей прямого распространения, каждый из которых решает задачу классификации оценок согласованности для сравниваемых пар ТВР на два класса: «нормальная работа», «атака». Блок S_1 в составе (9) на основе оценок (P_{C1}, P_{C2}, P_{C3}) вероятности наличия атаки, формирует оценку на основе линейной взвешенной комбинации:

$$P_{S_1} = \frac{w_1 \cdot P_{C_1} + w_2 \cdot P_{C_2} + w_3 \cdot P_{C_3}}{w_1 + w_2 + w_3},$$

весовые коэффициенты w_1, w_2, w_3, которой подбираются в процессе построения классификаторов.

Блок (10) включает три независимых бинарных классификатора ($C_{1,2}$, $C_{1,3}$, $C_{2,3}$) на основе многослойных полносвязных нейронных сетей прямого распространения, каждый из которых решает задачу классификации оценок согласованности для двух сравниваемых пар ТВР на два класса: «нормальная работа», «атака». Блок S_2 в составе (10) на основе оценок (P_{C12}, P_{C13}, P_{C23}) вероятности наличия атаки, формирует оценку P_{S2} на основе линейной взвешенной комбинации, весовые коэффициенты которой также подбираются в процессе построения классификаторов.

Блок (11) представляет собой бинарный классификатор (C_{123}) на основе многослойных полносвязной нейронной сети прямого распространения,

решающий задачу классификации оценок согласованности для трех сравниваемых пар ТВР на два класса: «нормальная работа», «атака».

Блок (12) позволяет сформировать взвешенную оценку в виде линейной взвешенной комбинации выходов блоков (9), (10) и (11).

Результирующий блок (13) основан на однослойной нейронной сети, реализует принятие решения ***R*** о текущем состоянии системы и позволяет произвести оценку вероятности правильности принятого решения ***P*** о наличии одного из состояний согласованности данных модели и САУ ГТД: «Отказ САУ ГТД», «Нормальная работа», «Нарушение целостности».

Построение ансамбля нейросетевых классификаторов поясняется с помощью схемы на рисунке 5.4.

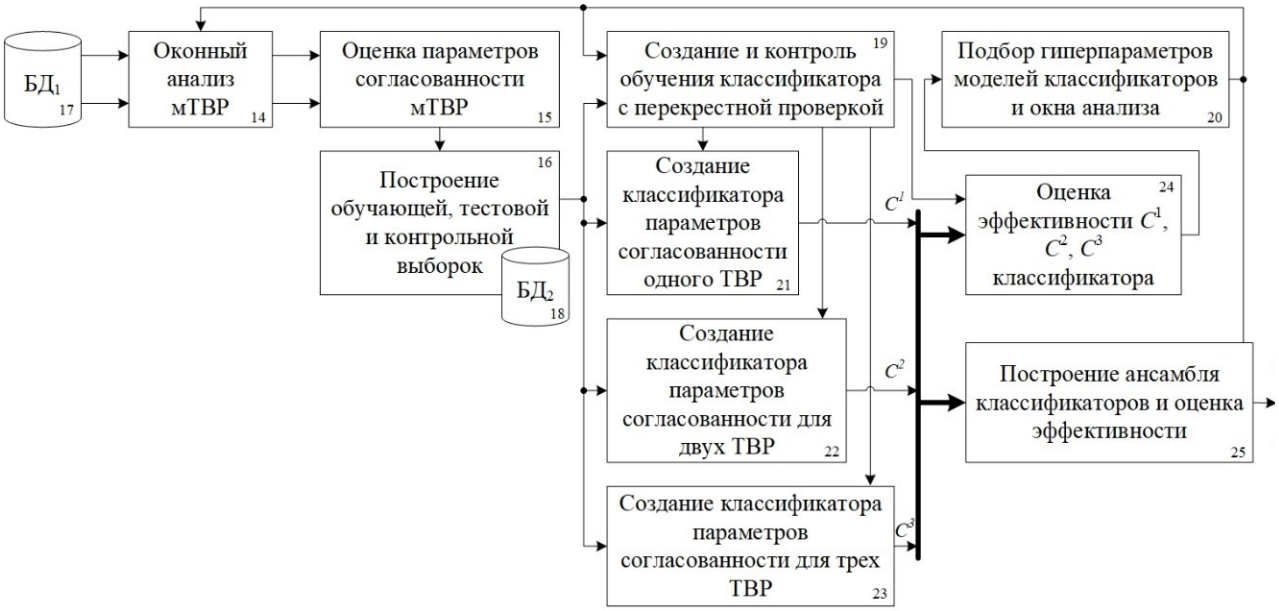


Рисунок 5.4 – Схема построения ансамбля нейросетевых классификаторов

$БД_1$ (17) содержит накопленные данные ТМИ, представляющие из себя два типа технологических временных рядов: ТВР, полученных с модели, и ТВР, полученных с борта ЛА. На ТВР, полученных с борта ЛА, накладывался шум, а также симулировались различные случаи нарушения целостности злоумышленником, согласно описанным в прототипе сценариям.

Накопленные данные подвергались адаптивному оконному анализу (14), длина скользящего окна W_S и шаг S рассматриваются как оптимизируемые гиперпараметры ансамбля классификаторов и подбираются с помощью поиска по сетке в процессе обучения с использованием алгоритма перекрестной проверки.

Все полученные в результате оконного анализа данные накапливаются в БД2 (18) в процессе построения обучающей, тестовой и проверочной выборок (16). Создаются группы бинарных нейросетевых классификаторов для пар ТВР, получаемых с модели САУ ГТД и с борта ЛА:

- три классификатора, каждый из которых в качестве входного вектора признаков использует параметры согласованности Q_1, Q_2 или Q_3 отдельных пар ТВР – C^1 (21),
- три классификатора, каждый из которых в качестве входного вектора признаков, использующих параметры согласованности ($\{Q_1, Q_2\}$, $\{Q_1, Q_3\}$, $\{Q_2, Q_3\}$) двух пар ТВР – C^2 (22);
- классификатора, в качестве входного вектора признаков, использующего параметры согласованности $\{Q_1, Q_2, Q_3\}$ трех пар ТВР – C^3 (23).

Блок (19) обеспечивает контроль и предотвращает переобучение нейросетевых моделей отдельных классификаторов, а также позволяет с помощью алгоритма перекрестной проверки оценить обобщающую способность отдельных классификаторов.

Блок (24) обеспечивает оценку эффективности ансамбля на основе подбора коэффициентов линейной взвешенной суммы выходов каждого из классификаторов для параметров согласованности одной, двух и трех ТВР. Блок (20) обеспечивает оптимизацию гиперпараметров ансамбля нейросетевых классификаторов: коэффициентов линейной взвешенной суммы одиночных участников, параметров архитектуры каждой из нейронных сетей, параметров адаптивного оконного анализа исходных ТВР – с помощью алгоритма перебора по сетке.

Блок (25) позволяет оценить качество бинарной классификации ансамбля моделей и сохранить в $БД_3$ весовые коэффициенты и подобранные параметры наилучшего из построенных решений.

Итак, предложенные способы и система позволяют выявлять несанкционированные воздействия на данные о состоянии САУ ГТД и тем самым повысить уровень защиты информации при ее передаче с борта ЛА на предприятие-изготовитель.

5.2 Мониторинг целостности наблюдаемых параметров технологического процесса на основе технологий интеллектуального анализа данных

Рассматриваемое предприятие, на котором производится полиэтилентерефталат, относится к категории опасных производственных объектов согласно Федеральному закону № 116-ФЗ. Предлагается создание системы мониторинга ТП получения полиэтилентерефталата на основе математической модели технологического процесса, рассмотренной в [130].

Исходными данными для анализа являются следующие параметры:

- Давление на входе насоса $p_{\text{вс}}$;
- Скорость вращения ротора n;
- Силы тока I на электродвигателе насоса от датчика.

Известен способ измерения вязкости данной жидкости (5.1):

$$\mu(t) = A \cdot \frac{I}{n} + B \cdot p_{\text{вс}} + \text{C} \qquad (5.1)$$

где A, B, C – постоянные коэффициенты;

$p_{\text{вс}}$ – давление на входе, Па;

n – скорость вращения ротора, об/мин;

I – сила тока на электродвигателе насоса, А.

По измеренным значениям режимных параметров $n, p_{\text{вс}}, I$ рассчитывают характеристическую вязкость μ контролируемой жидкости при измеряемой температуре. В вычислительном устройстве производиться вычисление значения вязкости μ. Контроль вязкости выполняется непрерывно в динамическом режиме. Измеренные значения со всех датчиков поступают в диспетчерскую систему сбора и управления технологическим процессом.

Разработана структурная схема системы мониторинга ТП производства полиэтилентерефталата в составе системы обнаружения вторжения (рис. 5.7).

Структурная схема системы мониторинга ТП производства состоит из шести взаимосвязанных друг с другом блоков. Первый блок – блок подготовки данных ТВР, на который подается временной ряд параметров технологического процесса, и происходит формирование данных для дальнейшей работы с ними. Следующий блок – блок построения математической модели технологического объекта на основе анализа ТВР, в основу которого положена NARX модель, позволяющая учитывать нелинейные процессы смена типа динамики. Третий блок –

это блок анализа ТВР. В данном блоке происходит адаптивная сегментация временного ряда и объединение похожих сегментов по типам с помощью метода кластеризации k-means.

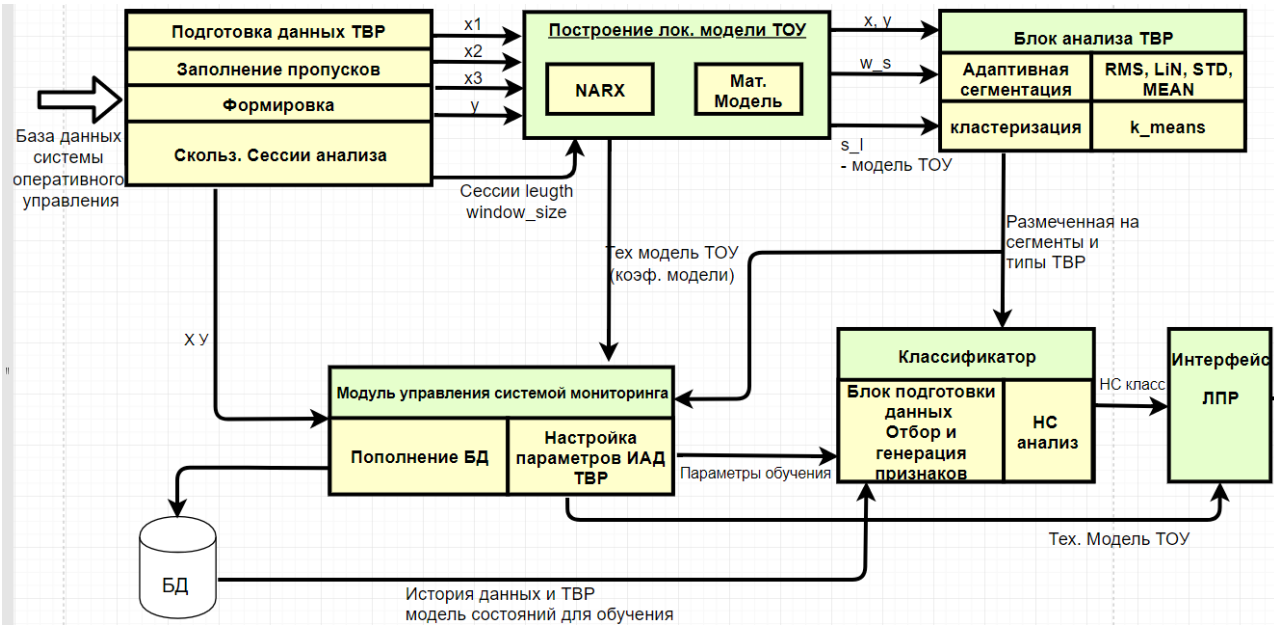


Рисунок 5.7 – Структурная схема системы мониторинга ТП в составе системы защиты информации в сегменте сети АСУ ТП

Четвертый блок – модуль управления системой мониторинга. В него поступают данные с первых трех блоков, он является связующим звеном передачи информации в БД для хранения, и подачи информации (параметров обучения) на следующий блок – блок классификатор для выявления известных типов событий на объекте. Задача данного классификатора – классифицировать для каждого типа сегментов события, происходящие на объекте, в том числе, обнаружение нарушения целостности данных о ходе ТП в виду их несанкционированной модификации).

5.2.1 Проведение эксперимента на натуральных данных о ходе ТП

На основе данных о ходе ТП производства полиэтилентерефталата за год, а именно вязкость, сила тока, скорость вращения ротора и давление всасывания – $y(t), u_1(t), u_2(t), u_3(t)$ был проведен эксперимент по построению нейросетевой модели обнаружения нарушений целостности, вызванных, в том числе, воздействием злоумышленника. Точность классификатора на тестовой выборке составила 87,99%.

Количество ошибок отдельных классификаторов для тестовой выборки представлено на рисунке 5.8.

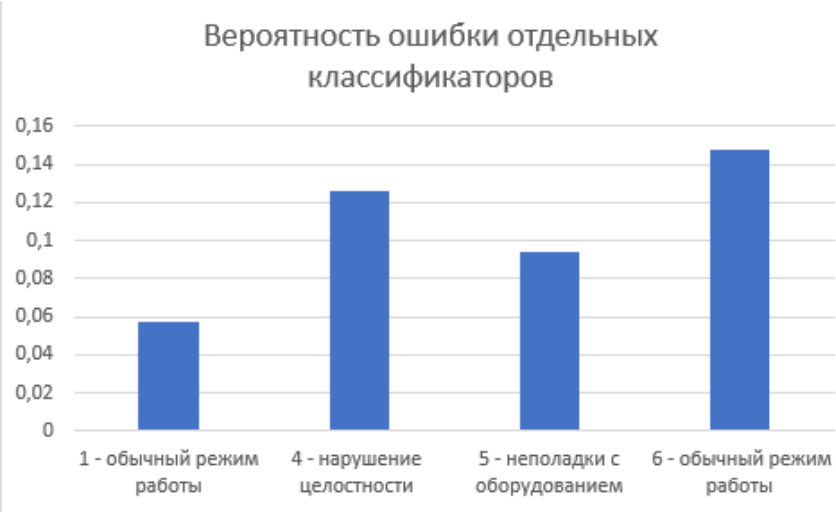


Рисунок 5.8 – Ошибки классификаторов

Таким образом, для тестовой выборки точность классификатора составила 87,99%, а вероятность ошибки отдельных классификаторов типов не превышает 14%.

Можно сделать вывод, что реализация данной системы мониторинга ТП на основе технологии искусственного интеллекта повысит степень защищённости результатов измерений от несанкционированной модификации в базах данных информационных систем промышленного предприятия.

5.3 Оценка рисков ИБ киберфизических объектов на основе прогнозирования и обнаружения аномалий их состояния

Предложенный исследователями из Южной Кореи (Institute of ETRI, Daejeon, South Korea) [168, 282] набор данных собран в ходе эксплуатации стендовой АСУ ТП и дополнен результатами программно-аппаратного моделирования (HIL) генерации энергии паровой турбиной и процесса гидроаккумулирования. Целью является исследование методов и алгоритмов обнаружения аномалий в таких киберфизических системах, как паровые турбины, водоочистные сооружения и электростанции. Первоначально были запущены три испытательных стенда: стенд турбины General Electronics, стенд паровых котлов Emerson и стенд MPS FESTO для водоочистки. Затем была построена система, которая объединила эти три стенда с программно-аппаратным симулятором, имитирующим выработку тепловой и гидроаккумулирующей энергии. Первая версия набора данных содержит нормальные и аномальные ситуации, соответствующие 34

сценариям атак [168, 169, 207, 282]. Результаты эксперимента приведены в Приложении Ж.

Особенностями предложенного подхода к построению ансамбля детекторов аномалий по сравнению с аналогичными исследованиями является:

- использование моделей, не требующих разметки на классы нормального и аномального функционирования, что потенциально позволяет обнаруживать аномалии, вызванные новыми типами атак злоумышленника;
- использование исходных обучающей и тестовой выборок, предложенных авторами набора данных HAI 2.0, без их объединения и утечки данных о природе аномалий из тестовой в обучающую выборку;
- возможность работы с несбалансированной выборкой как в отношении бинарной классификации (нормальная работа – аномалия), так и в задаче обнаружения отдельных типов атак;
- отсутствие допущений о периодичности и длительности атак на этапе тестирования модели, поскольку допущение, подобные [157], позволили для тестовой выборки уменьшить количество ложноположительных срабатываний более чем в 10 раз и получить уровень оценки метрики F1 = 0,9781 по сравнению с F1 = 0,977 в [157];
- итоговая оценка качества обнаружения (метрики оценки обнаружения аномалии и корректности границ аномалии во временных рядах) для композиции детекторов составляет TaR = 0,993, TaP = 0,915, что сравнимо (метрика TaR) и превосходит (метрика TaP) лучшие результаты исследователей [157] TaR = 0,968 и TaP = 0,805.

Корректность обнаружения аномалий первого типа с помощью гетерогенной модели детекторов составила 69%, второго типа – 78%, третьего типа – 80% с применением постфильтрации результатов на основе эвристик длительности и периодичности атак. Дальнейшая работа по подбору параметров глубины погружения в историю ВР параметров объекта и оптимизация архитектуры нейросетевого автоенкодера позволит добиться лучших результатов, снижая количество ложных срабатываний. Перспективной является гетерогенная архитектура нейросетевого автоенкодера и модели LOF, а также добавление еще одного выходного фильтра, позволяющего учитывать временные особенности реализации атак и длительность вызванных изменений в наблюдаемых параметрах.

Для выявления сложных атак злоумышленников, получивших доступ с сеть промышленного объекта, необходимо применение методов и инструментов расширенной аналитики данных, позволяющих выполнять оперативный анализ и выявление скрытых признаков злонамеренной активности на основе модели наблюдаемого КФО. Для построения модели обнаружения аномалий состояния КФО, вызванных действиями злоумышленника в промышленной сети в ходе реализации сложной сетевой атаки, нами был использован доступный набор данных, который был собран в ходе испытаний АСУ ТП промышленного объекта и дополнен результатами программно-аппаратного моделирования.

Разработан алгоритм интеллектуального анализа технологических временных рядов в задаче обнаружения аномалий наблюдаемых параметров состояния объектов АСУ ТП. Обнаружение аномалий по всем типам составило в среднем 65 % (первого типа – 69 %, второго типа – 78 %, третьего типа – 80 %) при принятии допущений о периодичности и длительности атак, что свидетельствует об эффективности решения поставленной задачи. Дальнейшее развитие фильтрации ложноположительных срабатываний на основе анализа временных характеристик потенциальных атак позволит повысить эффективность предлагаемого ансамбля детекторов.

5.4 Повышение безопасности эксплуатации инженерных сетей нефтедобывающего предприятия с использование методов ИАД

Целью является повышение безопасности эксплуатации инженерных сетей нефтедобывающего предприятия за счет повышения эффективности алгоритмов обработки диагностической информации в задаче выявления вмешательства злоумышленника в ход технологического процесса на основе ИАД.

Для достижения этой цели разработана диагностическая модель распознавания ситуаций на основе анализа технологических временных рядов, характеризующих технологический процесс добычи нефти в реальном масштабе времени. Модель основана на сопряжении подсистемы адаптивной сегментации ТВР и подсистемы нейросетевого нечеткого композиционного вывода в задаче обнаружения аномалий, вызванных вмешательством злоумышленника в ход технологического процесса.

Объектом анализа является инженерная сеть нефтедобывающего предприятия, которая представляет собой совокупность взаимосвязанных

технологических объектов добычи, сбора, подготовки, приема и сдачи продукции в совокупности со средствами измерения и управления [89].

Для дальнейшего анализа использованы временные ряды, описывающие давление на выходе узла и суммарный расход нефти. Анализ временных рядов с помощью однородных нейросетевых структур предпочтительнее, чем поэтапное построение многоуровневой системы обработки. Недостатками метода являются сложность и неформализуемость подбора параметров каждого из алгоритмов и излишняя сегментация исходного сигнала. Это ведет к частому переключению сигнализирующей о типе текущей динамики системы. Методы M_2 и M_3 позволяют сократить количество настраиваемых параметров и автоматизировать процесс построения нейросетевой системы. Использование данных методов позволяет избежать излишней сегментации и переключения сигнализирующей системы, а также расширить количество выделяемых классов событий, путем обнаружения переходных состояний, что видно из результатов, приведенных в таблице 1. Ошибка I рода – ложное распознавание. Ошибка II рода – пропуск события.

Таблица 5.5 – Результаты сегментации ТВР «Давление-Расход»

Метод	**Успешная классификация подвижным окном известных событий %, I/II ошибки, %**		**Успешная классификация подвижным окном смеси известных и неизвестных событий %, I/II ошибки, %**	
M_1	78,7		61,9	
	15,4	5,9	28,7	9,4
M_2	82		69	
	8,1	9,9	11,4	19,6
M_3	87		73	
	4,1	8,9	7,6	19,4

Таким образом, в ходе анализа результатов моделирования и оценки эффективности предлагаемой модели показана эффективность применения моделей M_2 и M_3 в составе интеллектуальной системы обработки диагностической информации.

Исходя из технологической легенды и экспертной информации для описываемых временных рядов расхода и давления на объекте, определены следующие количественные характеристики (таблица 5.6).

Таблица 5.6 – Количественные характеристики технологической легенды временных рядов «Давление» и «Расход»

Характеристика	**Экспертная оценка**	**Разработанная система**
Количество выявленных событий	50	230
Количество классов выявленных событий	8	29
Процент успешного распознавания выявленных событий	70	73
Количество классов, выявленных событий, включающих события нарушения целостности накапливаемых данных	5	5
Процент успешного распознавания выявленных событий нарушения целостности накапливаемых данных		81

Экспертная оценка позволяет выявить в исследуемых ТВР около 50 событий, нашедших отражение в технологической легенде. Из них 25 являются событиями, связанными с нарушением хода ТП. Общее количество событий распределено по 8 классам, из которых события, связанные с нарушением хода ТП, образуют 5 классов, включая класс событий, связанных с нарушением целостности накапливаемых параметров. Существующая система выделяет порядка 10 классов событий, а предлагаемая модель – 29. Диагностическая модель позволяет увеличить количество регистрируемых классов технологических событий на 30% путем введения субклассов, характеризующих промежуточные состояния, и дополнительных классов, описывающих похожие участки с близкими динамиками, что находит частичное отражение в технологической легенде.

Главной задачей эксперта является выявление и анализ ситуаций нарушения хода ТП. При анализе исторических данных сформировано 25 классов подобных событий. Определен временной интервал t = 20 отсчетов, в течение которого успешное распознавание события нарушения хода ТП и соответствующее управляющее решение могут значительно снизить ущерб (утечку, выход из строя оборудования и т.п.). В таблице 5.7 приводятся количественные характеристики, описывающие временные параметры выявляемых технологических событий (ТС), как-то:

– показатель эффективности описания события – отношение длины выделенных сегментов, характеризующих ТС, и длины участка временного ряда, описывающего ТС по легенде (усреднено по всем прецедентам, величина безразмерная);

$k = \frac{1}{n}\sum_{n}\frac{S_L^f}{S_L^d}$	

S_L^f – длина n-го найденного сегмента, характеризующего данное технологическое состояние;

S_L^d – длина n-го сегмента, характеризующего данное технологическое состояние согласно легенде

– время реакции – время запаздывания (по модулю) от начала ТС по легенде до начала соответствующего выделенного сегмента, описывающего ТС (усреднено по всем прецедентам, измеряется в отсчетах).

Таблица 5.7 – Количественные характеристики технологической легенды временных рядов «Давление» и «Расход»

Характеристика	**Существующая система**	**Разработанная система**
Показатель эффективности описания ТС, k	0,65	0,73
Время реакции, отсчетов	25	19

Как видно из таблицы, существующая система имеет на 10% большую погрешность описания ТС, и 24% худшее время реакции.

Использование диагностической модели и разработанных алгоритмов анализа ТВР, позволяет разрабатывать комплексные системы поддержки принятия решений, нацеленные на повышение безопасности эксплуатации объектов нефтедобывающего предприятия за счет снижения роли человеческого фактора при принятии решений в нештатных и аварийных ситуациях, связанных, в том числе, с воздействием злоумышленника на объекты промышленной сети.

5.5 Обнаружение сетевых атак в гетерогенной промышленной сети на основе технологий машинного обучения

Для повышения защищенности гетерогенной промышленной сети разработаны **система обнаружения сетевых атак в гетерогенной сети промышленного** и **алгоритм** интеллектуального анализа сетевого трафика **[142, 209, 255, 256, 276, 278, 285, 305, 306]**.

Для создания моделей машинного обучения (ML-моделей) используются общедоступные размеченные по типам атак и режимам работы базы сетевого трафика. Для обнаружения новых сетевых атак, реализуемых с помощью постоянно развивающегося инструментария злоумышленников, необходимо

периодическое обновление тренировочных наборов с реализацией новых сценариев атак и фиксацией параметров их проведения для дообучения ML-моделей.

Структурная схема системы обнаружения сетевых атак в гетерогенной сети промышленного Интернета вещей на основе интеллектуального анализа данных представлена на рисунке 5.9.

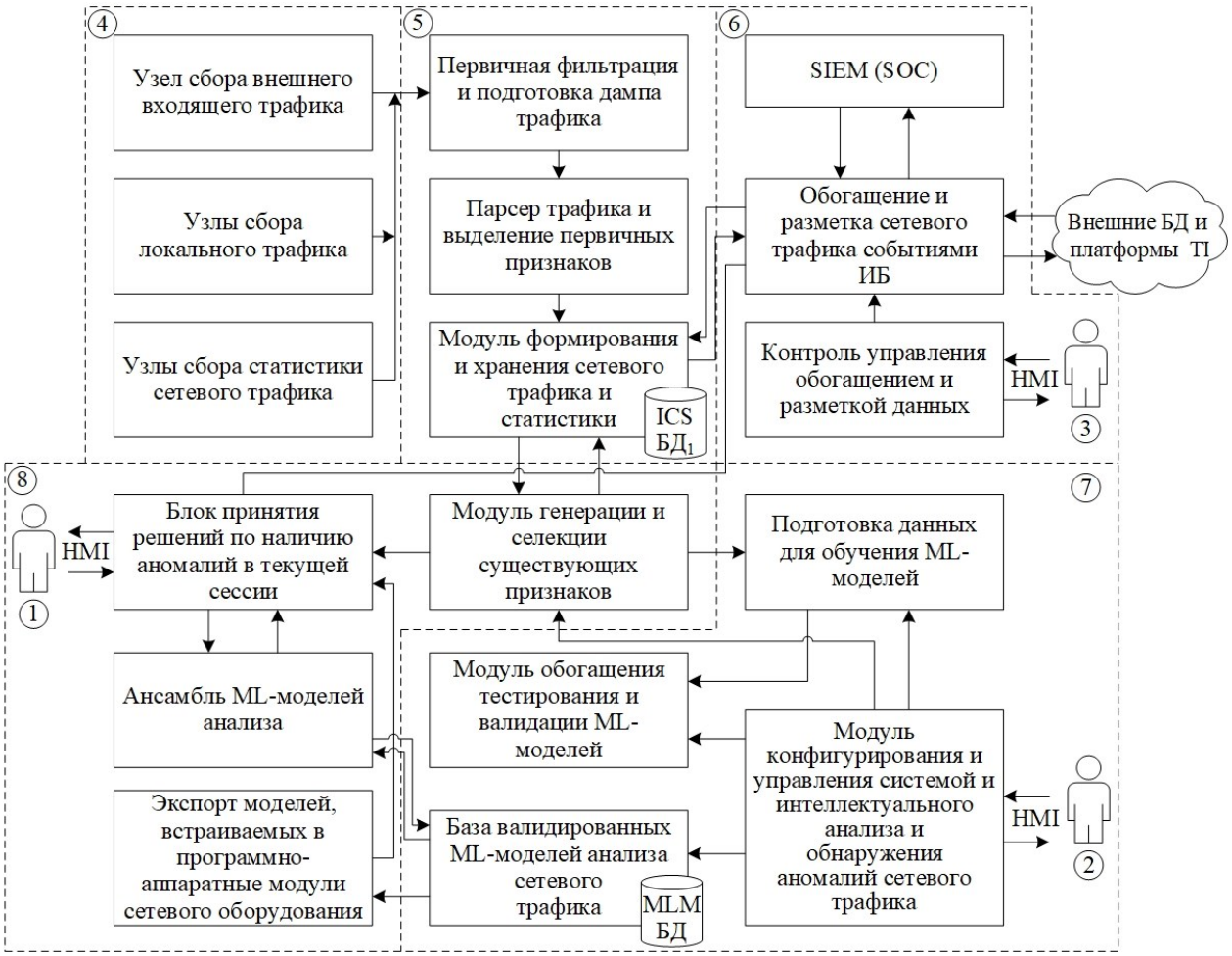


Рисунок 5.9 – Структурная схема системы обнаружения сетевых атак на основе интеллектуального анализа данных, HMI – Human-machine interface, человеко-машинный интерфейс, платформа TI (Threat Intelligence) – платформа управления данными кибербразведки

Коллектор (4) сетевых сессий собирает параметры трафика с агентов, установленных в ключевых точках сетевой инфраструктуры: агрегирующих коммутаторах, пограничном межсетевом экране, с точек доступа в виде дампа трафика канального уровня и в формате сессий (семейство протоколов netFlow). Модули (5) предобработки, выделения признаков и хранения статистики сетевого трафика позволяют фиксировать в долгосрочном хранилище (ICS БД) компактное описание сетевых сессий, что позволяет проводить ретроспективный анализ накопленных данных и оперативное обновление индикаторов компрометации при взаимодействии (6) с внешними платформами кибербразведки. Модуль

анализа и генерации признаков (8) используется при подготовке размеченных данных для построения и обучения моделей машинного обучения, сохраняемых в БД (MLM БД) для дальнейшего использования при оперативном анализе входящего и внутреннего сетевого трафика.

Модуль обогащения, тестирования и проверки ML-моделей позволяет провести дополнительную разметку сетевого трафика, связав определенные события ИБ с соответствующими сетевыми сессиями.

Оперативное двухстороннее взаимодействие системы в целом с подсистемой управления событиями безопасности и центром мониторинга ИБ и реагирования на инциденты (SIEM (SOC)) позволяет передавать метрики и дополнительную информацию о параметрах текущего состояния сети для последующей агрегации и анализа. Процессом разметки (обогащения) записей сетевых сессий управляет специалист (3) по сетевой безопасности текущего сегмента.

Специалист по интеллектуальному анализу данных (2) управляет работой ансамбля ML-моделей, выполняет задачи по корректировки параметров его работы и своевременного обновления банка моделей.

Обобщенный алгоритм интеллектуального анализа параметров сетевого трафика в задаче обнаружения аномалий и вредоносной сетевой активности изображен на рисунке 5.10. Представлены основные этапы сбора и обработки данных для построения и использования ML-моделей.

Предлагаемый алгоритм интеллектуального анализа сетевого трафика применялся для анализа следующих наборов данных (таблица 5.12).

Таблица 5.12 – Анализируемые наборы данных сетевого трафика

Набора данных	Количество сетей (кластеров)	Длительность сбора данных/число записей	Классы атак	Инструменты извлечения признаков	Ко-во признаков	Детальное описание эксперимента
NSL-KDD [280]	2	5 недель / 148517	4	Bro-IDS	41	[276]
CICIDS2017 [253]	1	5 дней / 2830540	15	CICFlowMeter	84	[306]
UNSW-NB15 [295]	33	16 дней 15 часов / 2059419	9	Argus, Bro-IDS и другие	47	[199]
WUSTL-IIOT-2018 [243]	1	25 часов / 7037983	5	ARGUS	4	[305]
WSN-DS-2016 [144]	5	1 день / 374661	4	LEACH protocol	19	[25]

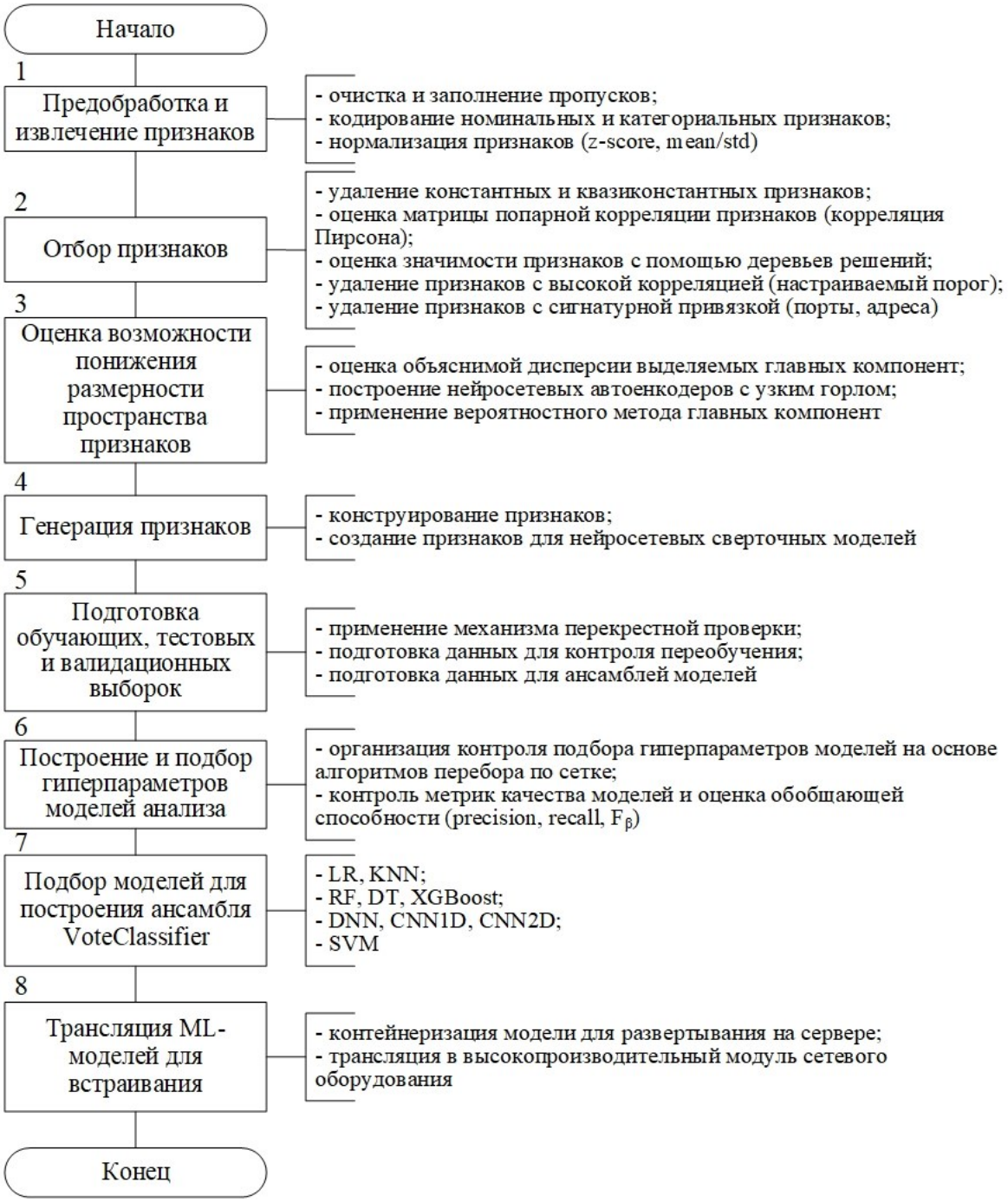


Рисунок 5.10 – Обобщенный алгоритм интеллектуального анализа сетевого трафика в задаче обнаружения аномалий и вредоносной сетевой активности

Специфика реализации алгоритма для каждого из наборов данных (таблица 5.12) приведена в Приложении З.

После подбора параметров классификаторов и выбора ML-моделей, продемонстрировавших приемлемую обобщающую способность, выполняется итоговая оценка моделей. По сочетанию времени, затрачиваемого на обучение модели, суммарного количества настраиваемых параметров модели, показателей F-1 меры и правильности (Acc – Accuracy) итоговой модели на тестовой выборке выбран классификатор на основе комитета деревьев решений (Таблица 5.13).

Таблица 5.13 – Результаты тестирования классификатора

Классификатор	CICIDS2017		NSL-KDD		UNSW-NB15		WUSTL-IIOT-2018		WSN-DS-2016	
	Acc	F-1	Acc	F-1	Acc	F-1	Acc	F-1	Acc	F-1
RF	0,967	0,910	0,896	0,885	0,897	0,810	0,999	0,919	0,999	0,947

Одни из лучших результатов показывают классификаторы XGBClassifier, Случайный лес и нейросетевые модели. В абсолютном значении лучшую эффективность показал VotingClassifier.

Обученные ML-модели RF и MLP предлагается использовать в виде встраиваемых программных модулей соответствующего сетевого оборудования. С помощью транслятора с языка Python созданы заголовочные файлы и файлы реализации на языке C с выгрузкой коэффициентов обученных моделей в качестве статических параметров. Дальнейшая компиляция с помощью кросс-компилятора позволила собрать исполняемые модули для платформы ARM семейства специализированных процессоров NXP LX2160A.

Разработана и описана структурная схема системы обнаружения сетевых атак на основе интеллектуального анализа данных.

Разработаны алгоритмы интеллектуального анализа параметров сетевого трафика в задаче обнаружения вредоносной сетевой активности. Приведена общая схема алгоритма. Проанализированы варианты построения ансамблей и комитетов классификаторов на основе традиционных моделей машинного обучения (модели случайного леса, рандомизированные деревья решений и пр.) и гетерогенных нейросетевых моделей (глубокие нейронные сети, сверточные нейронные сети и модели на основе автоенкодеров с долгой краткосрочной памятью).

5.6 Система автоматического профилирования действий пользователя

В составе системы автоматического профилирования (профайлинга) (рисунок 5.12) предложена обобщенная схема модуля видеоаналитики, позволяющего [26, 48, 49]:

1) анализировать тип двигательной активности оператора. Оценка эффективности программной реализации показала корректность классификации паттернов активности в 97 % случаев;

2) выполнять функции нейросетевой системы идентификации и аутентификации пользователя.

Итоговый блок принятия решений (14) позволяет оценить степень уверенности композиции классификаторов в типе распознаваемого образа (аутентификация на основе изображения лица), динамике движений субъекта (распознавание типа движений, жестов), типе психоэмоционального состояния и передать сформированный закрытый ключ в блок криптографической системы.

В функции подсистемы автоматического профайлинга также входит анализ информационного почерка пользователя (динамический профиль пользователя на основе анализа клавиатурного почерка), позволяющего выполнять процедуру непрерывной скрытой идентификации и аутентификации. Разработан алгоритм кодирования вектора признаков, характеризующих клавиатурный почерк пользователя с последующей унификацией пользовательских шаблонов на основе применения вейвлет-преобразования Хаара. Предложена модульная структура нейросетевого классификатора, корректно определяющая пользователя в 98 % случаев.

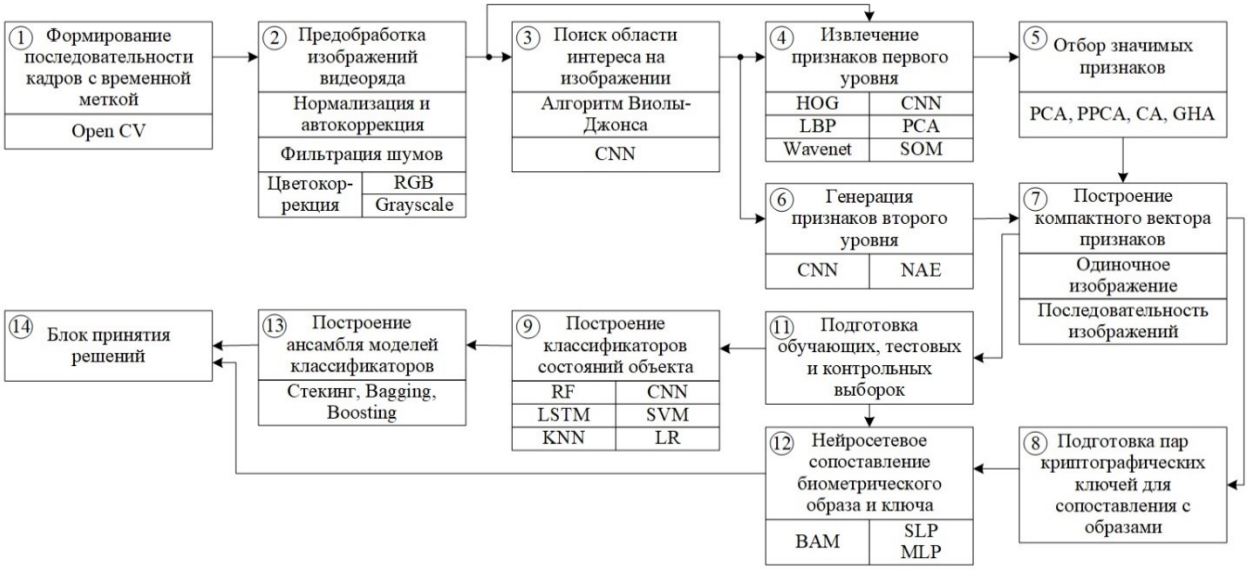


Рисунок 5.12 – Структура системы автоматического профилирования действий пользователя

Приняты следующие обозначения для структурных элементов схемы: 1 – видеоряд с привязкой к отметкам времени; 2 – нормализованный видеоряд с двумя цветовыми палитрами (RGB и Greyscale); 3 – силуэт человека; лицо человека (ROI – region of interest); ROI силуэта человека в видеоряде с привязкой к метке времени; ROI лица человека с привязкой к метке времени; 5 – компактный вектор признаков (ключевые точки скелета + ключевые точки лица); 6 – специалист по извлечению и представлению знаний; 7 – вектор оценок принадлежности объекта к возможным классам состояний, полученный набором

классификаторов (RF – Random Forest, классификатор на основе «случайного леса», CNN – Convolution Neural Network, классификатор на основе сверточной нейронной сети, SVM – Support Vector Machine, классификатор на основе машины опорных векторов, KNN – k-Nearest Neighbor, классификатор k-ближайших соседей); 8 – лицо, принимающее решение; 9 – системный администратор; БПР – блок принятия решения; HMI – Humane Machine Interface, человеко-машинный интерфейс; PCA – Primary Component Analysis, метод главных компонент; HOG – Histogram of Oriented Gradients, гистограмма ориентированных градиентов; LBP – local binary patterns, локальные бинарные шаблоны.

5.6.1 Подсистема интеллектуального анализа видеоданных в системе профилирования пользователя

Использование [48] интеллектуальных камер и датчиков в системах видеоаналитики в сочетании с человеком-оператором, с которого снята большая часть аналитической и зрительной нагрузки, позволяет увеличить эффективность видеонаблюдения и, как результат, повысить безопасность и результативность труда на производстве в целом.

Алгоритм распознавания позы человека представлен на рисунке 5.13:

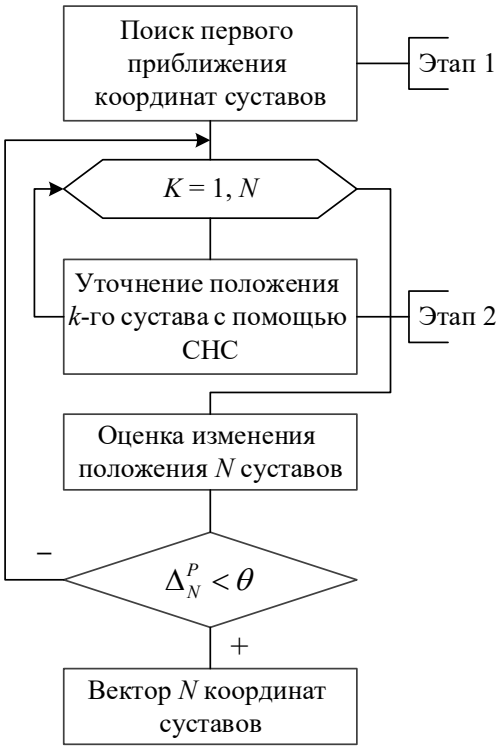


Рисунок 5.13 – Схема алгоритма распознавания позы

N – количество ключевых точек – суставов; Δ_N^P – область локализации k-го сустава, сравниваемая с пороговым значением θ

Схема алгоритма классификации человека по выделенному изображению лица на два класса «свой-чужой» представлена на рисунке 5.14.

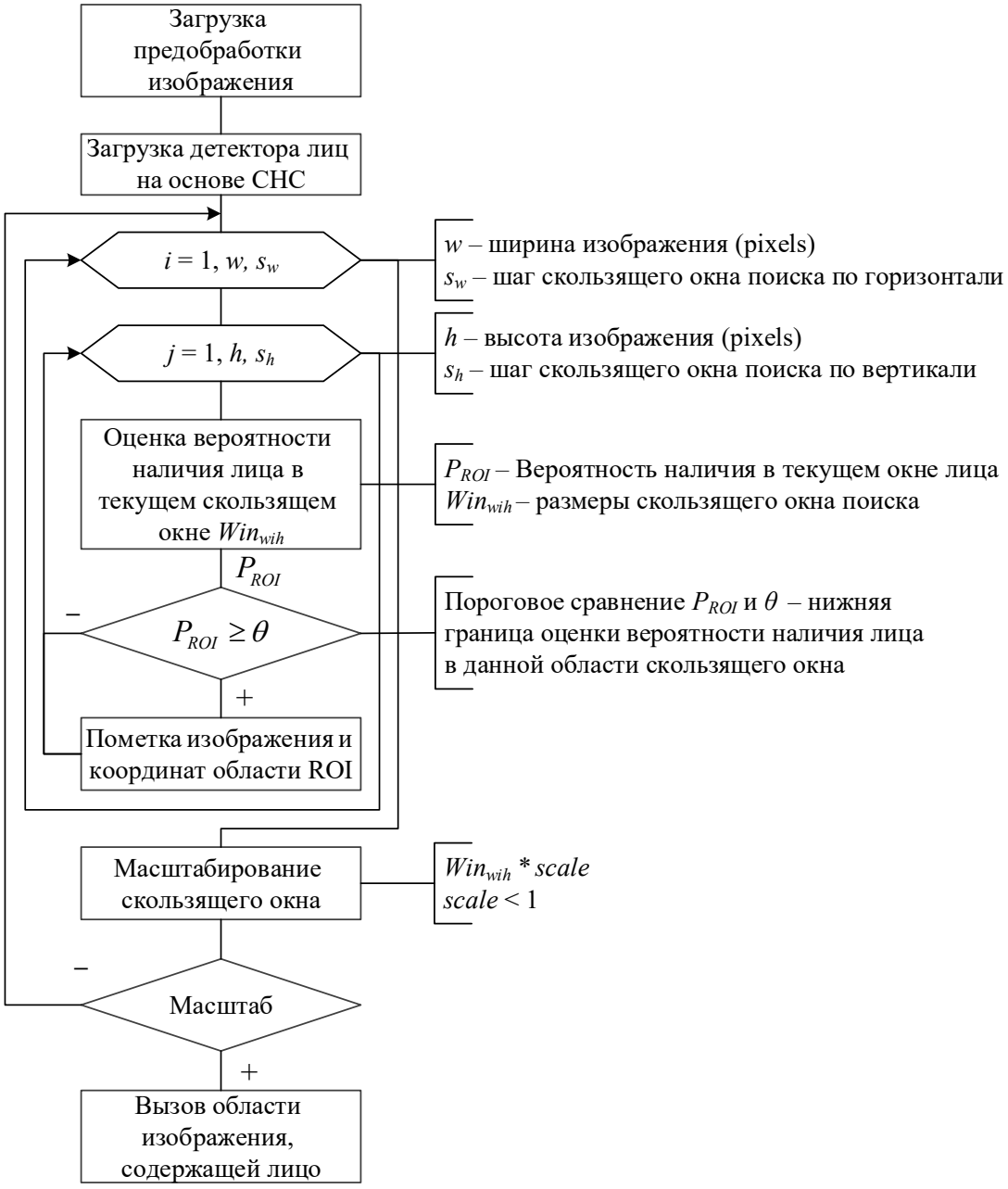


Рисунок 5.14 – Схема алгоритма распознавания лица. СНС – сверточная нейронная сеть

Оценка эффективности программной реализации алгоритмов анализа видеоданных на натурных данных показала корректность классификации в 97 % случаев после обобщения результатов перекрестной проверки.

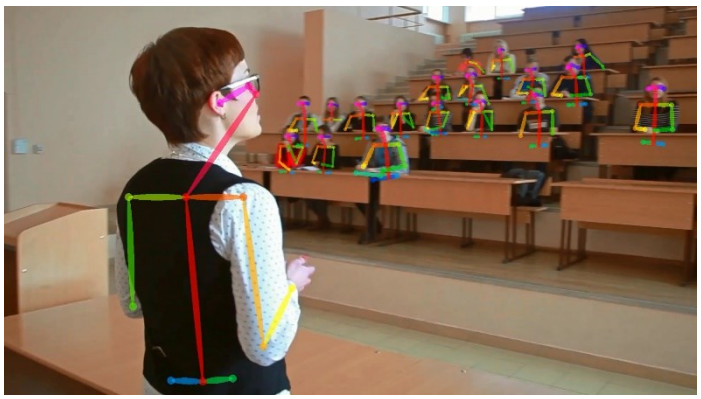


Рисунок 5.15 – Распознавание позы с помощью библиотеки OpenPose

Для снижения размерности вектора признаков в задаче идентификации по изображению лица применялся метод главных компонент для сжатия размерности пространства признаков. Оценка точности классификации 5 субъектов на два класса «свой» и «чужой» производилась методом перекрестной проверки и составила 99 % на тестовой выборке.

Оценка эффективности программной реализации алгоритмов анализа натурных видеоданных показала корректность классификации в 97 % случаев. Оценка эффективности классификации 5 субъектов на два класса «свой» и «чужой» производилась методом перекрестной проверки и показала точность 99 % на тестовой выборке.

5.6.2 Подсистема интеллектуального распознавания эмоционального состояния пользователя на основе анализа видеоданных в системе профилирования пользователя

Для повышения эффективности системы мониторинга состояния оператора за счет применения алгоритмов оценки психоэмоционального состояния с помощью методов интеллектуального анализа данных видеопоследовательности.

Блок принятия решений о текущем психоэмоциональном состоянии оператора реализует анализ на основе выделенных ключевых точек геометрии лица оператора. Исходными данными для этого является вектор оценок вероятностей наличия k-того эмоционального состояния в выделенном ROI с учетом меток времени для оператора. На данном этапе происходит выявление наличия специфических паттернов для оценки психоэмоционального состояния оператора в контексте изменения оценок вероятностей k-того эмоционального

состояния во времени. Выходные данные этого блока – вектор оценок психоэмоционального состояния – контролирует супервайзер.

На обучающей выборке точность классификатора на основе рекуррентной глубокой нейронной сети составила 97,62%, а на тестовой –79,48%.

Результаты распознавания приведены в таблице 5.14-5.15. Верхняя метка (зеленая рамка – область интереса, содержащая лицо, в которой происходит выделение опорных точек) – это истинная метка, назначенная для данного изображения экспертом, а нижняя – метка, назначенная классификатором.

Таблица 5.14 – Результаты перекрестной проверки.

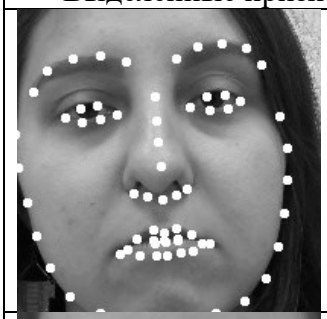
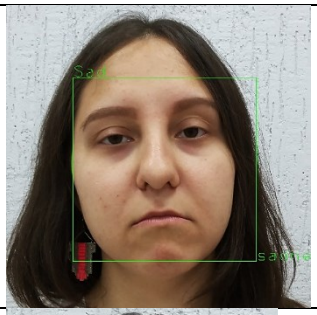
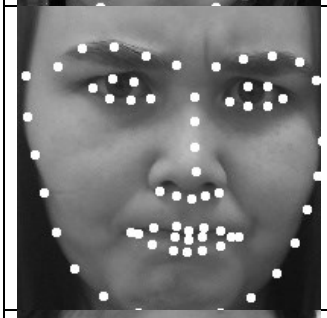
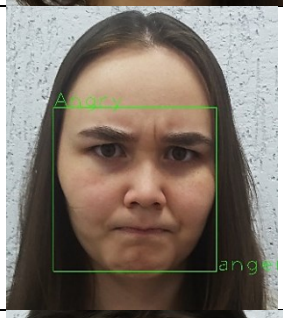
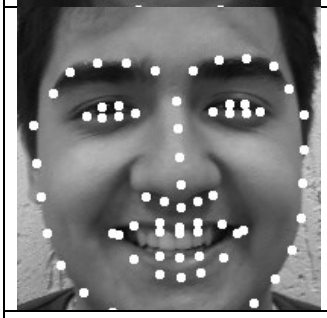
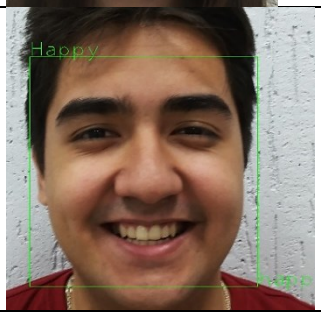
Выделенные признаки	Распознанная эмоция	Истинная метка
		Грусть
		Злость
		Радость

Таблица 5.15 – Результаты распознавания при использовании перекрестной проверки

Параметр	Обучающая выборка				Тестовая выборка			
Accuracy	82.4 %				82.9 %			
Precision	82.1 %				82.7 %			
F_1	82.2 %				82.8 %			
Confusion matrix, %	75,67	3,93	15,94	4,87	75,78	3,62	15,58	4,26
	4,20	88,42	7,18	5,03	5,13	88,36	6,68	7,10
	16,17	5,06	73,98	5,15	14,67	5,25	74,77	2,84
	3,95	2,59	2,91	84,96	4,42	2,77	2,97	85,80

Эффективность предложенного решения заключается в реализации в составе системы мониторинга состояния оператора функционала, позволяющего выявлять нестабильные психоэмоциональные состояния без использования дополнительных контактных датчиков в режиме мягкого реального времени на основе технологий интеллектуального анализа данных видеопоследовательности. Точность выявления нестабильных психоэмоциональных состояний составляет 79 %. Вероятность своевременного обнаружения нестабильного состояния без применения алгоритмов анализа видеопоследовательности существенно ниже.

5.6.3 Подсистема преобразования биометрических признаков пользователя в криптографический ключ

Предлагаемая структура нейросетевой системы (НС) биометрической аутентификации приведена на рисунке 5.16.

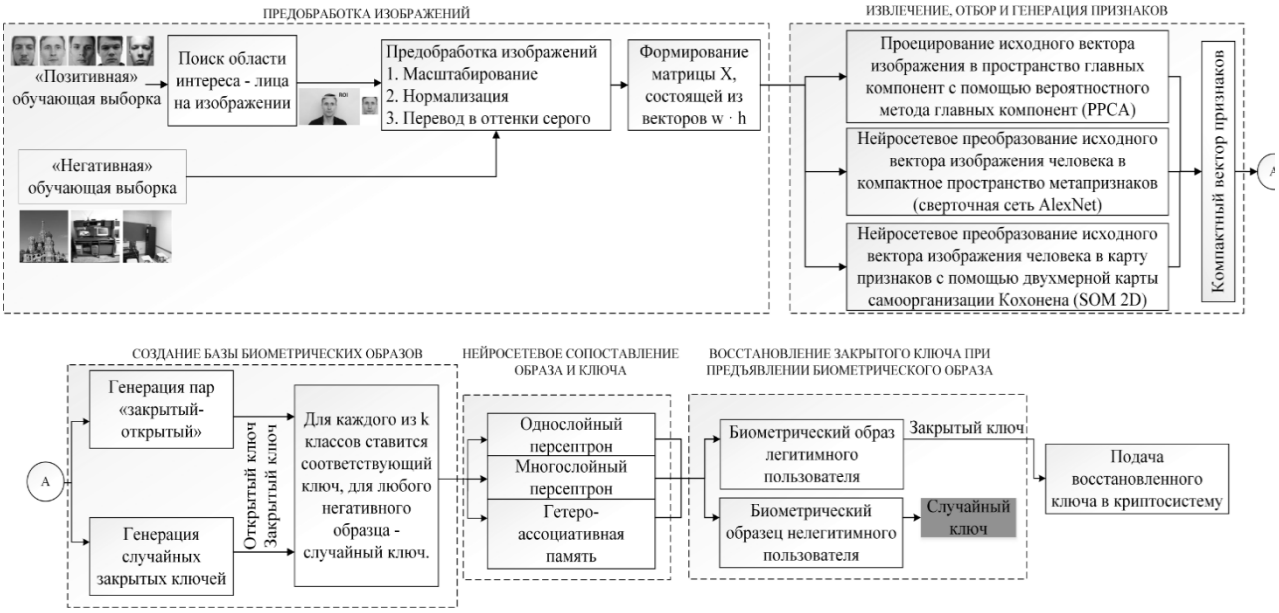


Рисунок 5.16 – Структура нейросетевой системы биометрической идентификации

При разработке структуры системы аутентификации с нейросетевым преобразованием исходных биометрических признаков в криптографический закрытый ключ алгоритм разделен на пять условных этапов:

1) предобработка признаков;
2) генерация признаков;
3) создание базы биометрических образов;
4) нейросетевое сопоставление образов и ключей;

5) восстановление ключа.

Задача блока предобработки признаков заключается в унификации изображения лица человека и построение первичного вектора признаков.

Далее вектора признаков подаются в блок генерации признаков, где происходит их преобразование в компактные вектора признаков, содержащие минимальный и достаточный объем информации.

Если текущей является задача добавления пользователя в систему, то компактный вектор признаков подается на вход блока создания базы биометрических образов, где выполняется нейросетевое сопоставление закрытого ключа и подаваемого вектора.

Блок восстановления ключа необходим для трансформации компактного вектора признаков в требуемый ключ пользователя (при несанкционированной авторизации система выдает случайный ключ, неиспользуемый в системе).

Для генерации признаков предлагается использовать следующие подходы:

1) самоорганизующаяся двумерная карта Кохонена (self-organizing map, SOM);
2) вероятностный метод главных компонент (ВМГК, probabilistic principal component analysis, PPCA);
3) сверточная нейронная сеть (convolutional neural network, CNN) AlexNet

Сопоставление компактных векторов биометрических образов и криптографических ключей реализовано с помощью следующих методов:

1) построение и обучение двунаправленной ассоциативной памяти на основе нейронной сети Б. Коско в варианте Й. Ванга (BAM) [233];
2) построение и обучение однослойных и многослойных нейронных сетей прямого распространения на основе персептронов (МСП).

Для оценки защищенности биометрической системы на основе ML-модели выполнен анализ актуальных угроз, уязвимостей и потенциальных векторов атак. Построена нечеткая серая когнитивная карта для моделирования и оценки рисков ИБ в случае воздействия злоумышленника без использования и с использованием архитектуры ML-модели нейросетевого преобразования «биометрия-ключ». Показатели риска ИБ нарушения работоспособности системы и отказ от ее использования (нарушение целостности) и модификации базы и ML-модели (нарушение конфиденциальности) снизились на 45 %.

Таблица 5.16 – Сравнительные архитектуры НС-блока и условия эксперимента

Параметры	Эксперимент				
	1	2	3	4	5
	МСП	ВМГК + МСП	Двумерная карта Кохонена + МСП	AlexNET + МСП	ВАМ
Исходные изображения	[64, 64, 1]	[64, 64, 1]	[64, 64, 1]	[227, 227, 3] в цветовой схеме RGB	[64, 64, 1]
Генерация компактного вектора признаков	Нет	с помощью ВМГК отобрано 64 главных компоненты	Двумерная карта Кохонена, 15 * 15 нейронов с гексагональной решеткой	Сверточная НС AlexNET (активации fc8 слоя)	нет
Архитектура НС блока сопоставления					
Размерность входного вектора	4096	64	225	1000	4096
Тип входного вектора	Десятичные целые числа [0, 255]	Вещественные числа	Бинарный вектор активностей нейронов выходного слоя карты Кохонена	Вещественные числа	Двоичный код Грея
Размерность выходного вектора	132 или 1056	1056	1056	1056	1056
Тип выходного вектора	Десятичные целые числа [0, 255] или двоичные в коде Грея	Двоичный код Грея	Двоичный код Грея	Двоичный код Грея	Двоичный код Грея
Тип НС	МСП	МСП	МСП	МСП	ВАМ
Количество нейронов по слоям	4096, 2018, 1056	64, 1056	225, 1056	1000, 1056	4096, 1056
Функции активации нейронов по слоям	elliotsig, elliotsig, satlins	elliotsig, satlins	elliotsig, satlins	elliotsig, satlins	satlins, satlins
Постобработка выхода НС	нет / hardlim	hardlim	hardlim	hardlim	hardlim

Таблица 5.17 – Сравнительные результаты экспериментов

Параметры	Обучение					Тестирование				
	МСП	ВМГК + МСП	Двумерная карта Кохонена + МСП	AlexNET + МСП	ВАМ	МСП	ВМГК + МСП	Двумерная карта Кохонена + МСП	AlexNET + МСП	ВАМ
Абсолютное количество ошибок / примеров	394 [4500]	362 [4500]	281 [4500]	273 [4500]	23 [450]	133 [1500]	124 [1500]	95 [1500]	88 [1500]	8 [150]

Параметры	Обучение					Тестирование				
	МСП	ВМГК + МСП	Двумерная карта Кохонена + МСП	AlexNET + МСП	ВАМ	МСП	ВМГК + МСП	Двумерная карта Кохонена + МСП	AlexNET + МСП	ВАМ
Доля корректно распознанных образов, %	91,24	91,96	93,76	93,93	94,89	91,13	91,73	93,67	94,13	94,67
Чувствительность	0,9688	0,9825	0,9784	0,9729	0,9865	0,9828	0,9806	0,9808	0,9808	1
Специфичность	0,9727	0,9753	0,9830	0,9811	0,9628	0,9763	0,9775	0,9774	0,9774	0,9758
Положительная прогностическая значимость	0,8794	0,8869	0,9188	0,9101	0,8391	0,8837	0,9004	0,9011	0,9014	0,8966
Прогностическая ценность отрицательных результатов	0,9934	0,9965	0,9957	0,9946	0,9972	0,9968	0,9959	0,9959	0,9959	1

Ключевыми для систем биометрической идентификации и аутентификации являются: подделка биометрических данных, предъявляемых через пользовательский интерфейсе, и утечка из базы биометрических образов. Уязвимости реализаций систем биометрической идентификации и аутентификации можно разделить на:

– уязвимости в используемых библиотеках и подключаемых модулях;

– уязвимости в непосредственном программном коде;

– архитектурные уязвимости.

Атаки на биометрические образы, предъявляемые через пользовательский интерфейс системы, можно разделить на две группы:

– нецелевая атака (общий тип атаки, когда основной целью является неверный результат классификации);

– целевая атака (целью является получение метки требуемого класса при данном входном изображении).

Для систем, использующих методы и технологии машинного обучения, выделяют два вида (adversarial machine learning) AML-атак:

– уклонение (evasion) – злоумышленник вызывает некорректное поведение моделью. Система рассматривается злоумышленником как черный ящик. Этот тип атак считается наиболее распространенным, к нему относятся спуффинг-атаки на биометрические системы, когда злоумышленник стремится замаскироваться под другого человека.

– отравление (poisoning), когда злоумышленник стремится получить доступ к данным и процессу обучения ML-модели, чтобы нарушить процесс обучения. Отравление можно рассматривать как злонамеренное заражение обучающих данных. Атакующий обладает сведениями об устройстве системы (Adversarial Knowledge, AK): источники и алгоритмы обработки данных для обучения, алгоритмы обучения и результирующие параметры.

Потенциальные угрозы нарушения информационной безопасности и кибербезопасности и потенциальные уязвимости нейросетевой системы биометрической аутентификации выделены в [2].

В таблице 6 основные уязвимости соответствуют концептам C_7 – C_9 НСКК. Угрозам C_2 – C_6 соответствуют сценарии воздействия внешнего злоумышленника в ходе эксплуатации одной или нескольких уязвимостей системы. Оценка рисков ИБ системы НСБАИ выполнена для наиболее вероятных векторов атак. Соответствующая НСКК представлена на рисунке 5.17

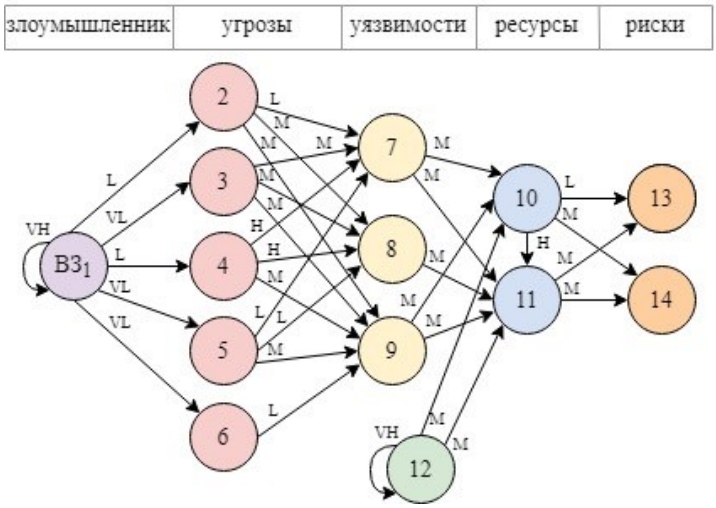


Рисунок 5.17 – Нечеткая когнитивная карта оценки рисков ИБ НСБИА

Таблица 5.18 – Описание концептов нечеткой серой когнитивной карты.

Концепт	Наименование	Тип концепта
$ВЗ_1$	Внешний злоумышленник	Концепт-драйвер
C_2	Угроза раскрытия информации о ML-модели (УБИ.218)	Угрозы
C_3	Угроза хищения обучающих данных (УБИ.219)	
C_4	Угроза нарушения функционирования ML-модели (УБИ.220)	
C_5	Угроза модификации модели ML (УБИ.221)	
C_6	Угроза подмены модели ML (УБИ.222)	
C_7	Уязвимость библиотек и моделей (подключаемых)	Уязвимости
C_8	Уязвимость программной реализации модели	
C_9	Архитектурные уязвимости	
C_{10}	База биометрических образов	Целевые ресурсы системы
C_{11}	ML-модель	

C_{12}	Контрмера на основе реализации нейросетевого преобразования «биометрия-ключ»	Концепт-драйвер
C_{13}	Нарушение работоспособности системы и отказ от ее использования (нарушение целостности)	Последствия
C_{14}	Модификация базы и ML-модели (нарушение конфиденциальности)	

Рассмотрим сценарий воздействия злоумышленника с использованием и без использования контрмеры на основе нейросетевого преобразования «биометрия-ключ» для обеспечения информационной безопасности и кибербезопасности НСБИА. Показатели риска ИБ для целевых концептов C_{13}, C_{14} отражены в таблице 5.19.

Таблица 5.19 – Результаты анализа рисков на основе НСКК.

Концепт	Без применения нейросетевого преобразования «биометрия-ключ»	После применения нейросетевого преобразования «биометрия-ключ»
Нарушение работоспособности системы и отказ от ее использования (нарушение целостности)	[0.0162; 0.4156]	[0.0442; 0.2560]
Модификация базы и ML-модели (нарушение конфиденциальности)	[0.0199; 0.4694]	[0.0527; 0.2846]

Предложен подход к анализу защищенности интегрированных систем биометрической аутентификации и идентификации на основе серых нечетких когнитивных карт. Особенностью биометрической системы является применение нейросетевого преобразования «биометрия-ключ», что обеспечивает распределенное хранение базы биометрических образов и позволяет использовать в качестве выхода нейронной сети генерируемый на основе образа секретный криптографический ключ.

Для оценки защищенности систем биометрической аутентификации и идентификации с применением ML-моделей проведен анализ актуальных угроз, уязвимостей и потенциальных векторов атак, на основе чего построена нечеткая серая когнитивная карта для оценки рисков ИБ в случае воздействия злоумышленника без использования и с использованием нейросетевого преобразования «биометрия-ключ». Показатели риска ИБ для ключевых информационных ресурсов снизились на 45 %.

5.6.4 Подсистема скрытой аутентификации пользователя на основе нейросетевого анализа динамического профиля в системе профилирования пользователя

Целью является повышение точности скрытой аутентификации пользователя на основе нейросетевого анализа динамического профиля, формируемого по клавиатурному почерку.

Предлагается подход для опознавания субъекта, основанный на проведении непрерывной скрытой аутентификации пользователя компьютерной системы в процессе его работы за компьютером. В качестве идентификационных характеристик используются особенности работы пользователя с клавиатурой – его клавиатурный почерк, который характеризуется временами удержания клавиш (ВУК) и временами между нажатиями клавиш (ВМН). Данные характеристики позволяет измерить стандартная клавиатура.

Время удержания зависит также от наложений. Наложение нажатий клавиш происходит, когда одна клавиша еще не отпущена, а другая уже нажимается. Наблюдается тенденция к повышению количества наложений с повышением скорости набора. Подавляющее большинство наложений происходит, когда клавиши соседних букв в слове нажимаются разными пальцами. Однако при очень быстром наборе скольжениями наложения также возможны. Из всего объема текста, вводимого пользователем в течение рабочего дня, предлагается обрабатывать не отдельные нажатия клавиш, а так называемые N-графы – триграфы и тетраграфы – последовательности трех или четырех подряд нажатых клавиш.

Из всех полученных значений ВУК и ВМН в течение рабочего дня будут обрабатываться только самые часто встречаемые N-графы, для этого формируется частотный словарь триграфов и тетраграфов. По данным частотного словаря выделяются словоформы с высокой частотностью для каждого претендента. Для анализа отбираются наиболее частые в употреблении N-графы, присутствующие у каждого из пользователей. В дальнейшем, именно на анализе этих словоформ и проводится аутентификация пользователей.

Весь набор полученных векторов биометрических признаков был разделен на 10 подмножеств, после чего 10 раз производилось тестирование по 9 наборам и проверка по одному оставшемуся. Результаты, полученные на каждой из 10 итераций, были усреднены и занесены в итоговую таблицу 5.20.

Таблица 5.20 – Процентное соотношение распознаваемости триграфов

Триграф		ени	льн	ния	нны	про	**Итог**
Количество		63	58	59	58	62	
Корректное распознавание (%)	Метод 1	96,34	98,48	100	99,81	100	**98,926**
	Метод 2	99,12	100	99,62	98,48	98,6	**99,164**

В таблице приведены значения корректного распознавания пользователя по каждому из отобранных триграфов при использовании двух методов.

Результаты, полученные при использовании обоих методов, были усреднены и занесены в итоговый столбец таблицы.

Получены следующие результаты:

– разработан алгоритм кодирования вектора признаков, характеризующих клавиатурный почерк пользователя, на основе нормализованного представления ВУК и ВМК;

– разработан алгоритм анализа клавиатурного почерка пользователя на основе нейросетевых классификаторов;

– разработана модульная структура нейронной сети, корректно распознающая пользователей в 98 % случаев;

– разработан прототип системы скрытой аутентификации пользователя на основе предложенного алгоритма анализа динамического профиля пользователя.

5.7 Выводы по главе

Для выявления сложных атак злоумышленников, получивших доступ с сеть промышленного объекта, необходимо применение методов и инструментов расширенной аналитики данных, позволяющих выполнять оперативный анализ и выявление скрытых признаков злонамеренной активности на основе модели наблюдаемого КФО.

Способ мониторинга целостности данных, получаемых с эксплуатируемой САУ ГТД ЛА, основан на применении алгоритмов адаптивной сегментации ТВР с использованием таких характеристик сигналов, как: амплитуда, форма волны (морфологии), длительность, распределение энергии, частотное содержание и т.д., с последующей идентификацией фрагментов ТВР и сопоставлением их с отдельными событиями. Блок принятия решений о наличии вмешательства злоумышленника и внесении модификации в контент сообщения при передаче информации с борта ЛА на ПИ обеспечивает обработку ТВР, генерируемых САУ ГТД на эксплуатируемом ЛА, а именно определяет режим работы САУ ГТД (установившийся или переходный) и производит сравнение этих данных с данными, генерируемыми моделью на предприятии-изготовителе. Предложенные способы и система позволяют выявлять несанкционированные воздействия на данные о состоянии САУ ГТД и тем самым повысить уровень защиты информации при ее передаче с борта ЛА на предприятие-изготовитель.

Реализация системы мониторинга ТП на основе технологии искусственного интеллекта повышает степень защищённости результатов измерений от несанкционированной модификации в базах данных информационных систем промышленного предприятия: для тестовой выборки точность классификатора составила 87,99%, а вероятность ошибки отдельных классификаторов типов не превышает 14%.

Для построения модели обнаружения аномалий состояния КФО, вызванных действиями злоумышленника в промышленной сети в ходе реализации сложной сетевой атаки, нами был использован доступный набор данных, который был собран в ходе испытаний АСУ ТП промышленного объекта и дополнен результатами программно-аппаратного моделирования.

Разработан алгоритм интеллектуального анализа технологических временных рядов в задаче обнаружения аномалий наблюдаемых параметров состояния объектов АСУ ТП. Обнаружение аномалий по всем типам составило в среднем

65 % (первого типа – 69 %, второго типа – 78 %, третьего типа – 80 %) при принятии допущений о периодичности и длительности атак, что свидетельствует об эффективности решения поставленной задачи. Дальнейшее развитие фильтрации ложноположительных срабатываний на основе анализа временных характеристик потенциальных атак позволит повысить эффективность предлагаемого ансамбля детекторов.

С целью снижения роли человеческого фактора в процессе диагностирования технического объекта и улучшения информационного обеспечения процесса поддержки принятия решений, разработана диагностическая модель распознавания ситуаций, возникающих на участках инженерной сети нефтедобычи, основанная на анализе ТВР. Использование разработанной нейросетевой модели позволяет избежать излишней сегментации и переключения сигнализирующей системы, расширить количество выделяемых классов событий на 20–30 % путем обнаружения переходных состояний, сократить количество настраиваемых параметров, а также увеличить на 10–12 % количество выявляемых событий и тем самым повысить достоверность описания ситуаций.

Разработаны алгоритмы интеллектуального анализа параметров сетевого трафика в задаче обнаружения вредоносной сетевой активности. Приведена общая схема алгоритма. Проанализированы варианты построения ансамблей и комитетов классификаторов на основе традиционных моделей машинного обучения (модели случайного леса, рандомизированные деревья решений и пр.) и гетерогенных нейросетевых моделей (глубокие нейронные сети, сверточные нейронные сети и модели на основе автоенкодеров с долгой краткосрочной памятью).

В составе системы автоматического профилирования (профайлинга) предложена обобщенная схема модуля видеоаналитики, позволяющего:

1) анализировать тип двигательной активности оператора. Оценка эффективности программной реализации показала корректность классификации паттернов активности в 97 % случаев;

2) выполнять функции нейросетевой системы идентификации и аутентификации пользователя.

Глава 6. Решение практических прикладных задач комплексной оценки рисков ИБ и обеспечения защищенности объектов КИИ с использованием исследовательского прототипа интеллектуальной системы поддержки принятия решений

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).

6.1 Архитектура интеллектуальной системы поддержки принятия решений

Архитектура ИСППР по оценке рисков ИБ объектов КИИ включает в себя следующие базовые модули:

- подсистема анализа угроз и уязвимостей объекта КИИ на основе технологий семантического анализа их текстовых описаний,
- подсистема оценки опасности уязвимостей на основе прогнозирования векторов метрики с помощью анализа текстового описания дескрипторов безопасности,
- подсистема построения и анализа семантической модели дескрипторов безопасности объектов зоны объекта КИИ,
- подсистема обнаружения сетевых атак в гетерогенной сети промышленного Интернета вещей,

- подсистема автоматического профилирования.

Особенностью данной ИСППР является возможность автоматизации основных этапов комплексной оценки рисков ИБ объектов КИИ.

6.1.1 Функциональная декомпозиция процесса ИАД CRISP-DM в рамках построения и функционирования ИСППР

С помощью методологии IDEF0 приводится функциональная декомпозиция процесса интеллектуального анализа данных CRISP-DM в рамках построения и функционирования ИСППР для задач интеллектуального анализа накапливаемых данных мониторинга состояния наблюдаемого объекта.

CRISP-DM [68] (The Cross Industries Standard Process for Data Mining – Стандартный межотраслевой процесс Data Mining) является наиболее популярной и распространенной методологией, описывающей в терминах иерархического моделирования процесс, который состоит из набора задач, описанных четырьмя уровнями обобщения: фазы, общие задачи, специализированные задачи и запросы.

Процесс «Анализ предметной области» позволяет осуществить знакомство с процессами управления, целями и задачами разработки интеллектуальных компонент системы сбора и обработки данных (рис. 6.1)

Рисунок 6.1 – Функциональная модель ИАД по методологии CRISP-DM. Нулевой уровень

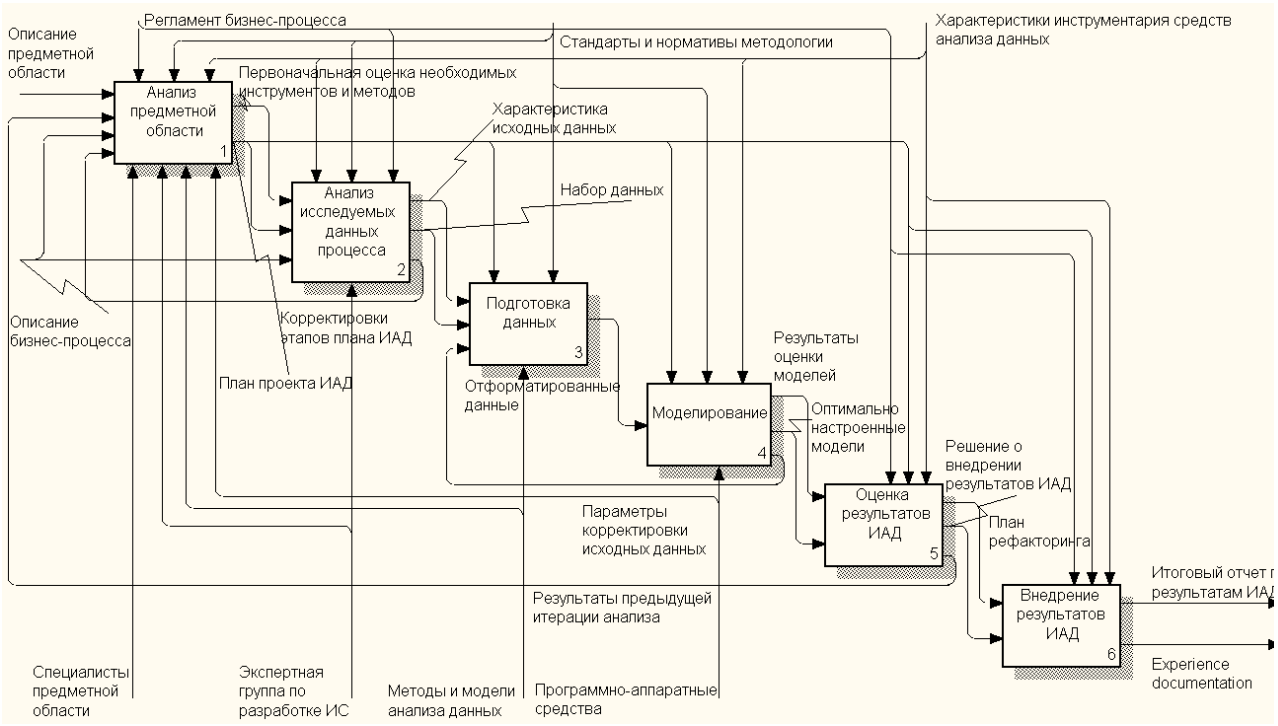


Рисунок 6.2 – Функциональная модель ИАД по методологии CRISP-DM. Первый уровень декомпозиции

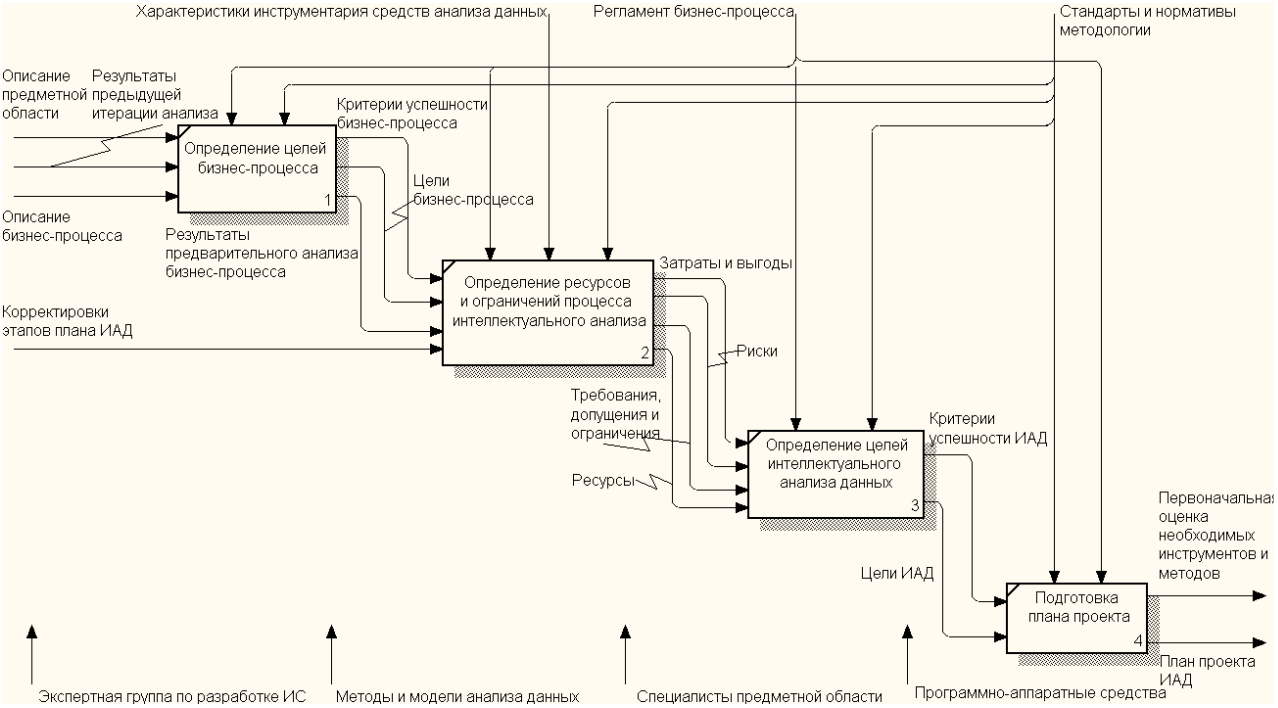


Рисунок 6.3 – Функциональная модель ИАД по методологии CRISP-DM. Декомпозиция блока «Анализ предметной области»

Важным этапом ИАД является анализ исследуемых данных. Именно на этом этапе выявляется характер данных, описывающих процесс развития и функционирования реального объекта (рис. 6.4).

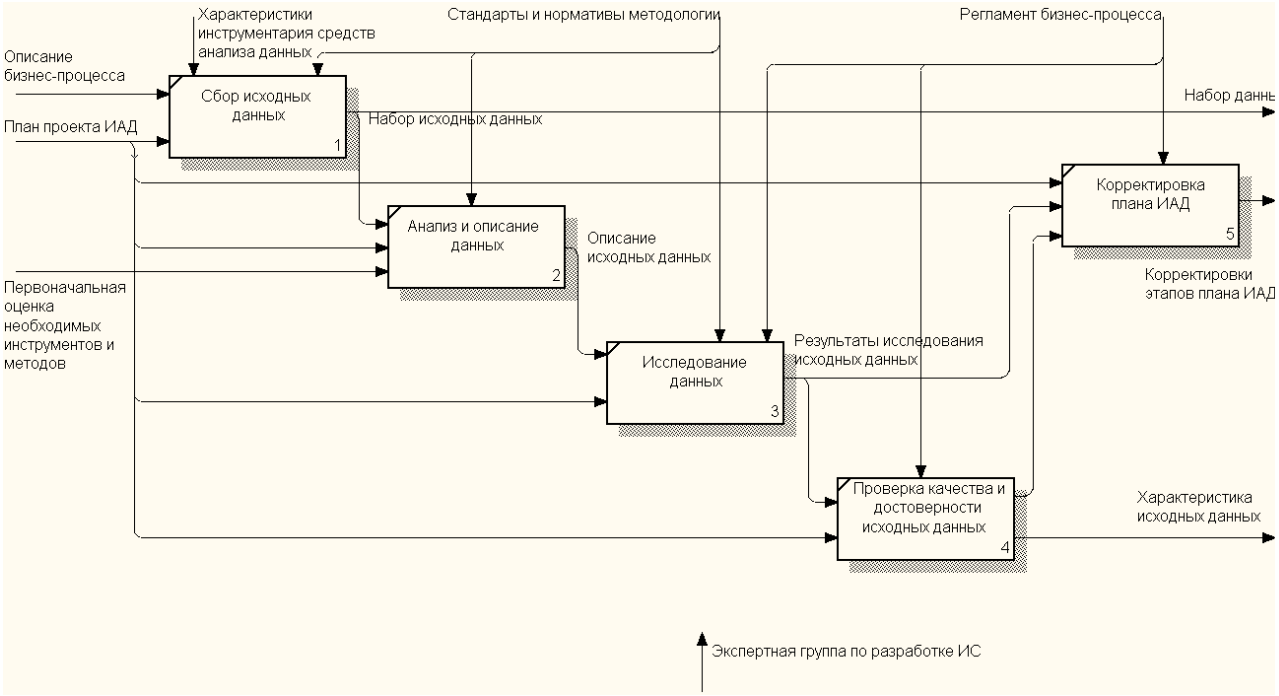


Рисунок 6.4. – Функциональная модель ИАД по методологии CRISP-DM. Декомпозиция блока «Анализ исследуемых данных процесса»

Использование сырых данных РВ затруднено, следовательно, необходим этап подготовки и предобработки подобных данных, извлекаемых из БД РВ. На этом шаге выполняются типовые процедуры препроцессирования исходных данных (рис. 6.5).

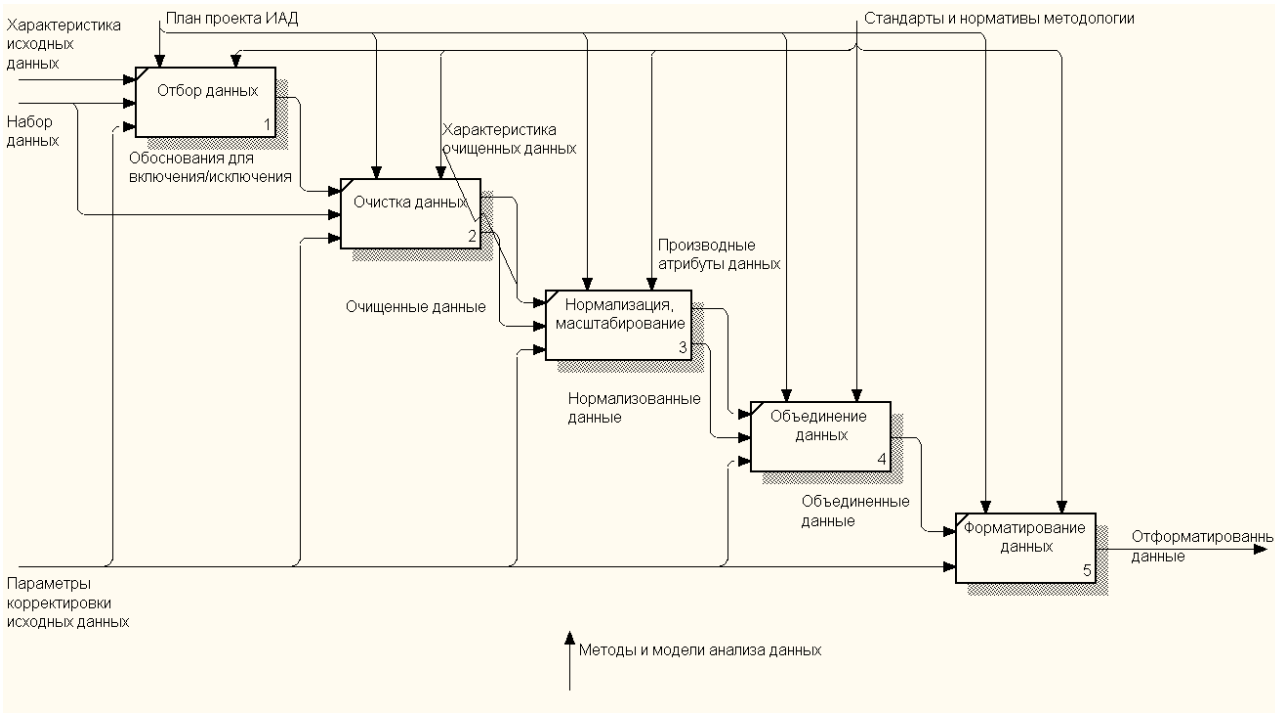


Рисунок 6.5 – Функциональная модель ИАД по методологии CRISP-DM. Декомпозиция блока «Подготовка данных»

Реализация нейросетевых моделей обработки ТВР и последующая оценка показателей модели являются следующим этапом ИАД (рис. 6.6).

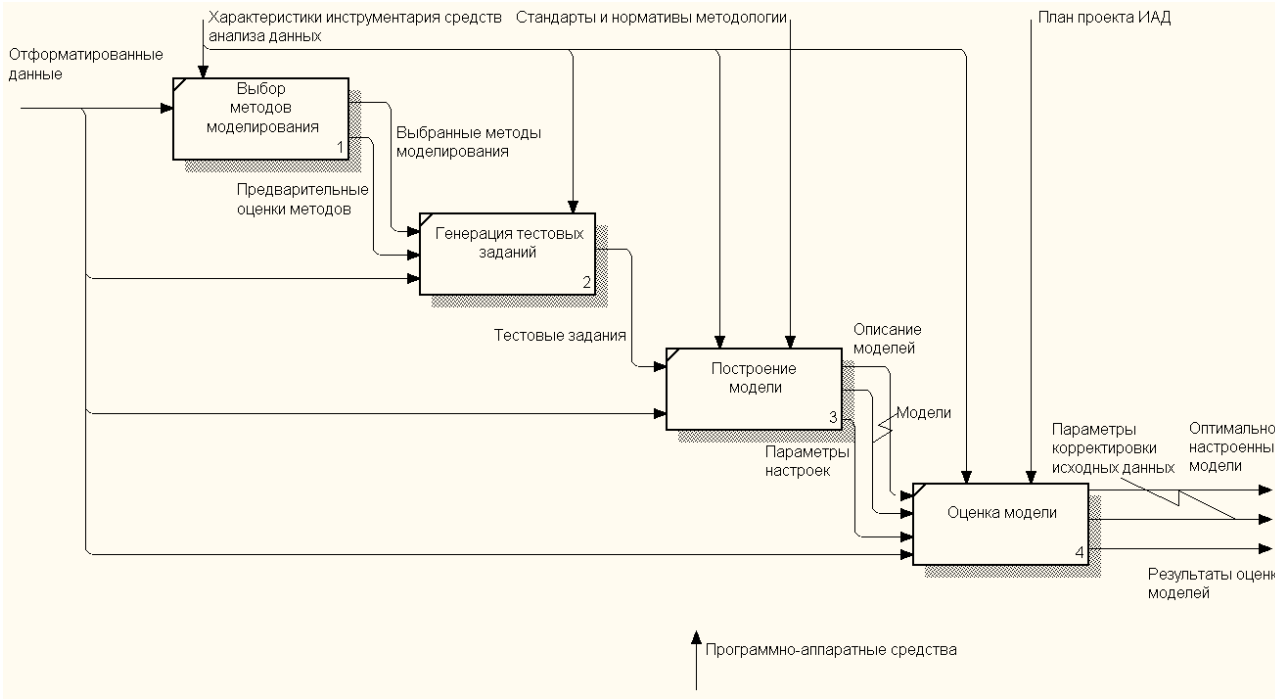


Рисунок А.6 – Функциональная модель ИАД по методологии CRISP-DM. Декомпозиция блока «Моделирование»

Результаты моделирования и выбранная наилучшая модель, отображающая скрытые закономерности наблюдаемых процессов, необходимо верифицировать и подтвердить их адекватность путем анализа накопленных данных (рис. 6.7).

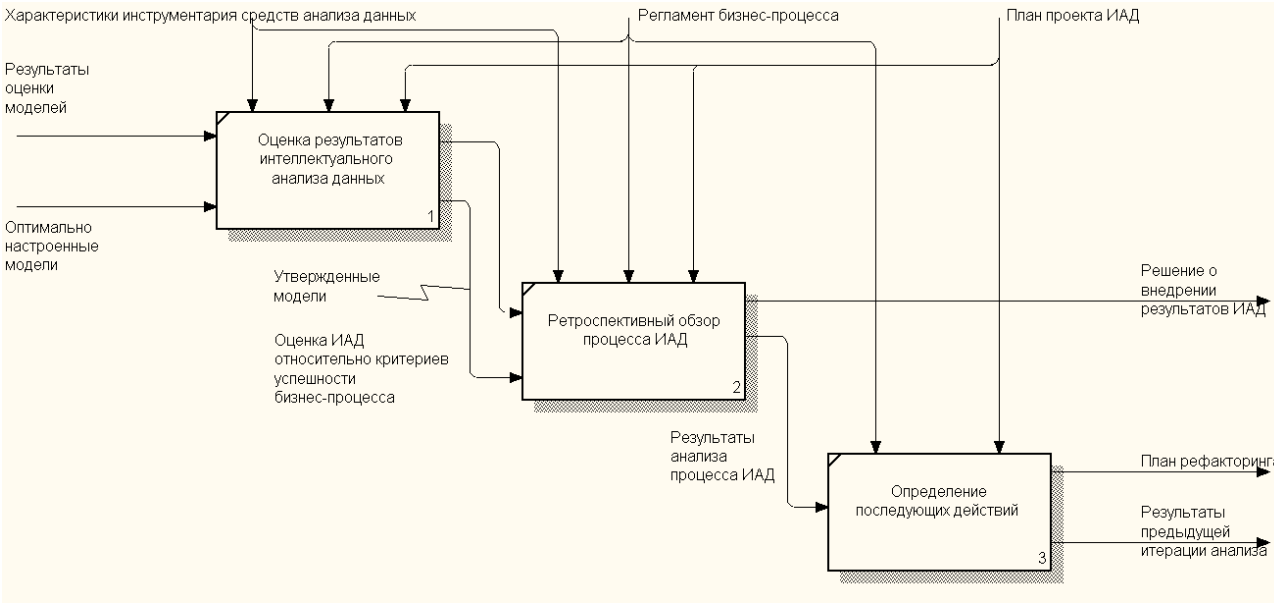


Рисунок 6.7 – Функциональная модель ИАД по методологии CRISP-DM. Декомпозиция блока «Оценка результатов ИАД»

Заключительным этапом является развертывание разработанного на основе выбранной модели ИАД программного комплекса и подготовка к последующим итерациям обслуживания системы обработки диагностической информации (рис. 6.8).

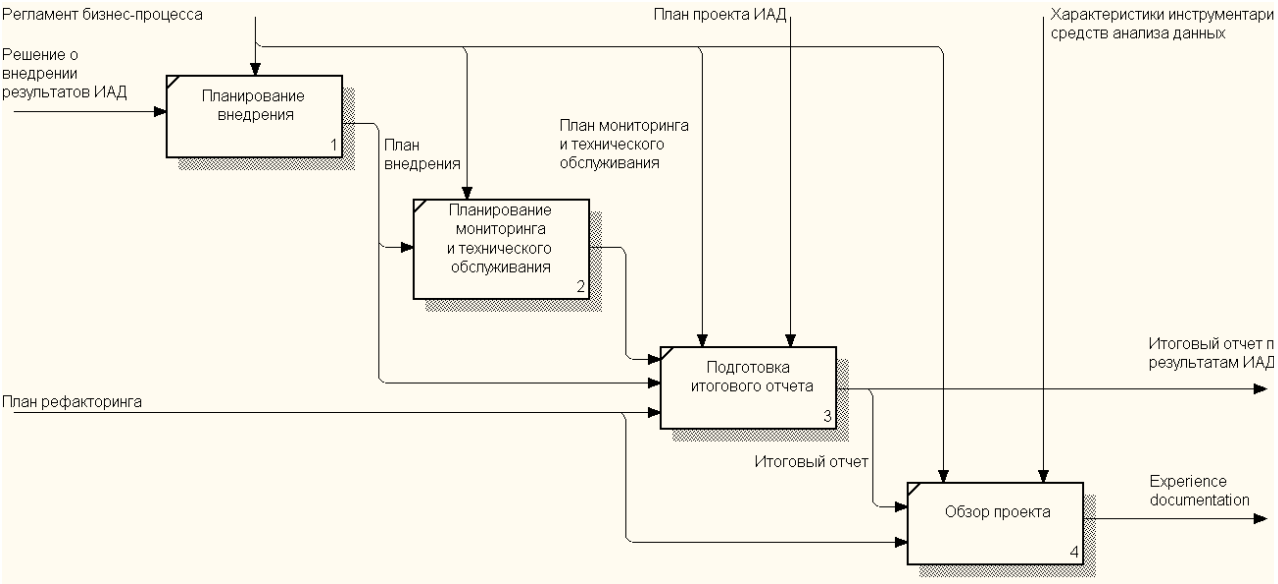


Рисунок 6.8 Функциональная модель ИАД по методологии CRISP-DM. Декомпозиция блока «Внедрение результатов ИАД»

6.1.2 Функциональная декомпозиция процесса анализа наблюдаемых параметров на основе интеллектуальной обработки данных в рамках построения и функционирования подсистем ИСППР

Опираясь на разработанную функциональную модель применения методологии ИАД CRISP-DM, необходимо декомпозировать и описать работу блоков анализа наблюдаемых параметров на основе интеллектуальной обработки данных. На рисунке приведена диаграмма блока «Адаптивная обработка данных ТВР с целью диагностики состояния ОУ» (рисунок 6.8).

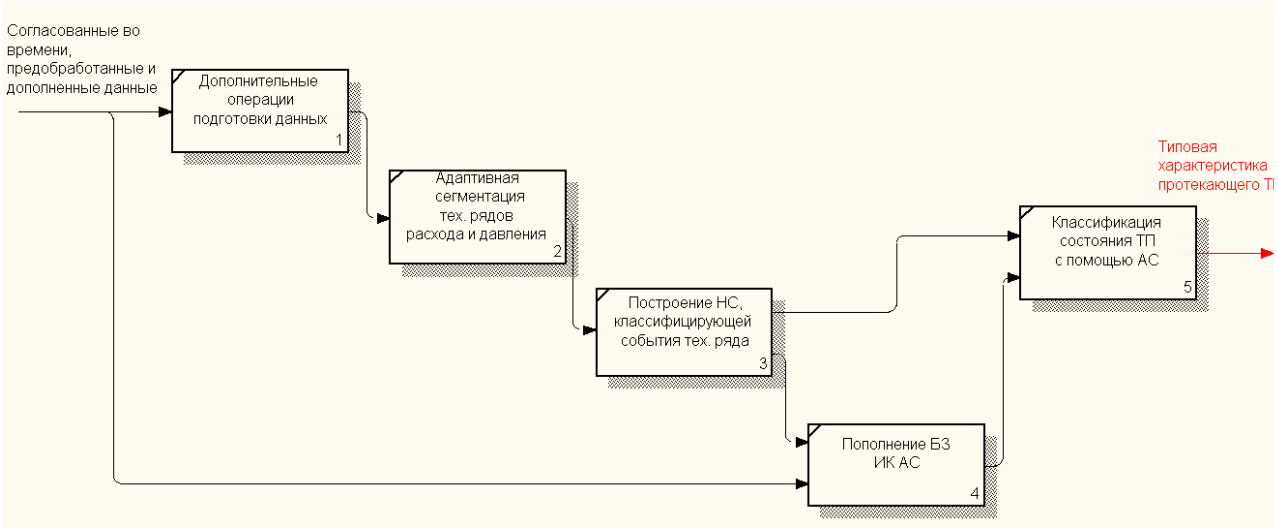


Рисунок 6.8 – Диаграмма функциональной модели IDEF0 «Адаптивная обработка данных ТП с целью определения текущего состояния ОУ»

Далее, описание работы модуля ППР, процедуры объяснения и интерпретации представляют собой декомпозицию блока «Оперативный анализ состояния участка инженерной сети» функциональной модели (рисунок 6.9)

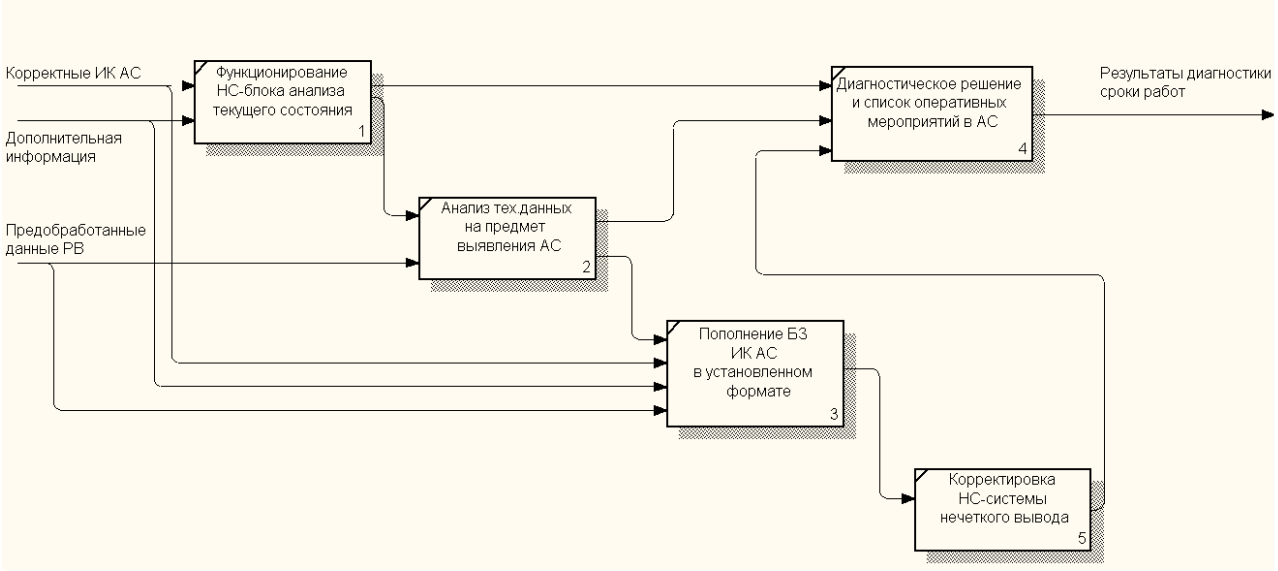


Рисунок 6.9 – Диаграмма функциональной модели IDEF0 «Оперативный анализ состояния участка инженерной сети»

Основываясь на предложенной логической модели данных, расширяющей подмножество моделей POSC Epicentre и объединяющей описываемые выше информационные потоки, разработана логическая модель подсистемы ППР (рисунок 6.10).

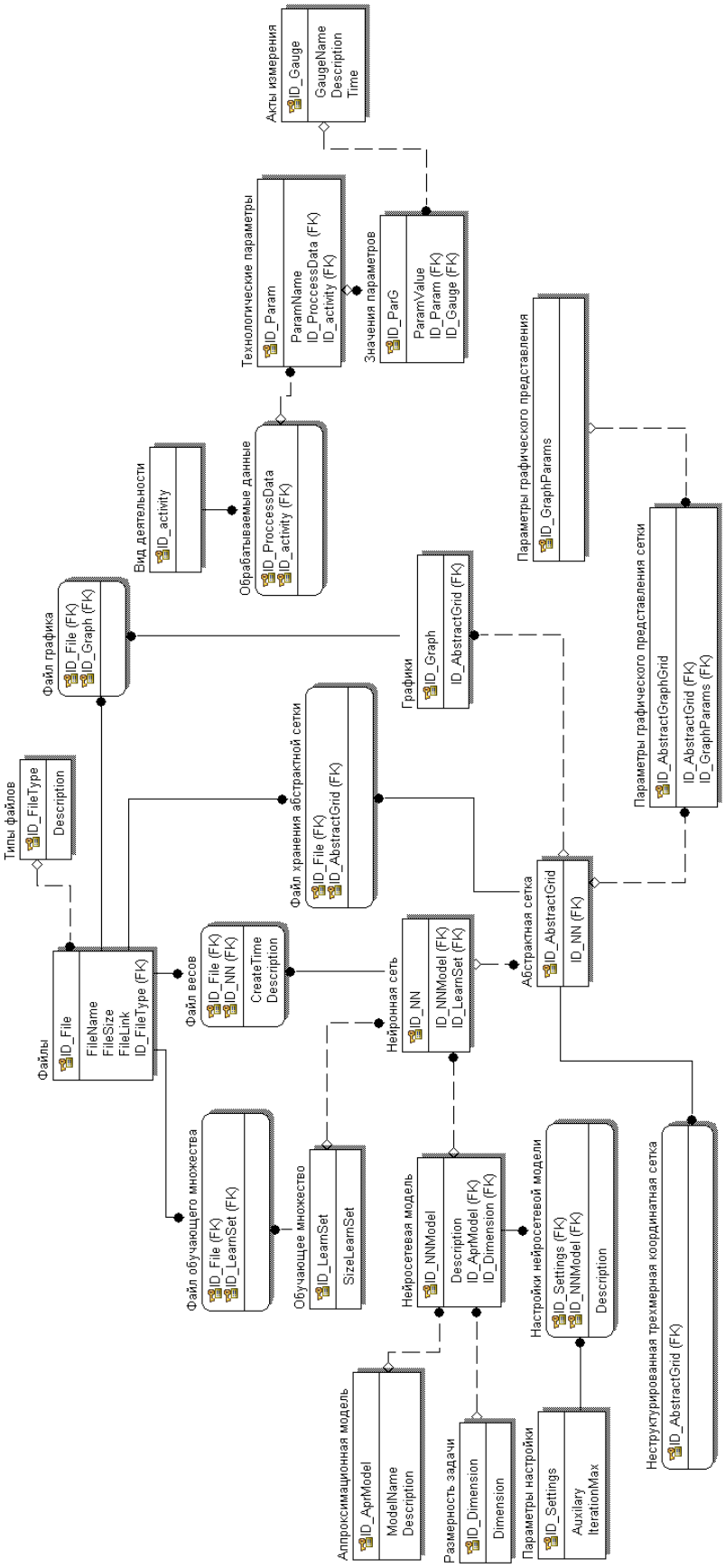


Рисунок 6.10 – Логическая модель данных для описания нейросетевой обработки ТВР

Процесс управления жизненным циклом разрабатываемого ПО, соответствует циклу PDCA и базовым требованиям процессного подхода,

сформулированным в МС ИСО 9000:2000, приведен в виде функциональной модели. Стандарт ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств» является основным нормативным документом, регламентирующим состав процессов жизненного цикла ПО (рисунок 6.11). Опираясь на итеративный процесс разработки ПК и методологию объектно-ориентированного анализа и проектирования, ниже представлены этапы разработки в нотациях UML-диаграмм.

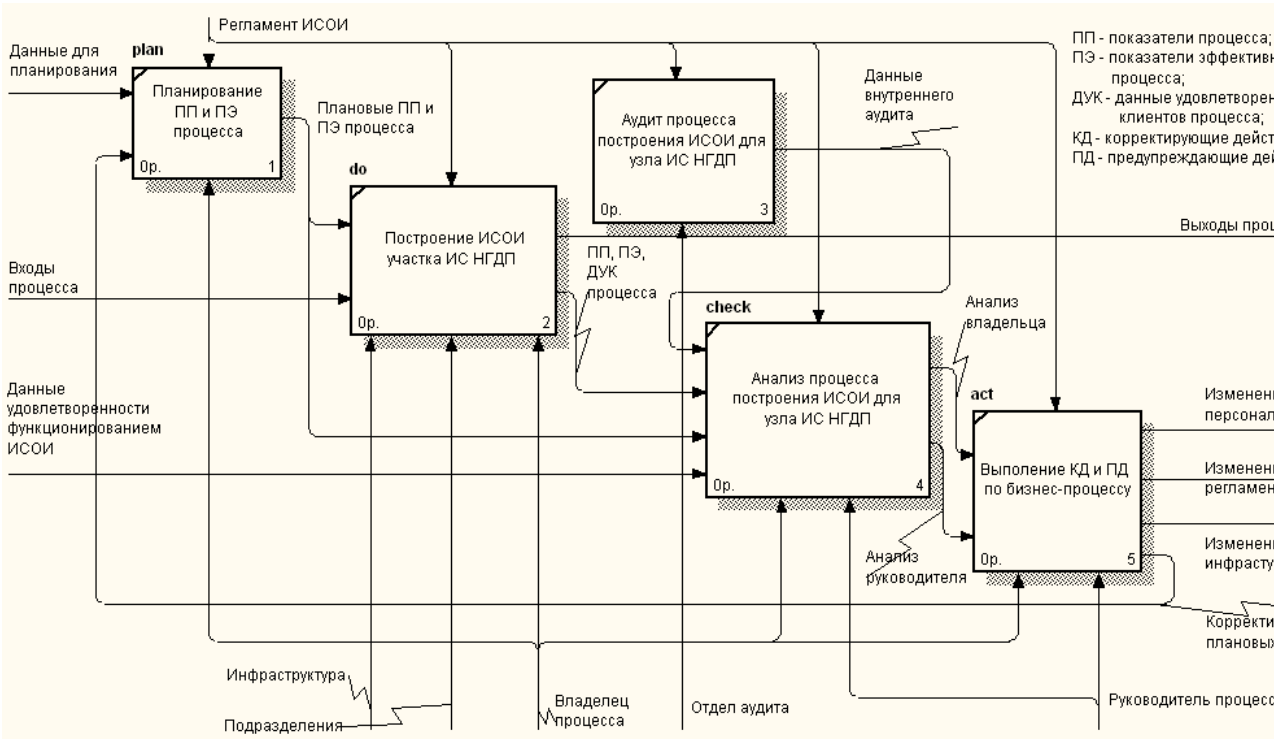


Рисунок 6.11– Управление процессом разработки программного комплекса

Диаграмма классов UML представлена на рис. 6.12. Приведены основные классы и интерфейсы нейросетевой библиотеки ПК. ИНС состоит из нескольких слоев и каждый слой, в свою очередь, из некоторого количества нейронов. Каждый нейрон характеризуется задаваемым функционалом, который определяет, как нейрон будет выполнять операции взвешенного суммирования, какую будет иметь функцию активации, как рассчитывать ошибку, смещение изменение весов и т.п.

Ниже перечислены основные функции классов и интерфейсов библиотеки: «INeuron», «INeuronStrategy», «INeuralNetwork» и «INetworkFactory» – интерфейсы:

– класс «Neuron» реализует абстрактный интерфейс «INeuron»

– класс «NeuralNetwork» реализует абстрактный интерфейс «INeuralNetwork»;

– каждый класс «Neuron» обладает стратегией поведения, определяемой конкретной реализацией абстрактного интерфейса «INeuronStrategy». Частная реализация интерфейса «INeuronStrategy» - класс «BackPropNeuronStrategy» для обеспечения процесса обратного распространения ошибки;

– конкретная нейронная сеть создается и инициализируется с помощью класса «INetworkFactory».

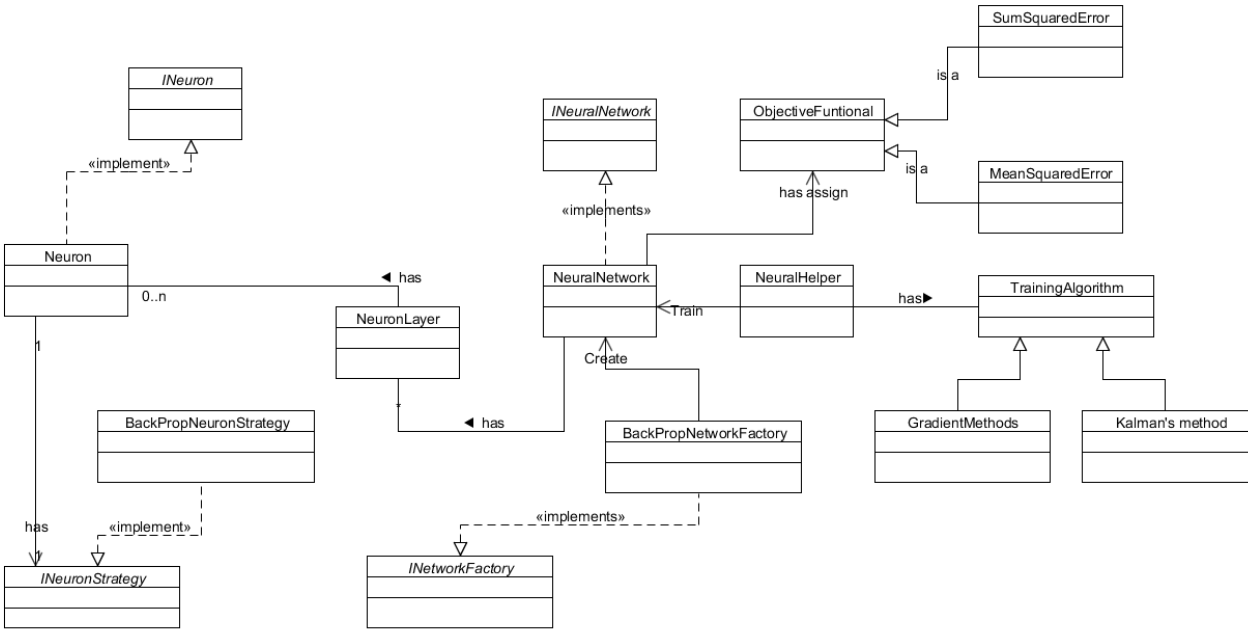


Рисунок 6.12 – Диаграмма классов нейросетевой библиотеки ПК

Основные интерфейсы и классы модели приведены в таблицах 6.1 и 6.2.

Таблица 6.1 – Основные интерфейсы диаграммы классов

Интерфейс	**Функционал**
INetworkFactory	Интерфейс определяет паттерн «Фабрика» для создания объекта «Нейронная сеть»
INeuron	Абстрактный нейрон
INeuronStrategy	Абстрактный класс, описывающий функционал нейрона
INeuralNetwork	Абстрактный класс, описывающий нейронную сеть

Таблица 6.2 – Основные классы нейросетевого модуля ПК

Класс	**Функционал**
BackPropNeuronStrategy	Имплементация INeuronStrategy, реализующая обратное распространение ошибки
NetworkHelper	Класс, определяющий процедуру создания, инициализации и обучения нейронной сети
NeuralNetwork	Базовая реализация интерфейса INeuralNetwork
NeuralNetworkCollection	Набор нейронный сетей

Neuron	Класс, описывающий отдельный нейрон

Диаграмма деятельности, описывающая алгоритм работы с ПК каждого из перечисленных выше пользователей, приведена на рисунке 6.13.

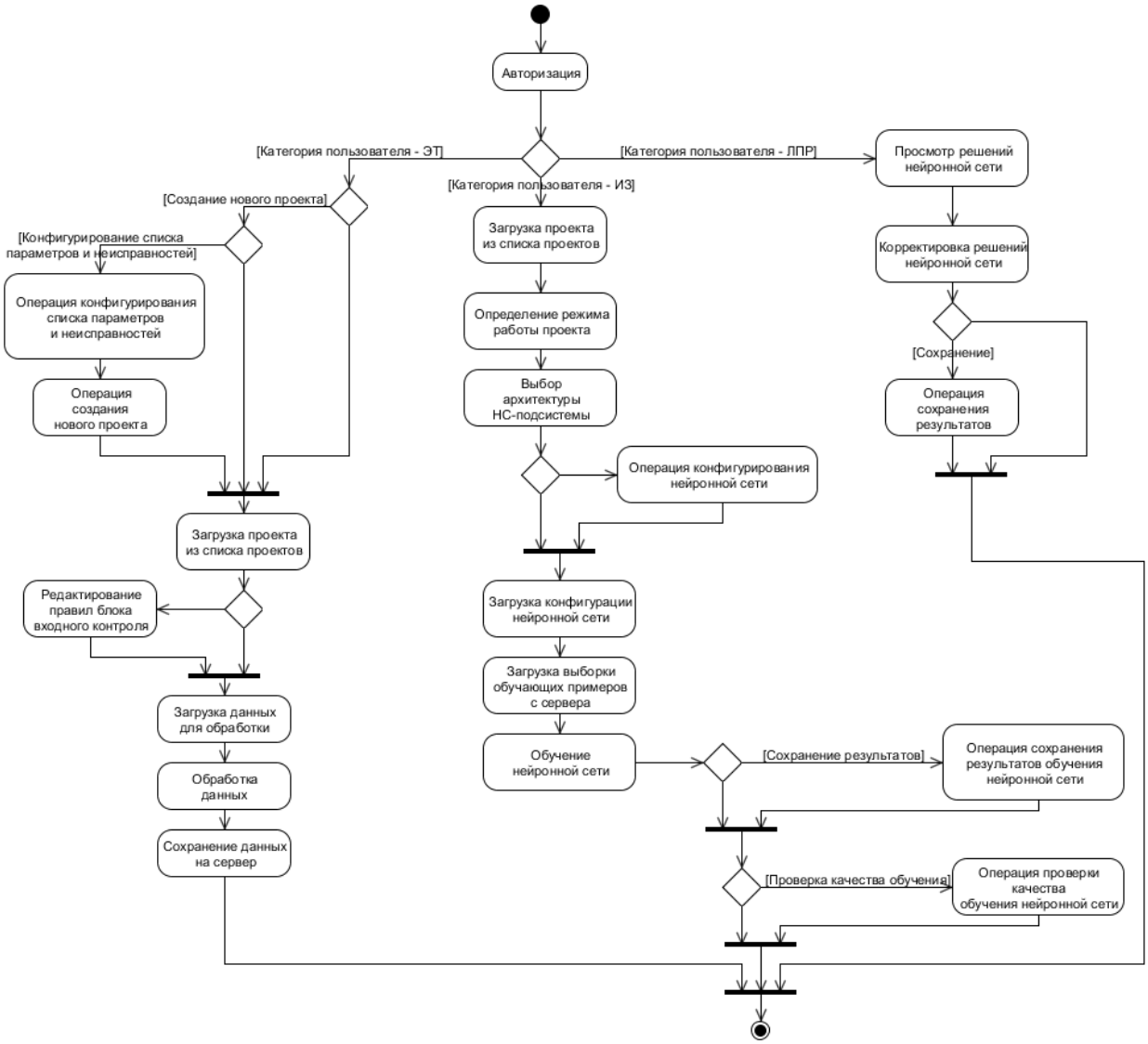


Рисунок 6.13– Диаграмма деятельности, описывающая функции пользователей ПК

Таким образом, разработаны функциональная и логическая модели, описывающие работу подсистем ИСППР. В рамках объектно-ориентированного подхода к разработке программного обеспечения выполнена объектная декомпозиция предметной области и разработаны диаграммы классов, деятельности и прецедентов.

На рисунке 6.14 приведена обобщенная структура цифровой платформы анализа данных в задаче обеспечения кибербезопасности, интегрирующая разработанные подсистемы ИСППР с внешними системами.

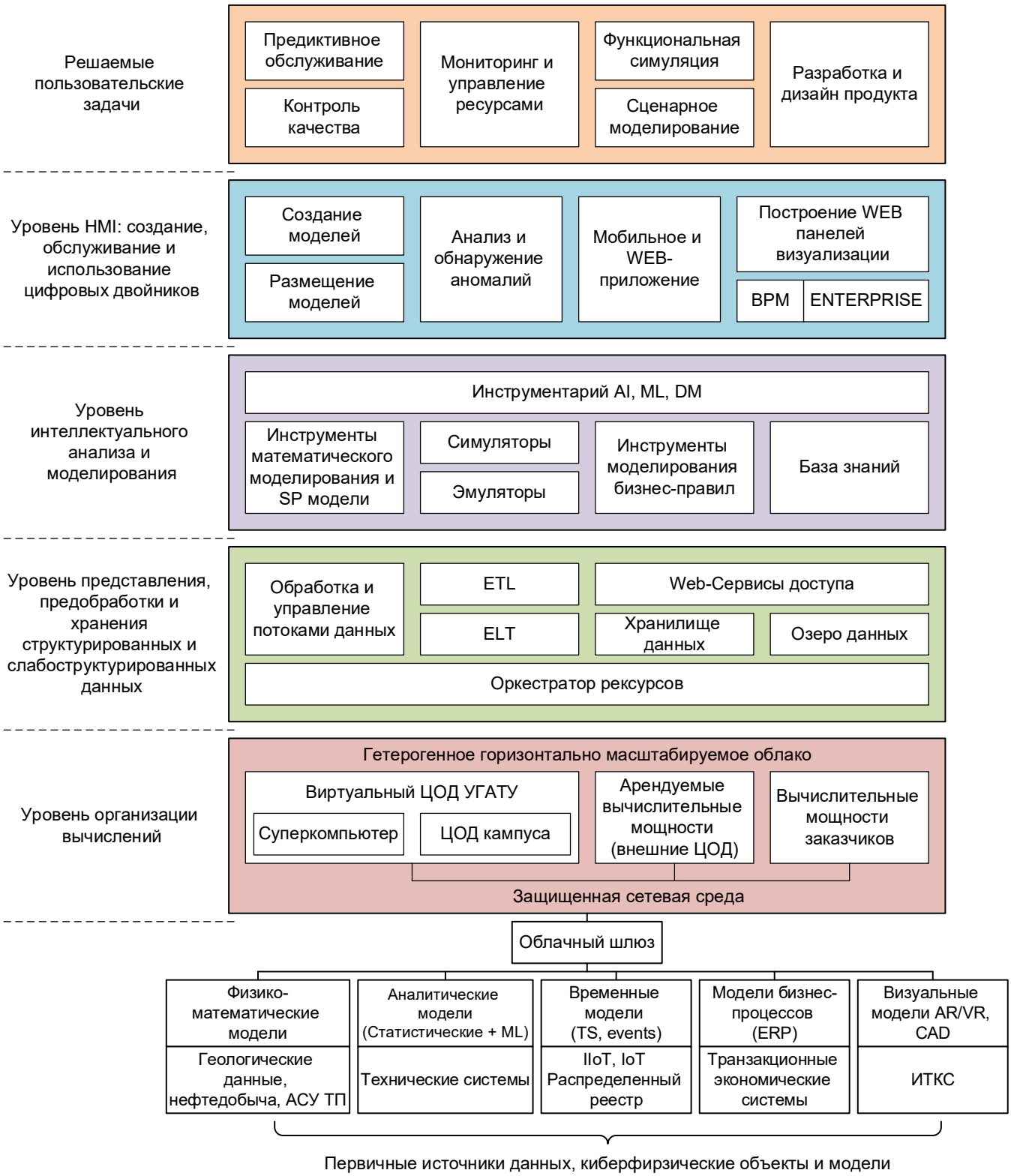


Рисунок 6.14– Обобщенная структура цифровой платформы анализа данных в задаче обеспечения кибербезопасности

6.2 Методика тестирования и оценка предложенных способов мониторинга целостности ТМИ

Тестирование представленного способа проводилось на выборке, включающей ТВР, полученные с модели САУ ГТД, и ТВР, полученные с борта ЛА. На ТВР, полученных с ЛА, накладывался шум, а также симулировались различные случаи нарушения целостности злоумышленником согласно описанной методике.

На ТВР, полученных с ЛА, накладывался шум, а также симулировались различные случаи нарушения целостности злоумышленником. В общем случае, подобные воздействия можно описать следующим выражением:

$$x(t) = \varepsilon(t) * (\varphi(x'(t))$$

где $x(t)$ – значение принимаемого параметра САУ ГТД в *t* момент времени,

$\varepsilon(t)$ – шум, накладываемый на сигнал в *t* момент времени,

$x'(t)$ – передаваемое значение параметра САУ ГТД в *t* момент времени, $\varphi(x'(t))$ – воздействие злоумышленника на передаваемое значение параметра САУ ГТД в *t* – момент времени.

Нарушитель может осуществлять следующие действия по нарушению целостности ТМИ [30]:

1) подмену базовой и/или абонентской радиостанции – подавление сигнала базовой/абонентской радиостанции и радиообмен с помощью собственной радиостанции нарушителя, передающей поддельную информацию;

2) отправку поддельной информации в радиоканал – создание пакета данных с поддельной телеметрической информацией и отправка его базовой/абонентской радиостанции;

3) повторную отправку ранее перехваченной в радиоканале информации – перехват легитимного сообщения, передаваемого по радиоканалу, и его повторная отправка участнику движения через некоторый период времени.

Для описания правил при принятии решения о целостности данных были введены лингвистические переменные, характеризующие каждый из параметров согласованности, представленные в таблице 6.3.

Таблица 6.3

Термы лингвистических переменных	Коэф. Детерминации	Евклидово расстояние	MAPE
низкий	x<0.6	x>3	x>15
средний	0.6<x<0.8	1<x<3	10<x<15

высокий	x>0.8	x<1	x<10

Исходя из перечисленных выше нарушений целостности и примеров анализа согласованности ТВР, можно сформулировать следующие типы атаки злоумышленника (Приложение И, фиг.6А, 6Б, 6В и 6Г): атаки, направленные на подделку данных, генерируемых датчиками САУ ГТД, т.е. самих параметров САУ ГТД (частоты вращения роторов высокого и низкого давления, расход топлива, температуру и давление газа и т.п.), и атаки, направленные на подделку управляющих и внешних воздействий (αРУД, высота полета, число Маха и т.п.). При подделке управляющих и внешних воздействий модель будет генерировать сигналы САУ ГТД, не соответствующие действительным значениям параметров полета. Подобные варианты атак представлены на рисунке 6Г (Приложение И). При такой атаке параметры согласованности принимают низкие значения, что позволяет однозначно указывают на наличие атаки, как показано в эксперименте 5Д.

При решении задачи кластеризации на типы согласованности выделены 7 типов согласованности, представленные в (Приложение И, таблица 3)

БПР реализует следующий набор правил, на основании которых выносится решение о целостности передаваемой ТМИ. Эти правила представлены в (Приложении И, таблице 4), где РРС – режим работы САУ двигателя (установившийся и переходный), СК – система контроля. Если сигнал К=1, САУ ГТД исправна, в противном случае К=0. При сигнале системы контроля К=0 данные, полученные с ЛА, будут считаться недействительными. Это выделено в особое событие для БПР «Отказ САУ ГТД».

Работу этих правил можно сопоставить с проделанным на (Приложение И, фиг. 5) экспериментом. Применение правил представлено в (Приложение И, таблице 5).

Тестирование алгоритма проводилось на 2500 тестовых ТВР. Каждая пара ТВР (ТВР с модели и ТВР, генерируемых САУ ГТД), представлял собой временное окно, состоящее из 100 отсчетов ТВР во временном окне. На некоторые данные, полученные с САУ ГТД, были произведены атаки злоумышленника, описанные в таблице 6 для получения разных типов согласования ТВР. Далее, для каждой пары вычислялись параметры согласования ТВР.

Примеры тестовой выборки параметров согласования и соответствующего типа согласованности представлены в (Приложение И, таблице 6)

Итоговой протокол экспериментов по классификации типа согласованности представлен в (Приложение И, таблице 7).

Итоговые протоколы по оценке целостности переданной с ЛА информации представлены в (Приложение И, таблицах 8, 9). Таблица 8 представляет собой протокол эксперимента для данных, переданных с САУ ГТД, находившейся в установившемся режиме полета. Таблица 9 представляет собой протокол эксперимента для информации, переданной с САУ ГТД, находившейся в переходном режиме полета. Таблица 6.4 представляет собой итоговый протокол эксперимента.

Таблица 6.4 – Итоговый протокол тестирования

Режим работы САУ ГТД	Количество тестовых выборок	Количество случаев успешного распознавания атаки	Оценка вероятности успешного распознавания атаки
Установившийся	3945	3498	0,89
Переходный	3415	2755	0,81
Итого	**5576**	**4670**	**0,85**

Таким образом, как видно из таблицы 10, оценка вероятности правильности принятого решения о типе согласованности ТВР, а, следовательно, и о целостности данных, принятых с борта ЛА, составила **0,85**.

Протокол второго этапа тестирования включает анализ 11207 подпоследовательностей трех пар тестовых ТВР:

– G – удельный расход топлива ($ТВР_1$);
– N – приведенная частота вращения ротора ($ТВР_2$);
– V – нормированная виброскорость подвески двигателя ($ТВР_3$).

Каждая пара ТВР (ТВР с модели и ТВР, генерируемых САУ ГТД), представляет собой подпоследовательность, попавшую во временное окно, состоящее из W_S отсчетов. На часть данных, полученных с САУ ГТД, были произведены атаки злоумышленника для получения разных типов согласования ТВР (таблица 6.5).

Таблица 6.5 – Количество подпоследовательностей анализируемых $ТВР_1$, $ТВР_2$, $ТРВ_3$, включающих нормальный режим работы САУ ГТД и атаки злоумышленника

Наличие атаки по каждому из анализируемых ТВР			Наличие атаки	Количество примеров подпоследовательностей
$ТВР_1$	$ТВР_2$	$ТВР_3$		
1	**1**	**1**	**1**	10925
0	**0**	**0**	**0**	9229
1	**0**	**1**	**1**	1413

	1	**0**	**1**	267
0	**1**	**1**	**1**	249
	0	**1**	**1**	49

Далее, для каждой пары ТВР вычислялись параметры согласованности и строились нейросетевые классификаторы. Итоговый протокол эксперимента приведен в таблице 6.6.

Таблица 6.6 – Итоговый протокол эксперимента по оценке вероятности успешного распознавания атаки

Номер	Способ	Тестовый ТВР	Оценка вероятности успешного распознавания атаки	Оценка F1 меры успешного распознавания атаки
1	Предложенный способ на основе методов кластеризации и классификации по одной паре ТВР	$ТВР_1$	0,850	0,820
2	Предложенный способ в случае анализа одной пары ТВР	$ТВР_1$	0,932	0,931
3		$ТВР_2$	0,954	0,950
4		$ТВР_3$	0,946	0,941
5		Взвешенная линейная комбинация	0,945	0,941
6	Предложенный способ в случае анализа двух пар ТВР	$ТВР_1$ и $ТВР_2$	0,951	0,950
7		$ТВР_1$ и $ТВР_3$	0,950	0,950
8		$ТВР_2$ и $ТВР_3$	0,951	0,951
9	Предложенный способ в случае анализа трех пар ТВР	$ТВР_1$, $ТВР_2$, $ТВР_3$	0,954	0,952
10	Предложенный способ в случае анализа трех пар ТВР в виде ансамбля моделей C^1, C^2, C^3	$ТВР_1$, $ТВР_2$, $ТВР_3$	0,962	0,960

Таким образом, как видно из таблицы 6.6, оценка вероятности правильности принятого решения о типе согласованности ТВР, а, следовательно, и о целостности данных, принятых с борта ЛА, составила **0,962**.

6.3 Оценка рисков ИБ системы сбора, хранения и обработки ТМИ о состоянии подсистем ЛА с помощью серых когнитивных карт

Возникающие неисправности и предотказные состояния бортовой аппаратуры летательного аппарата могут быть диагностированы на основе обрабатываемой ТМИ, что позволяет специалистам наземных технических служб планировать ремонтные и профилактические мероприятия на основе оценки текущего состояния оборудования. Накапливаемая и обрабатываемая ТМИ о фактическом состоянии отдельных модулей в процессе эксплуатации и всего комплекса бортовых систем ЛА в реальном масштабе времени на предприятие изготовитель (ПИ) узлов авиационной техники позволит повысить эффективность эксплуатации ЛА в штатном состоянии, при возникновении сбоев, а также атак злоумышленников – при расследовании инцидентов.

Целью является анализ защищенности системы сбора, хранения и обработки ТМИ о состоянии бортовых подсистем ЛА в аспекте обеспечения целостности ТМИ.

Физическая архитектура подсистемы сбора и хранения ТМИ на наземных станциях обслуживания ЛА построена в соответствии с NIST 800-82 и ISA/IEC 62443, анализ актуальных угроз и уязвимостей, построение графов атак и сценариев реализации атак приведено в Приложении Г.

С целью повышения эффективности оценки рисков ИБ с использованием НСКК было разработано специальное программное средство «Cognitive Map Constructor», используемое для построения иерархической модели НСКК и оценки рисков ИБ, обоснования выбора контрмер.

Помимо поддержки НСКК с установкой весов связей в виде верхних и нижних границ, программа допускает использование лингвистических термов нечеткой логики, а также задание весов в виде «белых» (четких) чисел.

На рисунке 6.16 приведен пример НСКК оценки рисков ИБ подсистемы сбора и хранения данных АИС, построенной в «Cognitive Map Constructor».

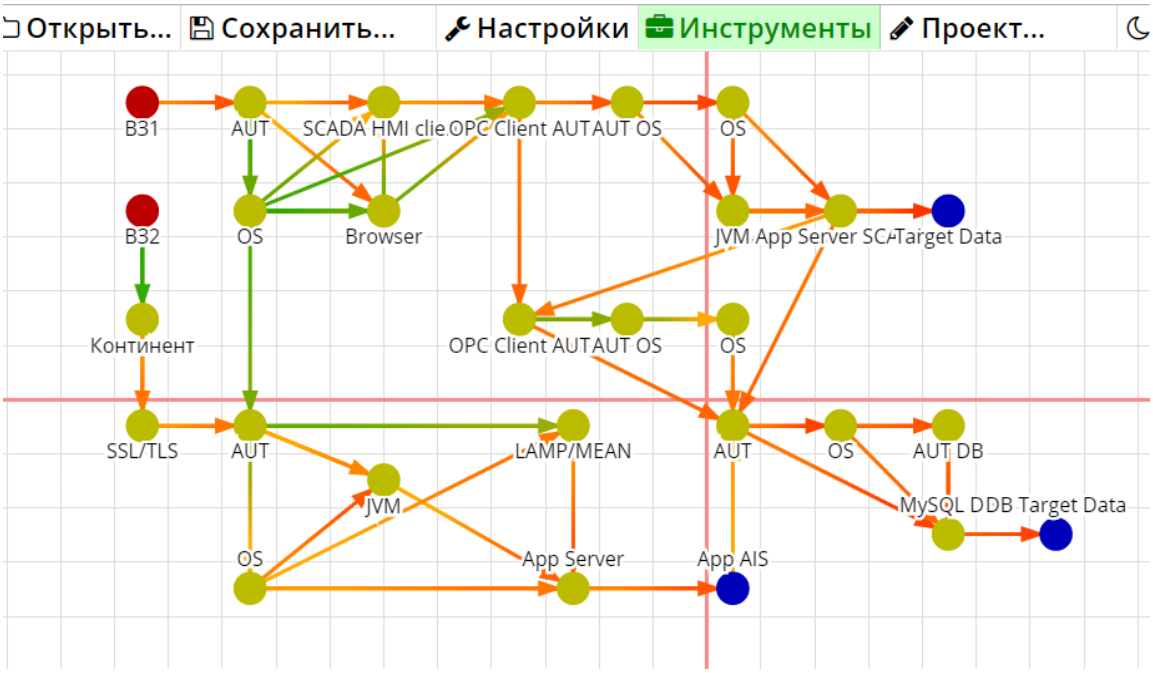


Рисунок 6.16 – НСКК для оценки рисков ИБ подсистемы сбора и хранения данных на станциях обслуживания (зона 1)

На рисунке 6.17 приведена НСКК оценки рисков ИБ, построенные в «Cognitive Map Constructor».

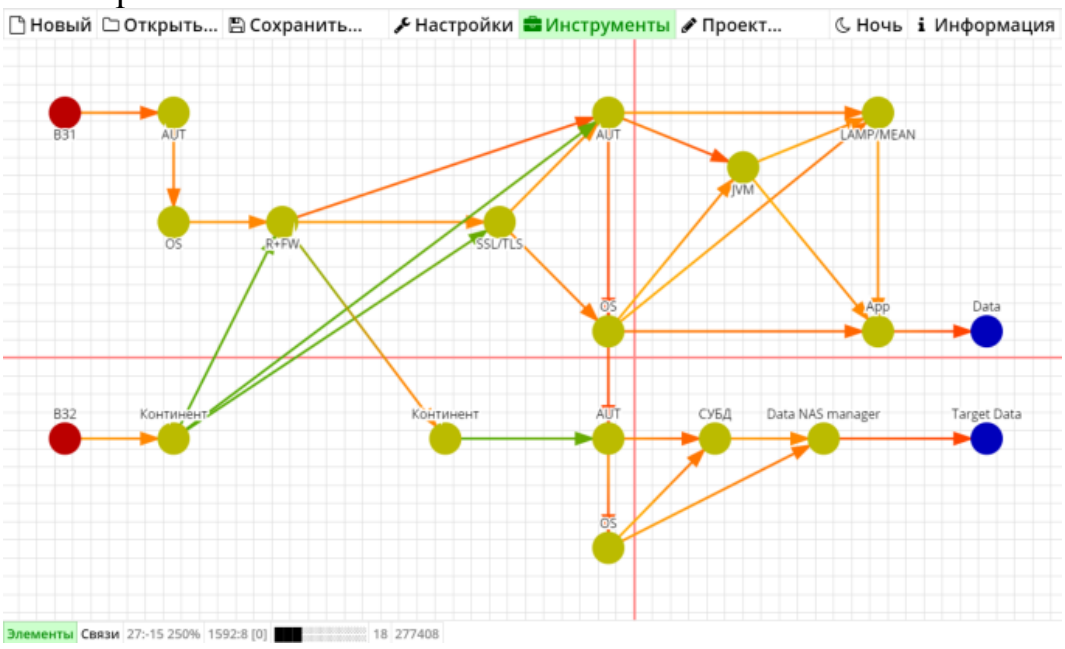


Рисунок 6.17 – НСКК для оценки рисков ИБ в ядре сети КИС предприятия-изготовителя (зона 2) и подсистеме хранения ТМИ с функциями отказоустойчивости (зона 3)

При нажатии на кнопку «Матрица достижимости» в подменю «Проект…» можно посмотреть матрицу весов взаимного влияния всех концептов НСКК (рисунок 6.18).

Матрица достижимости

	Все отключено						Все включено							
nt Browser	OS	OPC Client AUT	AUT OS	OS	JVM	App Server SCADA	Target Data	OPC Client AUT	AUT OS	OS	AUT	OS	AUT DB	M
B31	–	—	—	—	—	—	—	—	—	—	—	—	—	
AUT	— 0.3	—	—	—	—	—	—	—	—	—	—	—	—	
SCADA HMI client	–	0.55 — 0.65	—	—	—	—	—	—	—	—	—	—	—	
Browser	–	0.35 — 0.55	—	—	—	—	—	—	—	—	—	—	—	
OS	–	0.2 — 0.45	—	—	—	—	—	—	—	—	—	—	—	
OPC Client AUT	–	—	0.6 — 0.75	—	—	—	—	0.65 — 0.7	—	—	—	—	—	
AUT OS	–	—	—	0.75 — 0.8	0.6 — 0.75	—	—	—	—	—	—	—	—	
OS	–	—	—	—	0.65 — 0.75	0.6 — 0.75	—	—	—	—	—	—	—	
JVM	–	—	—	—	—	0.65 — 0.7	—	—	—	—	—	—	—	
App Server SCADA	–	—	—	—	—	—	0.7 — 0.85	0.55 — 0.65	—	—	0.65 — 0.7	—	—	
Target Data	–	—	—	—	—	—	—	—	—	—	—	—	—	
OPC Client AUT	–	—	—	—	—	—	—	—	0.35 — 0.4	—	0.65 — 0.7	—	—	
AUT OS	–	—	—	—	—	—	—	—	—	0.45 — 0.5	—	—	—	
OS	–	—	—	—	—	—	—	—	—	—	0.6 — 0.65	—	—	
AUT	–	—	—	—	—	—	—	—	—	—	—	0.65 — 0.8	—	0.
OS	–	—	—	—	—	—	—	—	—	—	—	—	0.7 — 0.75	0.
AUT DB	–	—	—	—	—	—	—	—	—	—	—	—	—	0.
MySQL DB	–	—	—	—	—	—	—	—	—	—	—	—	—	
DB Target Data	–	—	—	—	—	—	—	—	—	—	—	—	—	
AUT	–	—	—	—	—	—	—	—	—	—	—	—	—	
LAMP/MEAN	–	—	—	—	—	—	—	—	—	—	—	—	—	
JVM	–	—	—	—	—	—	—	—	—	—	—	—	—	
OS	–	—	—	—	—	—	—	—	—	—	—	—	—	
App Server	–	—	—	—	—	—	—	—	—	—	—	—	—	

Рисунок 6.18 – Матрица достижимости НСКК

Состояния концептов

	Все отключено						Все включено				
Browser	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11
OS	— 0.1711	0.0632 — 0.1712	0.0633 — 0.1713	0.0633 — 0.1713	0.0633 — 0.1713	0.0633 — 0.1713	0.0633 — 0.1713	0.0633 — 0.1713	0.0633 — 0.1713	0.0633 — 0.1713	0.0633 — 0.1713
OPC Client AUT	— 0.5376	0.2336 — 0.5393	0.2352 — 0.5401	0.2361 — 0.5406	0.2367 — 0.5407	0.2369 — 0.5408	0.2371 — 0.5409	0.2372 — 0.5409	0.2372 — 0.5409	0.2372 — 0.5409	0.2372 — 0.5409
AUT OS	— 0.357	0.1316 — 0.3628	0.1351 — 0.3659	0.1372 — 0.3674	0.1385 — 0.3683	0.1394 — 0.3687	0.1398 — 0.3689	0.1401 — 0.369	0.1403 — 0.3691	0.1404 — 0.3691	0.1404 — 0.3691
OS	— 0.2439	0.0859 — 0.2587	0.0921 — 0.2678	0.0964 — 0.2731	0.0993 — 0.2762	0.1012 — 0.2779	0.1025 — 0.2788	0.1033 — 0.2794	0.1038 — 0.2796	0.1041 — 0.2798	0.1041 — 0.2798
JVM	— 0.3506	0.1109 — 0.3805	0.1222 — 0.3997	0.1308 — 0.4116	0.137 — 0.4186	0.1414 — 0.4227	0.1444 — 0.425	0.1464 — 0.4263	0.1477 — 0.4271	0.1486 — 0.4275	0.1486 — 0.4275
App Server SCADA	– 0.2975	0.0904 — 0.3478	0.1066 — 0.3834	0.1201 — 0.407	0.1307 — 0.4219	0.1388 — 0.4309	0.1447 — 0.4363	0.1489 — 0.4394	0.1518 — 0.4412	0.1538 — 0.4422	0.1538 — 0.4422
Target Data	— 0.144	0.0384 — 0.1958	0.0508 — 0.2409	0.0626 — 0.276	0.0732 — 0.3013	0.0822 — 0.3185	0.0894 — 0.3296	0.0951 — 0.3366	0.0993 — 0.3408	0.1024 — 0.3434	0.1024 — 0.3434
OPC Client AUT	— 0.4263	0.1715 — 0.4605	0.1844 — 0.487	0.1954 — 0.5058	0.2045 — 0.5186	0.2119 — 0.5268	0.2176 — 0.5318	0.2219 — 0.5349	0.2251 — 0.5368	0.2273 — 0.5378	0.2273 — 0.5378
AUT OS	– 0.1329	0.0484 — 0.1506	0.0542 — 0.1658	0.0593 — 0.1784	0.0638 — 0.1881	0.0676 — 0.1952	0.0707 — 0.2002	0.0733 — 0.2036	0.0753 — 0.2058	0.0769 — 0.2072	0.0769 — 0.2072
OS	— 0.0457	0.0157 — 0.056	0.0187 — 0.0656	0.0216 — 0.0741	0.0241 — 0.0815	0.0264 — 0.0875	0.0284 — 0.0923	0.0301 — 0.0959	0.0315 — 0.0985	0.0327 — 0.1004	0.0327 — 0.1004
AUT	— 0.3669	0.1342 — 0.4379	0.1588 — 0.4948	0.1813 — 0.5368	0.2011 — 0.5658	0.2178 — 0.5852	0.2314 — 0.5979	0.2422 — 0.6061	0.2505 — 0.6114	0.2567 — 0.6148	0.2567 — 0.6148
OS	— 0.1735	0.0561 — 0.2293	0.0715 — 0.282	0.0871 — 0.3265	0.1021 — 0.3609	0.1159 — 0.3857	0.128 — 0.4028	0.1383 — 0.4141	0.1468 — 0.4215	0.1536 — 0.4262	0.1536 — 0.4262
AUT DB	— 0.0639	0.0216 — 0.0967	0.0304 — 0.1335	0.0402 — 0.1708	0.0505 — 0.2049	0.0609 — 0.2334	0.0709 — 0.2556	0.0801 — 0.2718	0.0882 — 0.2832	0.0952 — 0.291	0.0952 — 0.291
MySQL DB	— 0.2477	0.0828 — 0.3411	0.1104 — 0.4319	0.1397 — 0.5099	0.1695 — 0.5703	0.1983 — 0.6136	0.225 — 0.6431	0.2488 — 0.6627	0.2693 — 0.6754	0.2864 — 0.6837	0.2864 — 0.6837
DB Target Data	' — 0.09	0.0317 — 0.1431	0.0469 — 0.205	0.0647 — 0.2685	0.0846 — 0.3259	0.1054 — 0.3723	0.1264 — 0.4066	0.1465 — 0.4305	0.165 — 0.4465	0.1815 — 0.4569	0.1815 — 0.4569
AUT	— 0.1181	0.0392 — 0.1193	0.0395 — 0.12	0.0396 — 0.1204	0.0397 — 0.1206	0.0398 — 0.1207	0.0398 — 0.1208	0.0399 — 0.1208	0.0399 — 0.1208	0.0399 — 0.1208	0.0399 — 0.1208
LAMP/MEAN	— 0.0788	0.0185 — 0.0836	0.0193 — 0.0869	0.0199 — 0.0891	0.0202 — 0.0906	0.0205 — 0.0915	0.0207 — 0.0921	0.0207 — 0.0925	0.0208 — 0.0927	0.0209 — 0.0928	0.0209 — 0.0928
JVM	— 0.0996	0.0273 — 0.1054	0.0285 — 0.1094	0.0293 — 0.112	0.0298 — 0.1138	0.0301 — 0.1149	0.0303 — 0.1156	0.0304 — 0.116	0.0306 — 0.1162	0.0306 — 0.1164	0.0306 — 0.1164
OS	– 0.0548	0.0167 — 0.0569	0.0172 — 0.0582	0.0175 — 0.059	0.0176 — 0.0595	0.0178 — 0.0598	0.0178 — 0.06	0.0179 — 0.0601	0.0179 — 0.0602	0.0179 — 0.0602	0.0179 — 0.0602
App Server	— 0.1303	0.0287 — 0.1463	0.0313 — 0.1585	0.0333 — 0.1675	0.0347 — 0.1737	0.0357 — 0.1781	0.0364 — 0.181	0.0369 — 0.1829	0.0371 — 0.1842	0.0374 — 0.1849	0.0374 — 0.1849
App AIS	— 0.0654	0.0127 — 0.0814	0.015 — 0.0953	0.0169 — 0.1067	0.0184 — 0.1156	0.0196 — 0.1223	0.0205 — 0.1273	0.0212 — 0.1308	0.0217 — 0.1332	0.022 — 0.1348	0.022 — 0.1348
Континент	— 0.1478	0.0796 — 0.1478	0.0797 — 0.1478	0.0797 — 0.1478	0.0797 — 0.1478	0.0797 — 0.1478	0.0797 — 0.1478	0.0797 — 0.1478	0.0797 — 0.1478	0.0797 — 0.1478	0.0797 — 0.1478
SSL/TLS	— 0.095	0.0436 — 0.0953	0.0437 — 0.0954	0.0437 — 0.0954	0.0438 — 0.0955	0.0438 — 0.0955	0.0438 — 0.0955	0.0438 — 0.0955	0.0438 — 0.0955	0.0438 — 0.0955	0.0438 — 0.0955
B32	— 1	0.8 — 1	0.8 — 1	0.8 — 1	0.8 — 1	0.8 — 1	0.8 — 1	0.8 — 1	0.8 — 1	0.8 — 1	0.8 — 1

Рисунок 6.19 – Состояния концептов НСКК для оценки рисков зоны 1

Таким образом, разработанное программное средство «Cognitive Map Constructor» позволяет оценить эффективность применение системы мониторинга целостности ТМИ в защите телеметрической информации от воздействия внешних и внутренних угроз.

Рассмотрим численный пример оценки рисков ИБ для концепта C_1^*(рисунок 4.26) когнитивной карты из параграфа 4.4. Будем полагать, что при выборе серых значений весов НСКК необходимо ориентироваться на некоторую

нечеткую шкалу, определяющую силу связей между собой различных концептов (см. Таблицу 6.7).

Таблица 6.7 – Оценка силы связи между концептами

Лингвистическое значение силы связи	Числовой диапазон
Не влияет	0
Очень слабая	(0; 0,15]
Слабая	(0,15; 0,35]
Средняя	(0,35; 0,6]
Сильная	(0,6; 0,85]
Очень сильная	(0,85; 1]

Допустим далее, что эксперт оценил значения весов связей НСКК на рисунке 4.26 следующим образом (таблица 6.8).

Таблица 6.8 – Значения весов связей НСКК

Вес связи	Значение веса связи	Серость (разброс оценки)
$\otimes W_{T11,1}$	[0,6; 0,75]	0,075
$\otimes W_{T12,3}$	[0,5; 0,7]	0,1
$\otimes W_{T13,5}$	[0,5; 0,7]	0,1
$\otimes W_{T13,6}$	[0,15; 0,3]	0,075
$\otimes W_{T21,6}$	[0,55; 0,65]	0,05
$\otimes W_{12}$	[0,35; 0,55]	0,1
$\otimes W_{23}$	[0,55; 0,65]	0,05
$\otimes W_{24}$	[0,3; 0,5]	0,1
$\otimes W_{34}$	[0,15; 0,3]	0,075
$\otimes W_{54}$	[0,2; 0,45]	0,125
$\otimes W_{64}$	[0,24; 0,35]	0,055
$\otimes W_{65}$	[0,22; 0,37]	0,075

Используя для расчетов программное средство «Cognitive Map Constructor», выполним оценку изменения верхней и нижней границы переменной состояния концептов НСКК во времени $k = 1,2,3, \ldots$ (Таблицы 6.9, 6.10). Состояния входных концептов $T_1^1, T_1^2, T_1^3, T_2^1$ при этом были заданы как $[0,8; 1]$ для всех $k = 0,1,2, \ldots$; начальные условия для переменных состояния других концептов приняты нулевыми, т.е. равны $[0; 0]$.

Таблица 6.9 Верхние границы оценок состояния концептов

$\overline{X}_i$ \ k	1	2	3	4	5	6	7	8	9
$\overline{X}_1^{1,1}$	0,36	0,50	0,56	0,57	0,58	0,58	0,58	0,58	0,58
$\overline{X}_2^{1,1}$	0	0,10	0,19	0,24	0,27	0,29	0,29	0,30	0,30
$\overline{X}_3^{1,2}$	0,34	0,48	0,55	0,60	0,62	0,63	0,64	0,64	0,65
$\overline{X}_4^{1,2}$	0	0,10	0,19	0,26	0,31	0,33	0,35	0,36	0,36
$\overline{X}_5^{1,4}$	0,20	0,29	0,33	0,35	0,36	0,36	0,36	0,36	0,36

$\overline{X}_6^{1,3}$	0,27	0,39	0,44	0,46	0,47	0,47	0,48	0,48	0,48

Таблица 6.10 Нижние границы оценок состояния концептов

X_i \ k	1	2	3	4	5	6	7	8	9
$\underline{X}_1^{1,1}$	0,24	0,34	0,39	0,41	0,42	0,42	0,42	0,42	0,42
$\underline{X}_2^{1,1}$	0	0,04	0,08	0,11	0,13	0,13	0,14	0,14	0,14
$\underline{X}_3^{1,2}$	0,20	0,29	0,34	0,37	0,39	0,41	0,41	0,42	0,42
$\underline{X}_4^{1,2}$	0	0,28	0,51	0,63	0,68	0,70	0,71	0,71	0,71
$\underline{X}_5^{1,4}$	0,34	0,48	0,53	0,55	0,55	0,56	0,56	0,56	0,56
$\underline{X}_6^{1,3}$	0,44	0,60	0,65	0,66	0,67	0,67	0,67	0,67	0,67

В результате, установившееся значение серого вектора состояния $\otimes X$ для НСКК (т.е. для декомпозиции концепта C_1^*) находится как

$$\otimes X = \{[0{,}42; 0{,}58], [0{,}14; 0{,}30], [0{,}42; 0{,}65], [0{,}36; 0{,}71], [0{,}36; 0{,}56], [0{,}48; 0{,}67]\},$$

а искомое значение для состояния целевого концепта $C_4^{1,2}$ определяется серым числом $[0{,}36; 0{,}71]$.

Рассмотрим состояние целевого концепта C_R^*, т.е. ущерба, вызванного потенциальным нарушением целостности ТМИ в АИС, после уточнения значений всех весовых коэффициентов по уровням декомпозиции исходной НСКК. Предположим, что активной является внутренняя угроза T_1^*нарушения целостности ТМИ, уровень которой определяется серым числом $\otimes X_{T_1}^* \in [0{,}6; 0{,}95]$. Тогда получаем установившееся значение для оценки рисков ИБ вследствие нарушения целостности информации ТМИ: $\otimes X_R^* \in [0{,}19; 0{,}28]$.

Допустим далее, что в качестве возможной контрмеры для снижения ущерба от нарушения целостности ТМИ применяется дополнительная система мониторинга, развернутая в виде защищенного контейнера в Зоне 5. На рисунке 4.26 данная система обозначена как модуль контроля целостности ТМИ – концепт IST^5. Защищенный контейнер обеспечивает мониторинг целостности ТМИ в режиме онлайн и офлайн путем анализа оперативных данных и данных, собранных в хранилище (зона 3).

Как показали расчеты, оценка рисков ИБ вследствие нарушения целостности информации ТМИ после применения дополнительной контрмеры составляет $\otimes X_R^*|_A \in [0{,}07; 0{,}15]$, т.е. величина риска снижается в среднем в 2, 3 раза.

Оценка рисков для целевых концептов и оценка риска ИБ до и после реализации контрмер и состояние целевых концептов НСКК приведены на рисунке. 6.20.

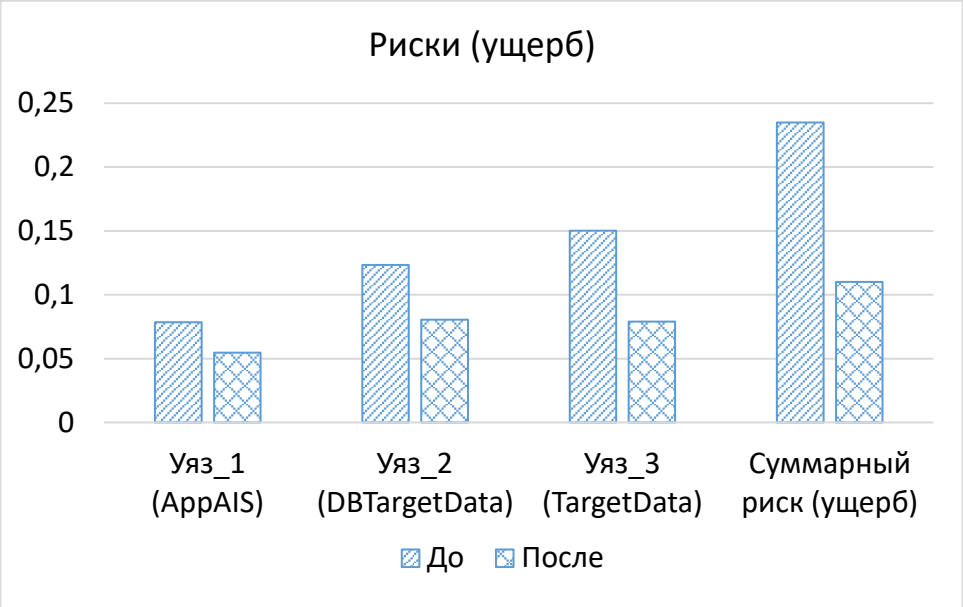


Рисунок 6.20 – Оценка рисков ИБ для целевых концептов и суммарного риска до и после реализации контрмер

Здесь: AppAIS – Эксплуатация уязвимости Web-приложения для запуска модуля доступа к БД оперативного хранения ТМИ на станциях обслуживания ЛА; DB Target Data – модификация оперативных данных ТМИ в БД хранения; Target Data – модификация ТМИ в долгосрочном хранилище.

Применение предложенного способа мониторинга целостности данных, получаемых с бортовых систем мобильного объекта, позволило снизить оценку суммарного риска ИБ для рассматриваемой системы на 45%.

Получены в рамках проведения научно-исследовательской работы по теме «Анализ и обеспечение информационной безопасности трафика передачи информации о состоянии агрегатов с борта летательного аппарата на предприятие» результаты, а именно:

– метод, алгоритмы и система мониторинга целостности телеметрической информации, получаемых с эксплуатируемой САУ ГТД летательного аппарата, и основанные на применении алгоритмов интеллектуального анализа многомерных технологических временных рядов;

– метод, модели и алгоритмы комплексной оценки рисков ИБ производственных объектов с использованием технологий нечеткого когнитивного моделирования и методов машинного обучения,

Практическая ценность предложенных решений заключается в возможности выявлять (до 85 % в развернутом тестовом окружении) несанкционированные воздействия на данные о состоянии САУ ГТД и тем самым повысить уровень защищенности информации при ее передаче с борта летательного аппарата на предприятие-изготовитель. Разработаны сценарии и графы атак для анализа защищенности системы с рекомендациями по повышению защищенности системы.

6.4 Оценка рисков ИБ АСУ ТП нефтедобывающего предприятия с помощью ансамбля когнитивных карт

Рассмотрим задачу оценки рисков ИБ АСУ ТП с использованием сценарного моделирования на основе рассмотренных выше разновидностей НКК и их ансамбля.

Цель: получение качественной и количественной оценки риска ИБ с учетом совокупности объективных и субъективных факторов неопределенности, влияющих на эти показатели для задач комплексной оценки рисков ИБ АСУ ТП промышленных объектов в условиях возможного воздействия на эти системы потенциальных внешних и внутренних угроз.

В качестве исследуемого объекта защиты рассматривается АСУ ТП нефтедобывающего предприятия, интегрированная в комплексную систему оперативного контроля и управления в реальном масштабе времени, и позволяющая передавать накапливаемые технологические данные в системы управления производственными процессами вышележащих уровней. Технологическая цепочка включает основные элементы: добыча нефти, сбор нефти, подготовка нефти, транспортировка товарной нефти. Результаты эксперимента приведены в Приложении К и в таблице 6.11.

Таблица 6.11 – Итоговые результаты моделирования рисков ИБ промышленного объекта

Тип НКК	R_5	R_7	R_{10}	R_{13}
НКК	0,466	0,096	0,353	0,015
НСКК	0,453	0,106	0,353	0,023
ИНКК	0,303	0,057	0,223	0,009
$\underline{R_i}$, НСКК	0,237	0,040	0,176	0,003
$\overline{R_i}$, НСКК	0,669	0,171	0,530	0,042
Среднее для всех карт	0,407	0,086	0,310	0,015
Отклонение	0,070	0,020	0,058	0,005

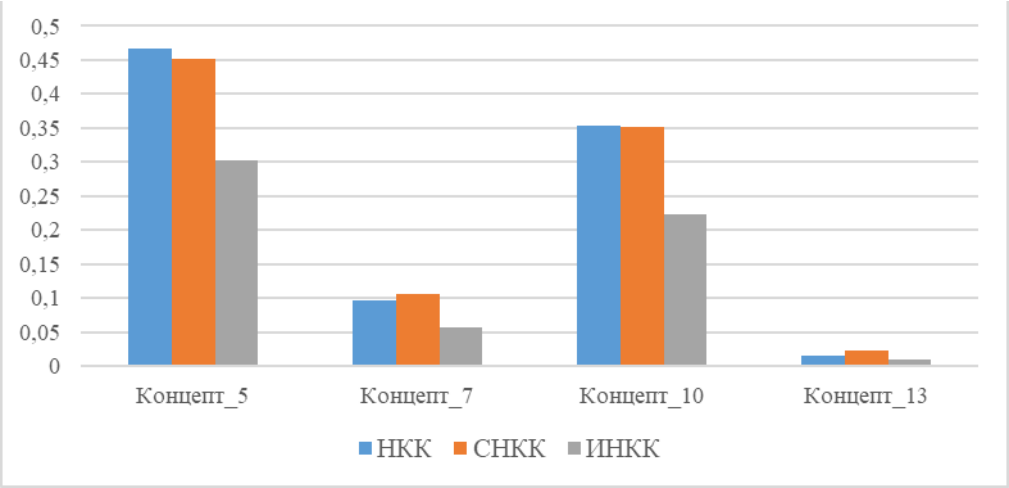


Рисунок 6.21 – Оценки рисков ИБ R_i для целевых концептов C_5, C_7, C_{10} C_{13}

Под риском R_i понимается потенциальный ущерб, наносимый i-ому активу АСУ ТП предприятия (в относительных единицах) и приводящей к нарушению целостности телеметрической информации, содержащей сведения о балансе материальных потоков на объекте (дебит жидкости, энергетические затраты и др.), и к нарушению хода самого ТП. Предполагается, что значение риска вычисляется как $R_i = X_i^*$, где X_i^* – установившееся значение состояния i-го целевого концепта (i = 5, 7, 10, 13).

Заметим, что средневзвешенная оценка рисков ИБ, формируемая с помощью ансамбля когнитивных карт (см. таблицу 6.11), более предпочтительна с точки зрения разброса оценок состояния целевых концептов, чем использование отдельных НКК. Разброс оценок состояния концептов ансамбля меньше, чем разброс оценок их серых значений с помощью НСКК, в среднем в 1,5-1,7 раза, что говорит о снижении влияния фактора субъективности на результаты оценки рисков.

Как следует из рисунка 6.21 и таблицы 6.11, наибольшее значение риска $R_5 = X_5^* = 0{,}41$ соответствует целевому концепту C_5 («Несанкционированное управление кустовой площадкой»), что, в свою очередь, указывает на необходимость принятия дополнительных мер по снижению этого показателя. Это может быть сделано, в частности, посредством применения соответствующих средств защиты информации: межсетевых экранов для сегментирования промышленной сети, локализации сетевого трафика внутри виртуальных сетей и т.п. Основные недостатки существующей конфигурации связаны с использованием учетных записей и параметров промышленных контроллеров и сетевого оборудования, задаваемых производителем по умолчанию. Аналогичные мероприятия,

направленные на снижение других показателей риска ИБ, позволят обеспечить предъявляемые требования к обеспечению кибербезопасности АСУ ТП. Как показало сценарное моделирование, применение средств защиты и организационных мер позволяет снизить оценку рисков ИБ на 10-15 %.

Таким образом, применение предложенной методики нечеткого когнитивного моделирования позволяет дать обоснованную качественную и количественную оценку показателей рисков ИБ АСУ ТП промышленного объекта с учетом мнений экспертов – специалистов в рассматриваемой предметной области, что, в свою очередь, может явиться основой для выбора эффективных защитных контрмер в соответствии с требованиями существующих нормативных документов.

При использовании технологий когнитивного моделирования в рамках предложенной методики одной из основных проблем является оценка силы связей концептов. Необходимо учитывать субъективное мнение каждого эксперта, и не сводить эти мнения к некоторой усредненной числовой оценке, а применять способы учета возникающей неопределенности за счет различных подходов к формализации знаний экспертов при построении НКК. Применение ансамбля нечетких когнитивных карт позволяет учесть неопределенность мнений экспертов в оценке риска ИБ по сравнению с оценками, получаемыми отдельными НКК. Разброс оценок состояния концептов ансамбля при этом меньше, чем разброс оценок их серых значений с помощью НСКК, в среднем в 1,5-1,7 раза, что говорит о снижении влияния фактора субъективности на результаты оценки рисков ИБ. Оценки рисков ИБ для целевых концептов после оптимизации распределения ресурсов, выделенных на контрмеры, уменьшились как в отношении разброса («серость»), так и в отношении центрального значения оценок («белизна») на 70-80 %. При этом не только возросла оценка эффективности использования контрмер, но и уменьшилась оценка стоимости их эксплуатации. Таким образом, предложенная методика позволяет получить качественную и количественную оценку показателей риска ИБ с учетом совокупности объективных и субъективных факторов неопределенности.

6.5 Оценка рисков ИБ на основе анализа и определения аномалий пользовательского окружения

6.5.1 Оценка эффективности алгоритмов интеллектуального анализа данных пользовательского окружения в задаче обнаружения удаленного управления

Предлагается следующая обобщенная структурная схема системы обнаружения удаленного подключения в среде виртуального окружения Web-браузера на основе анализа динамических биометрических признаков, представленная на рисунке 6.22. Введены следующие обозначения:

1) настоящий пользователь;
2) пользователь удаленного подключения;
3) параметры, фиксируемые в браузере на стороне клиента и пересылаемые на сервер (траектория движения мыши + клавиатурный почерк);
4) параметры пользовательской сессии (включая динамические биометрические признаки);
5) параметры, передаваемые в существующую систему анализа параметров пользовательского окружения;

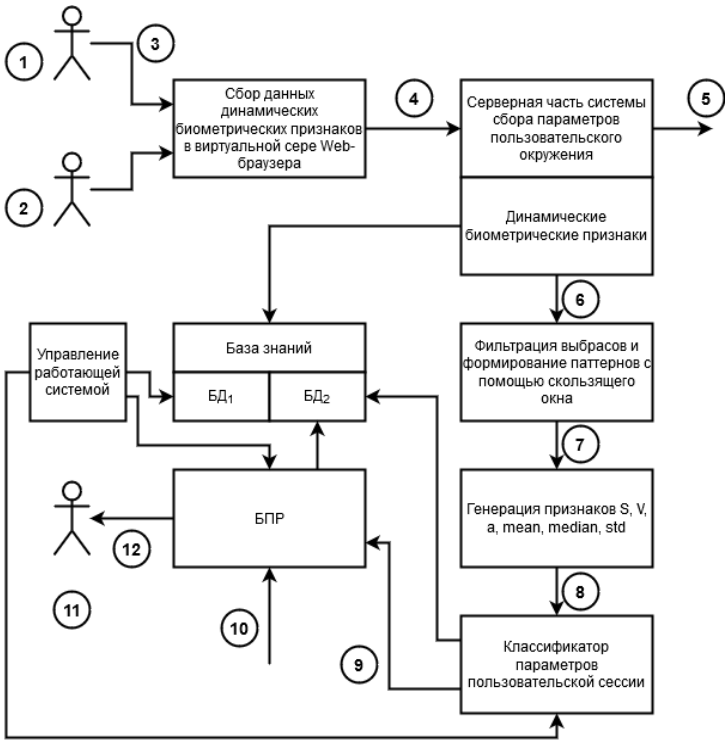


Рисунок 6.27 – Обобщенная структурная схема системы обнаружения удаленного подключения в среде виртуального окружения Web-браузера на основе анализа динамических биометрических признаков

6) фиксируемые динамические биометрические признаки;
7) подготовленные паттерны динамических биометрических признаков с привязкой к пользовательской сессии;
8) вектор признаков пользовательской сессии;
9) оценка вероятности наличия удаленного подключения;
10) оценка вероятности мошеннических действий из системы в рамках текущей сессии;
11) аналитик антифрод-системы;
12) оценка вероятности мошеннических действий в пределах сессии;

$БД_1$ – БД параметров пользовательской сессии;

$БД_2$ – параметры текущей работы предобработка и классификация.

Для анализа будем использовать динамические биометрические признаки – параметры использования компьютерной мыши, а именно:

– координаты точек промежуточной остановки указателя мыши;

– временные интервалы между началом движения мыши и ее остановкой.

Для имитации траектории движения пользователя построим кубический сплайн по промежуточным точкам остановки курсора мыши, фиксируемых внутри страницы Web-браузера. Применение кусочно-линейной интерполяции не позволяет приблизится к реальным траекториям движения курсора мыши и качественно оценивать длины соответствующих участков траектории.

Становится возможным определить скорости и ускорения на каждом временном интервале между двумя соседними точками траектории движения мыши.

Таким образом можно построить иерархию признаков, характеризующих участок траектории движения курсора мыши в окне Web-приложения, которые фиксируются и передаются в СМТ для последующего анализа. Финальный вектор признаков представлен в таблице 6.12.

Таблица 6.12 – Финальный вектор признаков

Временные отсчеты промежуточных событий движения курсора мыши	t	длительность одного сегмента траектории движения
	mean(t), $\bar{t}$	среднее значение длительности одного сегмента
	std(t), std_t	отклонение
	median(t), Me_t	медиана

Координаты точек промежуточных событий движения курсора мыши	s	длина одного сегмента траектории движения
	mean(s), $\overline{s}$	среднее значение длины одного сегмента
	std(s), std_s	отклонение
	median(s), Me_s	медиана
Относительная скорость движения курсора мыши между двумя промежуточными событиями движения	v	относительная скорость движения курсора мыши в сегменте траектории движения
	mean(v), $\overline{v}$	среднее
	std(v), std_v	отклонение
	median(v), Me_v	медиана
Ускорения движения курсора мыши между двумя промежуточными событиями движения	a	ускорение курсора мыши в сегменте траектории движения
	mean(a), $\overline{a}$	среднее
	std(a), std_a	отклонение
	median(a), Me_a	медиана

В качестве классификаторов будут использованы:

– KNN (классификатор *k*-ближайших соседей);

– RF (классификатор на основе комитета случайных деревьев, Random Forest).

Имеется два класса («удаленное управление» и «работа настоящего пользователя») и алгоритм, определяющий принадлежность каждого объекта одному из классов.

Сбор данных о пользовательском окружении осуществляется посредством скрипта JavaScript. В итоге полный набор признаков получился следующим: временные интервалы (64 признака), кубический сплайн по временным интервалам (64 признака), скорости (63 признака), ускорения (62 признака), медианы и средние значения по временным интервалам, кубическому сплайну по временным интервалам, скоростям и ускорениям (8 признаков). Для обучения были использованы разные группы признаков (см. таблица 6.13).

Таблица 6.13 – Группы признаков

№	Состав группы		Количество признаков
	Название	Обозначение	
1	Медианы и средние значения для временных интервалов, сплайна, скорости, ускорения	Me_t, Me_s, Me_v, Me_a, $\overline{t}$, $\overline{S}$, $\overline{v}$, $\overline{a}$	8
2	Временные интервалы, сплайн по временным интервалам, скорости, ускорения	*t, S, v, a*	252
3	Временные интервалы	*t*	64
4	Сплайн по временным интервалам	*S*	64
5	Скорости	*v*	63

6	Ускорения	*a*	62

Была использована перекрестная проверка с k=10 заходами. Лучший результат получился с использованием значений только временных интервалов (3 группа – 64 признака) и классификатора Random Forest, точность – 93,61% (см. рисунок 6.22).

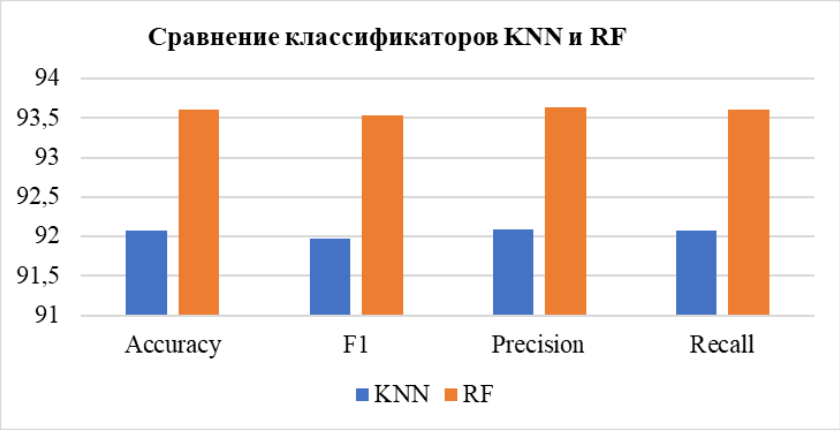


Рисунок 6.22 – Сравнение классификаторов KNN и RF. По оси ординат показатель качества классификации, %

Наибольшую эффективность показал алгоритм классификации «случайный лес» с группой признаков, состоящих из временных интервалов. Доля верных предсказаний для этого алгоритма составила 0,9361. Предложен подход на основе анализа изменения паттернов динамических биометрических признаков в случае удаленного управления сеансом.

Разработана структура системы обнаружения удаленного доступа с современным подходом к сбору и анализу пользовательского окружения в сочетании с методами машинного обучения. Применение методов машинного обучения позволит автоматизировать процесс адаптации системы к новым схемам мошенничества. Проведен анализ алгоритмов машинного обучения для анализа данных пользовательского окружения, рассмотрены алгоритмы классификации, а также различные метрики качества. Разработана методика сбора данных.

Проведен вычислительный эксперимент [107, 114] на натурных данных. Наибольшую эффективность показал алгоритм классификации «случайный лес» с группой признаков, состоящих из временных интервалов между событиями движения курсора компьютерной мыши. Доля верных предсказаний для этого алгоритма составила 93 % на тестовых данных.

6.5.2 Оценка рисков ИБ с использованием алгоритмов интеллектуального анализа текстовой метки банковской транзакции в задаче обнаружения аномалий пользовательского профиля

Система мониторинга банковских транзакций должна реализовывать механизмы поддержки принятия решений по процедурам онлайн контроля платежей клиентов-юридических лиц с учетом динамического профиля риска клиента.

Целью является повышение эффективности системы выявления высокорискованных транзитных операций на основе методов и алгоритмов интеллектуального анализа текстовой метки банковских транзакций.

Основной проблемой построения системы классификации назначения платежей является слабые требования к формализации текстовой метки со стороны банка, а также сама длина текстовой метки. Необходимо формирование семантических пространств каждой из категорий, указанных в нормативных документах, для улучшения показателей работы классификаторов.

Технологии дистанционного банковского обслуживания (ДБО) для доступа к счетам и операциям через веб-браузер не требуют установки клиентской части ПО и получили очень широкое распространение.

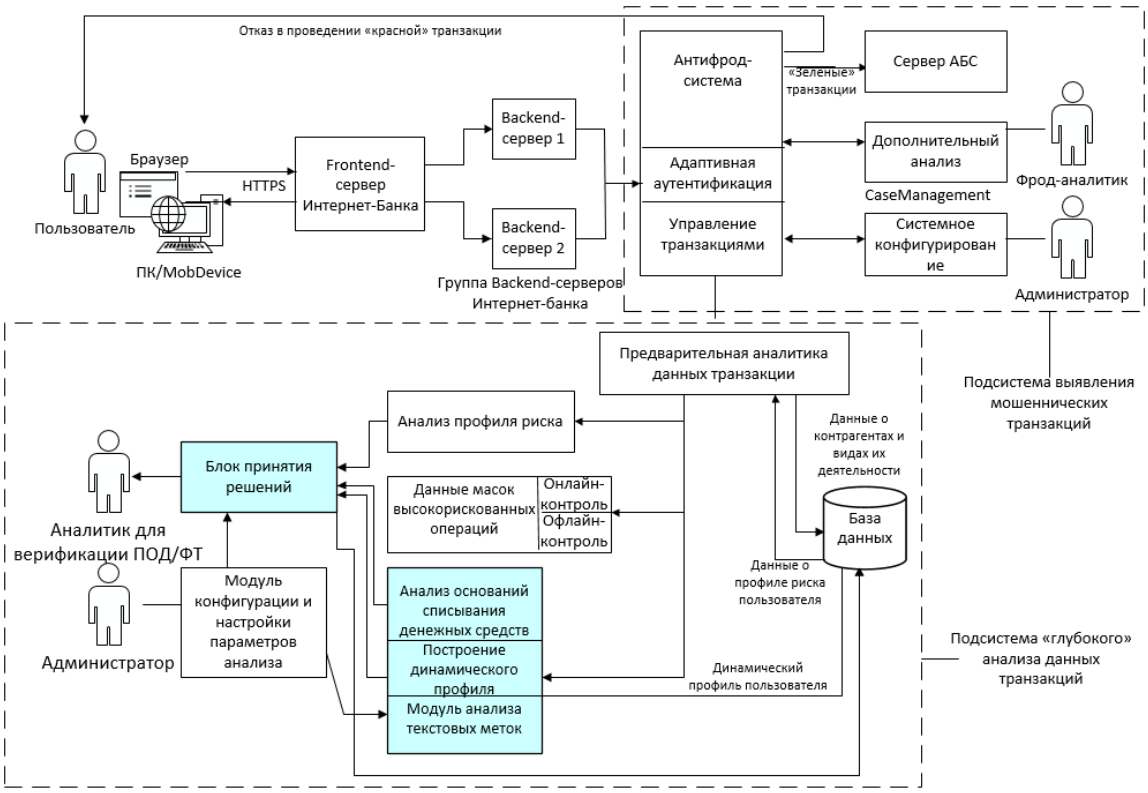


Рисунок 6.23 – Архитектура системы мониторинга банковских транзакций с модулем интеллектуального анализа текстовой метки

Анализ текстовой метки, сопровождающей банковские транзакции, позволяет провести более глубокий анализ активности клиента. Однако ввиду сложности такого анализа не представляется возможным генерировать новые правила для системы, основанной на сигнатурных проверках, поддерживать эти правила в актуальном состоянии и постоянно добавлять новые правила.

Необходим классификатор, который может оперативно анализировать текстовую метку и классифицировать её в соответствии с кодом ОКВЭД.

Дальнейшая работа со словарями подразумевает построение нейросетевого классификатора для комплексной разметки поступающих данных текстовых меток назначений платежей и классификатора на основе алгоритмов интеллектуального анализа данных.

Разработанная структура подсистемы обработки текстовых меток назначения платежей с помощью нейросетевого блока анализа представлена на рисунке 6.24.

Рисунок 6.24 – Структура подсистемы обработки текстовых меток назначения платежей с помощью нейросетевого блока анализа

Разработанный конвейер обработки текстовых данных с помощью методов интеллектуального анализа представлен на рисунке 6.25.

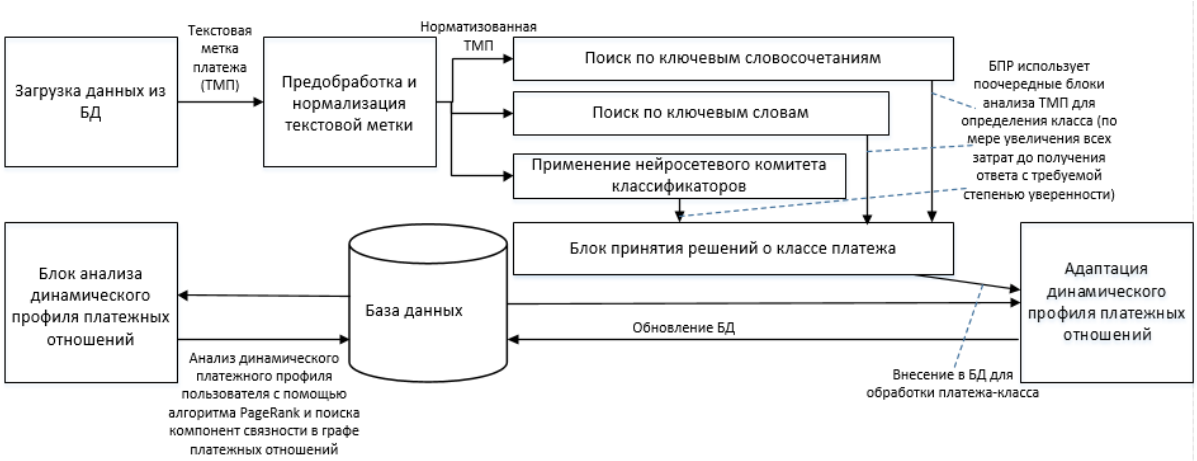


Рисунок 6.25 – Конвейер обработки текстовых данных с помощью методов интеллектуального анализа в составе модуля СМТ

Предлагаемый алгоритм интеллектуального анализа текстовой метки, сопровождающей банковские транзакции, составит из множества этапов. Среди них можно выделить 3 группы:

– работа со словарями;
– предобработка текстовой метки;
– классификация текстовой метки.

При оценке эффективности предложенных алгоритмов работы модуля интеллектуального анализа использовалась база примеров, содержащая по 1000 примеров в 10 классах. Сводные параметры классификаторов приведены в табл. 6.14.

Таблица 6.14 – Результаты, полученные с использованием группы классификаторов

Метод формирования пространства признаков	Классификатор	Значение метрик на тестовой выборке			
		Accuracy (правильность)	Precision (точность)	Recall (полнота)	F_1 (совместная оценка)
Bag of Word (BOW) (мешок слов)	Логистическая регрессия	0,878	0,878	0,878	0,877
BOW + XGboost	XGBoost (градиентный бустинг)	-	0,82	0,82	0,82
N-gramm+TF-IDF (метод оценки важности Нграмм в документе)	XGBoost	-	0,72	0,72	0,72
TF-IDF+PCA (метод оценки важности слова в документе + метод главных компонент)	K Nearest Neighbor (метод ближайших соседей)	0,80	0,80	0,80	0,80
	Stochastic Gradient Descent (стохастический градиентный спуск)	0,80	0,80	0,80	0,80
	Random Forest (случайный лес)	0,77	0,77	0,77	0,77
	AdaBoost (адаптивный бустинг)	0,71	0,70	0,71	0,70
	Gaussian Naive Bayes (наивный Байесовский классификатор)	0,70	0,71	0,70	0,70
	Decsision Tree (дерево решений)	0,69	0,69	0,69	0,69
Word2Vec (приведение слова в векторную форму)	Логистическая регрессия	0,768	0,769	0,768	0,768
	CNN (сверточные нейронные сети)	0,84	-	-	0,89

Для оценки результатов классификации применяются метрики, основывающиеся на основных показателях классификации:

- Истинно положительные (TP).
- Истинно отрицательные (TN).
- Ложно положительные (FP).
- Ложно отрицательные (FN).

$$M = \begin{pmatrix} TP & FP \\ FN & TN \end{pmatrix}$$

$$f1 = 2 \cdot \frac{precision \cdot recall}{precision + recall}$$

$$precision = \frac{TP}{TP + FP}$$

$$recall = \frac{TP}{TP + FN}$$

С использованием композиции классификаторов достигнута точность классификации 81% (на тестовом множестве при перекрестной проверке), тогда как базовая версия алгоритма (при помощи регулярных выражений) позволяла достичь классификации с точностью около 60%.

6.5.3 Определение аномалий пользовательского окружения в составе системы мониторинга транзакций

Для повышения эффективности выявления мошеннических транзакций предлагается [107, 151, 174, 181] интегрировать в состав данной системы модуль, способный выполнять анализ данных пользовательского окружения с целью выявления потенциальных мошеннических действий. Для анализа подобных данных необходимо реализовать сбор информации, хранение и интерфейс доступа для применения инструментов ИАД. Для анализа эффективности методов интеллектуального анализа данных была использована база банковских транзакций UCSD-FICO data mining contest 2009. Для всех классификаторов выполнена одиночная проверка на обучающем и тестовом множествах и затем, для оценки обобщающей способности, 10-кратная перекрестная проверка (k-fold cross validation).

Для оценки результатов классификации, как правило, применяются метрики точность (precision), полнота (recall), F1 и коэффициент корреляции Мэтьюса (MCC):

$$MCC = \frac{(TP \cdot TN) - (FP \cdot FN)}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}.$$

Таблица 6.15 – Сравнение результатов с работами других авторов

Название статьи	**Алгоритмы**	**MCC**
A novel credit card fraud detection model based on frequent itemset mining	Алгоритм Apriori	0,78
	Метод опорных векторов (SVM)	0,39
	Метод k-ближайших соседей (k-nn)	0,62
	Метод наивного Байеса (NB)	-0,21
	Алгоритм случайного леса (RF)	0,64
Data mining techniques for credit card detection: empirical study	Метод k-ближайших соседей (k-nn)	0,47
	Деревья решений	0,41
	Метод наивного Байеса (NB)	0,51
	Метод опорных векторов (SVM)	0,39
	МСП с 10-кратной перекрестной проверкой	0,82

Предлагаемый алгоритм интеллектуального анализа данных банковских транзакций в составе системы противодействия финансовому мошенничеству	RF с 10-кратной перекрестной проверкой	**0,91**
	Метод опорных векторов (SVM) с 10-кратной перекрестной проверкой	0,78

Характеристики рассмотренных в данной классификаторов сравнимы и в ряде случаев превосходят значения классификаторов, реализованных авторами указанных статей. Это объясняется тем, что для серии экспериментов устранен перекос в размерности классов.

Развитием данной системы является мониторинга банковских транзакций на основе методов интеллектуального анализа является сбор и анализ информации о пользовательском окружении. Для проведения эксперимента были собраны данные о посетителях трех веб-страницы, с внедренным скриптом сбора информации о пользовательском окружении по 40 основным параметрам.

Выявлена устойчивая структура образов, отражающая совокупность отпечатков пользовательских окружений со следами и без следов удаленного управления.

Характеристики рассмотренных нейросетевых классификаторов в задаче определения мошеннических транзакций по результатам анализа данных базы сравнимы и в ряде случаев превосходят значения классификаторов, реализованных авторами статей. Это объясняется тем, что для серии экспериментов устранен перекос в размерности классов.

Классификатор на основе случайного леса показал наилучшие результаты среди рассмотренных классификаторов. Он позволяет получить меньшее количество ложно отрицательных и ложно положительных ошибок. К достоинствам данного алгоритма можно отнести простоту используемой модели и эффективность параллельной реализации вычислительной схемы.

Таким образом, с помощью алгоритмов кластерного анализа на основе карты самоорганизации Кохонена и иерархических алгоритмов кластеризации выявлена устойчивая структура образов, отражающая совокупность отпечатков пользовательских окружений со следами и без следов удаленного управления.

6.5.4 Проектирование структурной и функциональной схемы обработки данных пользовательского окружения в составе системы обнаружения аномалий

Реализация алгоритмов [105, 107-109, 114, 150, 151] выявления финансового мошенничества на основе ИАД банковских транзакций в составе системы распределенной обработки данных банковских транзакций требует решения ряда задач, связанных с проектирование и развертыванием соответствующей инфраструктуры для хранения и обработки накапливаемых данных.

На сегодняшний день существует множество инструментов распределенной обработки данных банковских транзакций (фреймворки: Hadoop, Apache Spark, ClickHouse, ElasticSearch, Splunk Free). Предлагаемая структура системы распределенной обработки данных банковских транзакций представлена на рисунке 6.26.

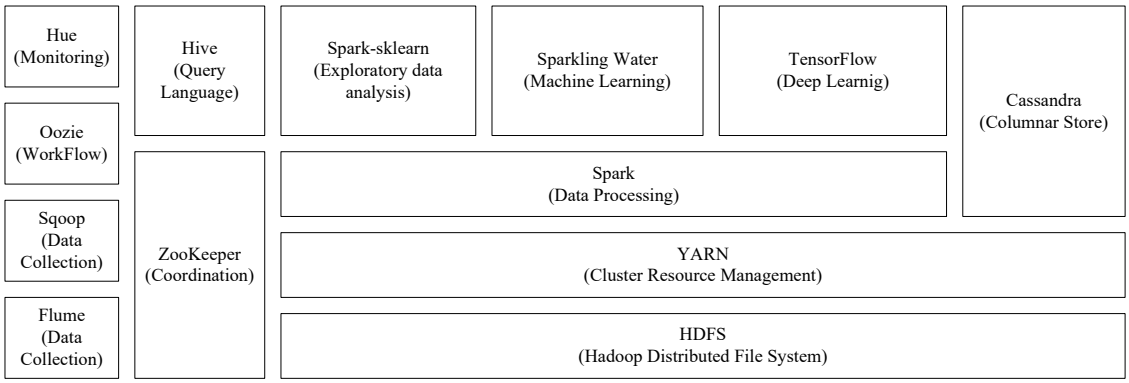


Рисунок 6.26 – Структура кластера Hadoop

Основным элементом системы распределенной обработки данных банковских транзакций является распределенная файловая система. Наиболее популярной на сегодняшний день является HDFS.

Следующий элемент системы обработки больших данных – инфраструктура распределенного программирования и машинного обучения. Ядром этого элемента является Spark – инфраструктура кластерных вычислений, сходная в MapReduce. В состав данной инфраструктуры входит и инструмент машинного обучения MLLib, позволяющий реализовать инструменты ИАД накапливаемых данных.

Структура программно-аппаратного стенда для тестирования алгоритмов выявления аномалий пользовательского окружения на основе ИАД на основе выбранного стека технологий обработки Big Data представлена на рисунке.

Модуль сбора и анализа данных представляет собой

– комплекс ПО Sentry для сбора логов скрипта клиентской стороны,

– сервис Gitlab для организации совместной работы над исходным кодом реализуемых алгоритмов анализа,

– DVWA (Damn Vulnerable Web Application) для тестирования скрипта сбора данных по пользовательском окружении.

Модуль нагрузочного тестирования предназначен для автоматизации сбора базы данных о пользовательском окружении.

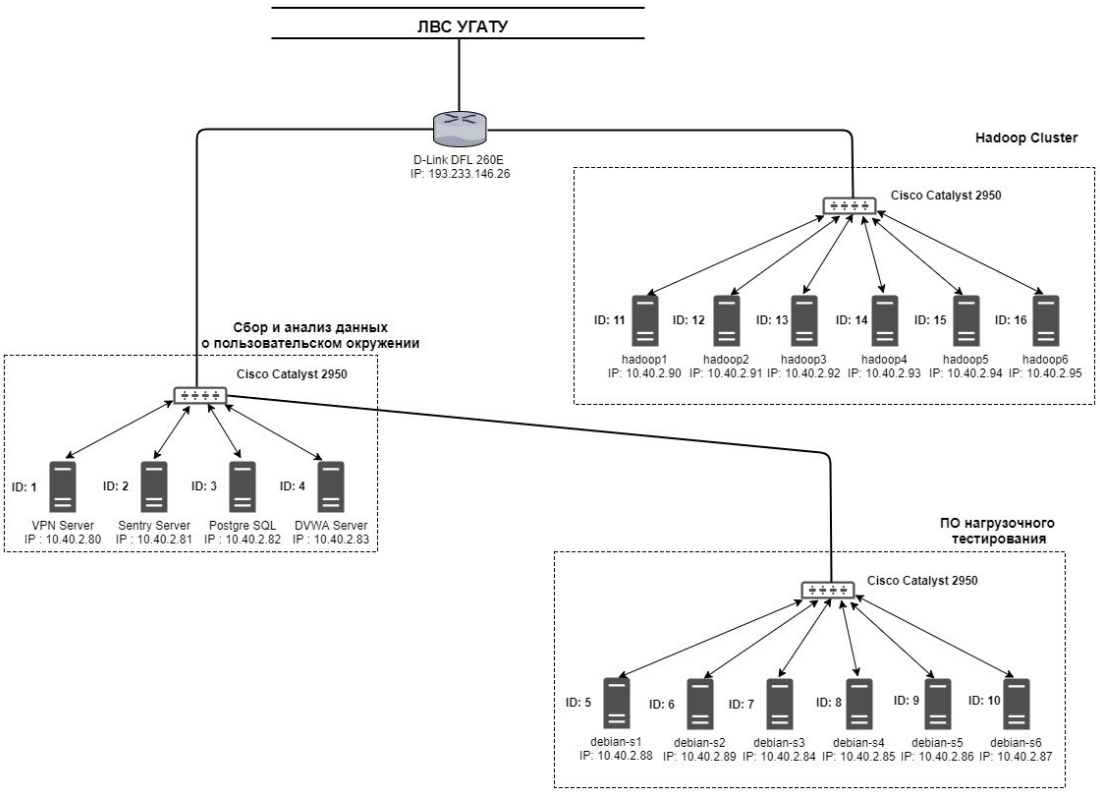


Рисунок 6.27 – Структура программно-аппаратного стенда для тестирования алгоритмов обнаружения аномалий пользовательского окружения

Типовая конфигурация используемого серверного парка машин приведена в таблице 6.16.

Таблица 6.16 – Параметры серверов

ID	Сектор	IP	Конфигурация	ОС	Модель
1	Сбор и анализ данных о пользовательском окружении	10.40.2.80	2x3.4 GHz / 4GB DDR2	debian 8.2	HP ProLiant DL360 G4
2	Сбор и анализ данных о пользовательском окружении	10.40.2.81	2x3.4 GHz / 2GB DDR	debian 8.2	HP ProLiant DL360 G4
3	Сбор и анализ данных о пользовательском окружении	10.40.2.82	2x3.0 GHz / 1GB DDR	ubuntu 16.04	HP ProLiant DL360 G4

4	Сбор и анализ данных о пользовательском окружении	10.40.2.83	1x2.4 GHz / 1GB DDR	ubuntu 16.04	HP ProLiant DL360 G3
5	ПО нагр. тестир.	10.40.2.88	2x3.0 GHz / 3GB	debian 9.2	HP ProLiant DL360 G4
6	ПО нагр. тестир.	10.40.2.89	2x3.0 GHz / 3GB	debian 9.2	HP ProLiant DL360 G4
7	ПО нагр. тестир.	10.40.2.84	2x3.0 GHz / 4GB	debian 9.2	HP ProLiant DL360 G4
8	ПО нагр. тестир.	10.40.2.85	2x3.0 GHz / 3GB	debian 9.2	HP ProLiant DL360 G4
9	ПО нагр. тестир.	10.40.2.86	2x3.0 GHz / 4GB	debian 9.2	HP ProLiant DL360 G4
10	ПО нагр. тестир.	10.40.2.87	2x3.0 GHz / 3GB	debian 9.2	HP ProLiant DL360 G4
11	Hadoop Cluster	10.40.2.90	2x3.4 GHz / 12GB DDR2	ubuntu 14.04	HP ProLiant DL380 G4
12	Hadoop Cluster	10.40.2.91	2x3.4 GHz / 12GB DDR2	ubuntu 14.04	HP ProLiant DL380 G4
13	Hadoop Cluster	10.40.2.92	2x3.4 GHz / 8GB DDR2	ubuntu 14.04	HP ProLiant DL360 G4
14	Hadoop Cluster	10.40.2.93	2x3.4 GHz / 6GB DDR2	ubuntu 14.04	HP ProLiant DL360 G4
15	Hadoop Cluster	10.40.2.94	2x3.2 GHz / 6GB DDR2	ubuntu 14.04	HP ProLiant DL360 G4
16	Hadoop Cluster	10.40.2.95	2x3.0 GHz / 6GB DDR2	ubuntu 14.04	HP ProLiant DL360 G4

Основной проблемой повышения точности выявления аномалий пользовательского окружения является недостаточный объем фиксируемых параметров, передаваемых с клиентской стороны онлайн-банкинга в процессинговый центр, и несовершенство методов и алгоритмов сигнатурного анализа в силу низких возможностей по адаптации и гибкой настройке.

Предложена инфраструктура для сбора и анализа данных пользовательского окружения в составе системы выявления аномалий пользовательского окружения на основе технологий обработки больших данных.

6.6 Обнаружение аномалий ИТКС

Для тестирования предлагаемых моделей машинного обучения разработана архитектура стенда промышленного объекта, имитирующая основные элементы инфраструктуры (рисунок 6.28), и включающая основные уровни: полевой, сбора данных, управления и т.п. Мониторинг состояния информационной и сетевой инфраструктуры реализован на основе развернутого решения на базе ELK-стека (Elasticsearch, Beats, Logstash, Kibana) [51].

Процесс мониторинга [51] разбит на 5 шагов.

1. Источником событий выступают AuditBeat и WinlogBeat на серверах.
2. Данные собираются в SIEM-системе Apache NiFi.
3. Хранение происходит в Elasticsearch.
4. Данные обрабатываются и визуализируются с помощью Kibana.
5. Полученная информация анализируется экспертами.

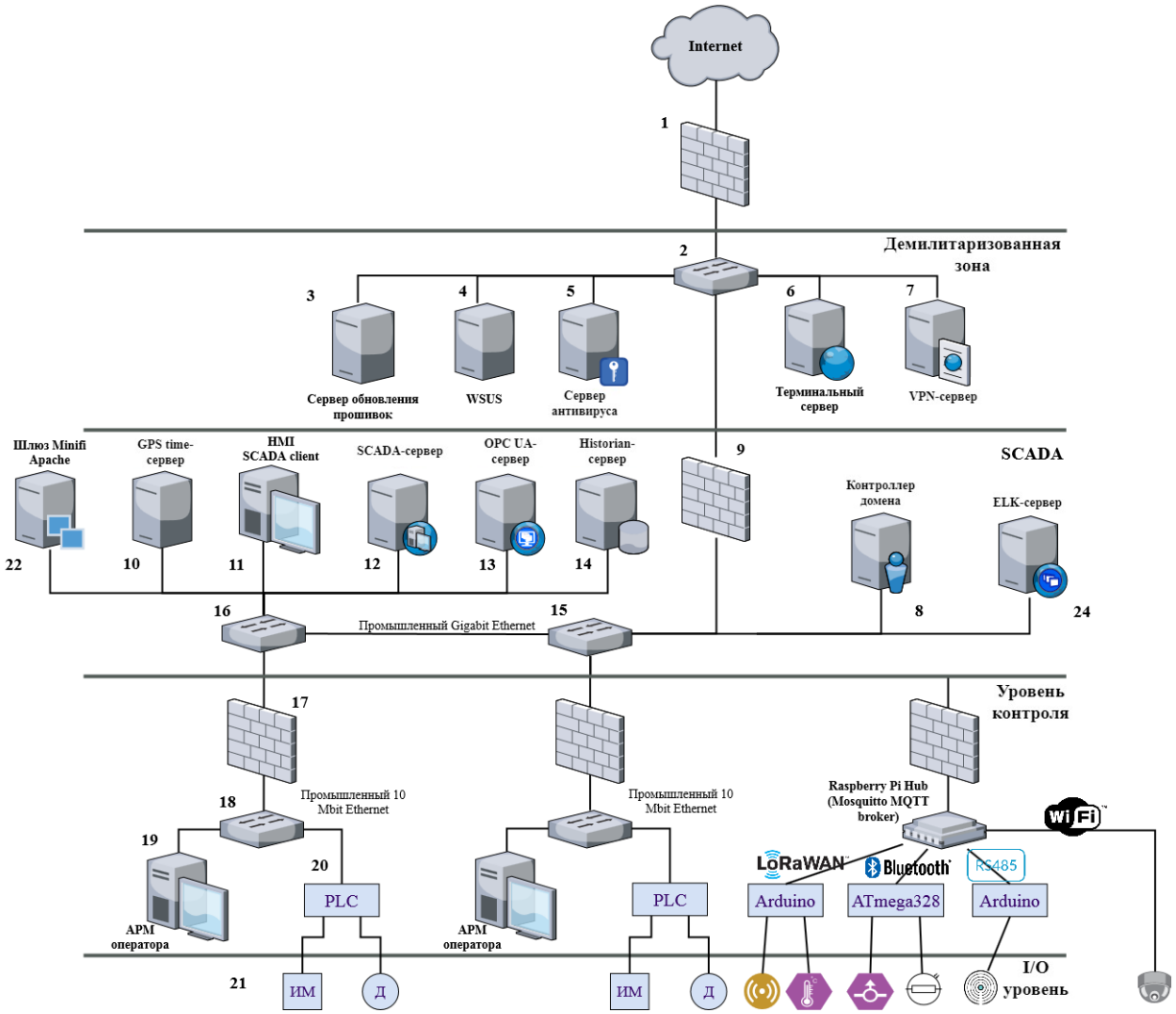


Рисунок 6.28 – Архитектура стенда промышленного объекта (ИМ – исполнительные механизмы, Д – датчики)

Упрощенная схема системы сбора и обработки данных о событиях ИБ модельного объекта приведена на рисунке 6.29.

Данные поступают в систему мониторинга, сбора и корреляции событий ИБ в промышленной сети через коллектор данных (реализованный при помощи MQTT-брокера). Связующим звеном является Apache NiFi сервер, пересылающий полученные данные в Elasticsearch, где к ним может иметь доступ подсистема машинного обучения на базе TensorFlow.

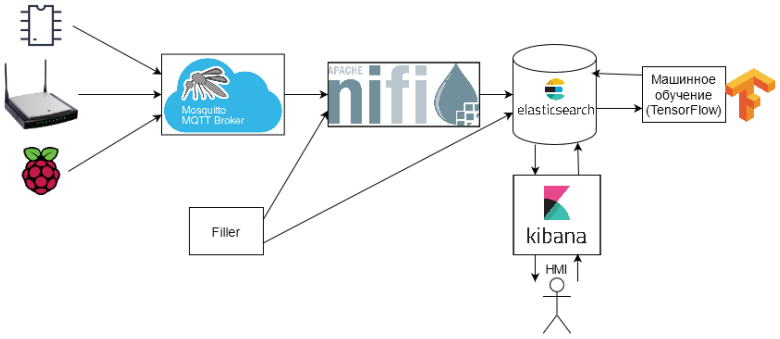


Рисунок 6.29 – Упрощенная схема системы сбора и обработки данных о событиях ИБ модельного объекта (Filler – источник дополнительных данных о событиях ИБ)

Согласно архитектуре стенда (рис. 6.28 и 6.29), в системе эмуляции и виртуализации EVE-NG [300] спроектирован и реализован стенд следующего вида (рис. 6.30).

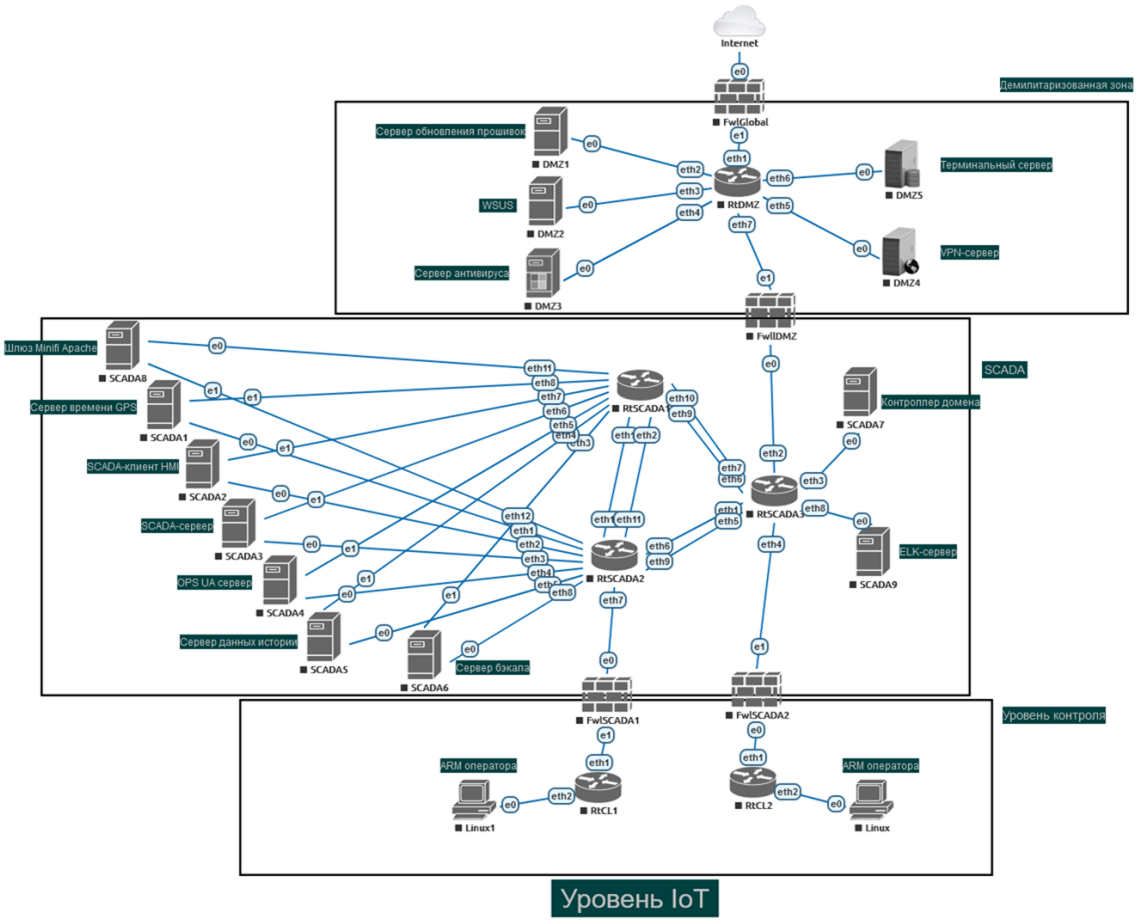


Рисунок 6.30 – Архитектура разработанного стенда сегмента промышленной сети (e0-e1, eth0-eth10 – нумерация сетевых интерфейсов)

ELK-сервер (24) осуществляет сбор всех типов данных для их последующего использования в системе машинного обучения распознавания аномалий сетевого трафика.

Эксперименты в виртуальном полигоне с разработанными ML-моделями и сценариями реализации сетевых атак подтвердили эффективность

предлагаемого решения.

Проанализированы варианты построения ансамблей и комитетов классификаторов на основе традиционных моделей машинного обучения (модели случайного леса, рандомизированные деревья решений и пр.) и гетерогенных нейросетевых моделей (глубокие нейронные сети, сверточные нейронные сети и модели на основе автоенкодеров с долгой краткосрочной памятью). Оценка F1-меры при работе с тестовыми выборками достигает 96%.

Проанализирована возможность встраивания полученных моделей в качестве модулей сетевого оборудования для повышения оперативности анализа сетевого трафика промышленных систем или использования в составе сетевой системы обнаружения вторжений.

Эффективность полученных решений при оценке качества обнаружения сетевых атак на исходных наборах данных сравнима для протестированных моделей. Наиболее перспективным для применения в специализированных сигнальных процессорах сетевого оборудования является классификатора на основе комитета случайных деревьев. Данный классификатор обеспечивает хорошее качество обнаружение сетевых атак и не требует значительных вычислительных ресурсов при запуске модели с подобранными в процессе обучения коэффициентами. Разработан виртуальный полигон для оценки эффективности применения ML-моделей для обнаружения сетевых атак.

6.7 Выводы по главе

Способ и система обнаружения нарушений целостности ТМИ позволяют выявлять несанкционированные воздействия на данные о состоянии САУ ГТД и тем самым повысить уровень защиты информации при ее передаче с борта ЛА на предприятие-изготовитель. Практическая ценность предложенных решений заключается в возможности выявлять (до 85 % в развернутом тестовом окружении) несанкционированные воздействия на данные о состоянии САУ ГТД и тем самым повысить уровень защищенности информации при ее передаче с борта летательного аппарата на предприятие-изготовитель. Разработаны сценарии и графы атак для анализа защищенности системы с рекомендациями по повышению защищенности системы. Применение предложенного способа мониторинга целостности данных, получаемых с бортовых систем мобильного объекта, позволило снизить оценку риска ИБ для рассматриваемой системы на 45%.

Рассмотрена процедура оценки рисков ИБ промышленной сети АСУ ТП нефтедобывающего предприятия с использованием когнитивного моделирования на основе классических, серых и интуиционистских НКК и их ансамбля. Реализованы основные стадии анализа и моделирования объекта защиты, согласно ГОСТ 62443: построен фрагмент референсной модели архитектуры АСУ ТП месторождения, включающий основные элементы АСУ кустовых площадок. Рассмотрено применение предложенной методики для оценки рисков ИБ обеспечения целостности телеметрической информации в промышленной сети и непрерывности технологического процесса.

При использовании технологий когнитивного моделирования в рамках предложенной методики одной из основных проблем является оценка силы связей концептов. Необходимо учитывать субъективное мнение каждого эксперта, и не сводить эти мнения к некоторой усредненной числовой оценке, а применять способы учета возникающей неопределенности за счет различных подходов к формализации знаний экспертов при построении НКК. Применение ансамбля нечетких когнитивных карт позволяет учесть неопределенность мнений экспертов в оценке риска ИБ по сравнению с оценками, получаемыми отдельными НКК. Разброс оценок состояния концептов ансамбля при этом меньше, чем разброс оценок их серых значений с помощью НСКК, в среднем в 1,5-1,7 раза, что говорит о снижении влияния фактора субъективности на результаты оценки рисков. Оценки рисков ИБ для целевых концептов после оптимизации распределения ресурсов, выделенных на контрмеры, уменьшились как в отношении разброса («серость»), так и в отношении центрального значения оценок («белизна») на 70-80. При этом не только возросла оценка эффективности использования контрмер, но и уменьшилась оценка стоимости их эксплуатации.

В процесс 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. С помощью алгоритмов кластерного анализа на основе карты самоорганизации Кохонена и иерархических алгоритмов кластеризации выявлена устойчивая структура образов, характеризующая совокупность отпечатков (fingerprints) пользовательских окружений со следами и без следов удаленного управления. Предложена гетерогенная модель ансамбля классификаторов для

обнаружения удаленного управления пользовательским сеансом при работе с банковской системой с группой признаков, состоящих из временных интервалов между событиями движения курсора компьютерной мыши. Проведен вычислительный эксперимент на натурных данных. Точность определения удаленного управления составила 93 %.

Проведен анализ угроз нарушения информационной безопасности и соответствующие им меры противодействия, по уровням архитектуры программно-определяемых сетей. Разработаны и реализованы инструменты (алгоритмическое и программное обеспечение, архитектура системы взаимодействия) защиты управляющего трафика программно-определяемых сетей. Проанализированы варианты построения ансамблей и комитетов классификаторов на основе традиционных моделей машинного обучения (модели случайного леса, рандомизированные деревья решений и пр.) и гетерогенных нейросетевых моделей (глубокие нейронные сети, сверточные нейронные сети и модели на основе автоэнкодеров с долгой-краткосрочной памятью). Оценка F1-меры при работе с тестовыми выборками достигает 96%.

С целью осуществления мониторинга и обмена данными об инцидентах ИБ в финансовой сфере разработана структурная схема системы мониторинга банковских транзакций в составе антифрод-системы, которая включает модуль интеллектуального анализа текстовых меток назначения платежа. Внедрение модуля позволяет делать выводы о принадлежности транзитной операции к одному из предложенных классов, строить динамический профиль пользователя и повысить обоснованность рекомендаций системы мониторинга. Предложен алгоритм поэтапного анализа текстовой метки назначения платежа. Отличие алгоритма заключается в использовании адаптивных словарей категорий, построении векторного представления текстовых описаний и многопроходном применении гетерогенных нейросетевых классификаторов, что позволяет повысить обоснованность принимаемого решения о принадлежности транзакции к одному из выделенных классов. С использованием композиции классификаторов достигнута точность классификации 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.

ЗАКЛЮЧЕНИЕ

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.

Список сокращений и условных обозначений

ADM	Anomaly Detection and Mitigation, системы обнаружения и устранения аномалий
APT	Advanced Persistent Threats, многошаговые скоординированные распределенные атаки
ARIMA	Auto Regressive Integrated Moving Average, модели авторегрессии
CAPEC	Common Attack Pattern Enumeration and Classification, перечень и классификатор шаблонов типовых атак
CBOW	Continuous Bag-Of-Words, модель непрерывного «мешка слов»
CPE	Common Platform Enumeration, формальный язык описания всех возможных продуктов, операционных систем и аппаратных устройств при описании уязвимостей
CVE	Common Vulnerabilities and Exposures, база данных (стандарт) в области унификации именования и регистрации обнаруженных уязвимостей ПО
CVSS	Common Vulnerability Scoring System, общепринятый стандарт для определения степени опасности уязвимостей в программном обеспечении
CWE	Common Weakness Enumeration, база данных недостатков (слабых мест) ПО, которые могут быть использованы нарушителями при проведении атак
Doc2Vec	методов вложения на уровне документов
EDR	Endpoint Threat Detection and Response, системы обнаружения и реагирования на угрозы для конечных точек
FastText	Предобученные модели векторного представления слов
FCM	Fuzzy Cognitive Maps, нечеткая когнитивная карта
IF	Isolation Forest, модели обнаружения аномалий на основе изолирующего леса
IIoT	Устройства промышленного Интернета вещей
IOA	Indicator of Attack, индикатор атак
IOC	Indicator of Compromise, индикатор компрометации
LDA	Латентное размещение Дирихле
LinearSVC	Linear Support Vector Classifier
LOF	Local Outlier Factor, модели оценки выбросов с автоподстройкой порога
LSTM	Long Short-Term Memory, нейронные сети с долгой краткосрочной памятью
MITRE ATT&CK Matrix	Формальное описание техник и тактик реализации кибератак
MLP	Multilayer perceptron, многослойный персептрон
MSE	Mean squared error, среднеквадратичная ошибка
NAE	Нейросетевой автоенкодер
NARX	Nonlinear autoregressive exogenous model, нейросетевая регрессионная модель
NB	Наивный байесовский классификатор
NTA	Network Traffic Analysis, системы анализа сетевого трафика
NVD	National Vulnerability Database, хранилище данных уязвимостей, основанное на стандартах правительства США
OSVM	One-Class Support Vector machine, метод опорных векторов с одним классом
PCA	Метод главных компонент
Random Forest	Классификатор на основе случайного леса
RNN	Recurrent Neural Network, рекуррентные нейронные сети

SIEM	Security Information and Event Management, системах управления информацией и событиями безопасности
SOAR	Security Orchestration and Automated Response, системы управления безопасностью и автоматизации реагирования
SOC	Security Operation Center, центр мониторинга и реагирования на инциденты ИБ
SVM	Метод опорных векторов
UEBA	User and Entity behavior Analytics, системы анализа безопасности поведения пользователей и сущностей
Word2Vec	методов вложения слов
XDR	Extended Detection and Response, концепция расширенного обнаружения и устранения угроз
АИС	Автоматизированная информационная система
АСУ ТП	Автоматизированная система управления технологическим процессом
БДУ	банка данных угроз безопасности информации ФСТЭК России
БИ	безопасности информации
ВР	временной ряд
ИАД	интеллектуальный анализ данных
ИБ	информационная безопасность
ИС	информационная система
ИСПДн	информационная система персональных данных
ИСППР	интеллектуальная система поддержки принятия решений
КИИ	критическая информационная инфраструктура
КФО	киберфизический объект
КФС	киберфизическая система
ЛПР	лицо, принимающее решения
МВР	многомерные временные ряды
НКК	нечеткая когнитивная карта
НКК	нечеткая когнитивная карта
НПКК	нечеткия продукционная когнитивная карта
НС	нейронная сеть
НСКК	нечеткая серая когнитивная карта
ПО	программное обеспечение
РВ	реальное время
ТВР	технологический временной ряд
ТМИ	телеметрическая информация
ТО	технологический объект
ТП	технологический процесс

Словарь терминов

Big Data – структурированные и неструктурированные данные «больших» объёмов и значительного многообразия, эффективно обрабатываемых горизонтально масштабируемыми программными инструментами;

F1 мера – гармоническое среднее между точностью и полнотой в задаче классификации;

Text Mining – методы семантического анализа текстов;

Аномалия – отклонения в функционировании КФО или отклонения, связанные с нарушением взаимодействия устройств при обмене данными в составе КФО;

Кибербезопасность – обеспечение конфиденциальности, целостности и доступности в киберпространстве (ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity);

КИИ – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки;

Меташаблон атаки – абстрактная характеристика конкретной методологии или техники, используемой в атаке;

Объект КИИ – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

Предиктивный анализ – предсказание и раннее обнаружение атак;

Проактивная защита – опережающая стратегия защиты;

Семантическая близость – мера близости, предназначенная для количественной оценки семантической (смысловой) схожести текстовых описаний;

Субъект КИИ – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети,

автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Технологический временной ряд – последовательность дискретных упорядоченных в неслучайные равноотстоящие моменты времени измерений параметра, характеризующего состояние технологического объекта.

Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей.

Риск ИБ.

ГОСТ Р ИСО/МЭК 27000-2012:

- риск информационной безопасности (п.2.24) – потенциальная возможность того, что уязвимость будет использоваться для создания угрозы активу или группе активов, приводящей к ущербу для организации;
- риск (п.2.34) – сочетание вероятности события и его последствий;
- количественная оценка риска (п.2.40) – процесс присвоения значений вероятности и последствий риска;

ГОСТ 56205/62443-1-1: Риск (п.5.6.4.1) – ожидание ущерба, выраженное вероятностью того, что определенный источник угрозы воспользуется определенной уязвимостью объекта, что приведет к отрицательным последствиям. Риск зависит от угрозы, уязвимости и последствий, где последствия – это отрицательное воздействие на организацию, которое обусловлено конкретным вредом имущественному объекту или объектам внутри организации, причиняемым конкретной угрозой или уязвимостью.

ГОСТ 62443-2-1-2015: дается уравнение риска (разд. А 2.3.3.7.2):

Риск = Вероятность наступления события * Последствия = Вероятность реализации угрозы * Вероятность используемой уязвимости * Последствия;

ГОСТ 27005: (Приложение Е. Подходы к оценке рисков информационной безопасности. Разд. Е.2.2., Таблица Е2) – мера риска определяется как произведение степени вероятности возникновения угрозы на последствия (ценность актива), где ценность актива определяется в баллах или в денежном эквиваленте;

Уязвимость – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (-ая) может быть использован (-а) для реализации угроз безопасности информации (ГОСТ Р 56546-2015).

Степень опасности уязвимости – мера (сравнительная величина), характеризующая подверженность информационной системы уязвимости и ее влияние на нарушение свойств безопасности информации (конфиденциальности, целостности, доступности).

Описание зарегистрированных и классифицированных уязвимостей (с указанием степени их опасности) хранятся в различных официальных реестрах CVE, NVD, БДУ ФСТЭК России и др.

«**Потенциальные слабости**» – это возможные уязвимости.

Методика ФСТЭК России [2] (разд. 2.3):

«Исходными данными для оценки угроз безопасности информации являются:

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstek.ru), …;

б) описание векторов (шаблоны) компьютерных атак, содержащиеся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

…

ж) результаты оценки рисков (ущерба), проведенной обладателем информации и (или) оператором.

… По результатам оценки, проведенной в соответствии с настоящей Методикой, должны быть выявлены актуальные угрозы безопасности информации, реализация (возникновение) которых может привести к нарушению безопасности информации, обрабатываемой в системах и сетях информации…»

Разд. 5.3.3 Методики: «Угроза безопасности информации возможна, если имеются нарушитель или иной источник угрозы, объект, на который осуществляется воздействие, способы реализации угрозы безопасности информации, а реализация угрозы может привести к негативным последствиям:

$УБИ_i$ = [нарушитель (источник угрозы); объекты воздействия; способы реализации угроз; негативные последствия].»

Разд. 5.3.4-5 Методики: «Сценарии реализации угроз безопасности информации должны быть определены для соответствующих способов реализации

угроз применительно к объектам воздействия и видам воздействия на них. Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техники, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

… При наличии хотя бы одного сценария реализации угрозы безопасности информации такая угроза признается актуальной для системы и сети и включается в модель угроз безопасности систем и сетей для обоснования выбора организационных и технических мер по защите информации (обеспечению безопасности), а также выбора средств защиты информации».

Вектор атаки (Attack Vector) – последовательность действий нарушителя, приводящая к получению несанкционированного доступа к защищенной информационной системе. Как правило, вектор атаки не является единственным, выбор конкретного вектора атаки зависит от мотивации и квалификации нарушителя. [20].

Мониторинг информационной безопасности – процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей (ГОСТ Р 59547-2021. Защита информации. Мониторинг информационной безопасности. Общие положения (утв. 27.07.2021))

Инцидент информационной безопасности – одно или несколько нежелательных или неожиданных событий информационной безопасности, которые со значительной степенью вероятности приводят к компрометации операций бизнеса и создают угрозы для информационно безопасности (ГОСТ 27000). Аналогичное определение инцидента ИБ дается в ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности (Переиздание: апрель 2020 г.) – М.: Стандартинформ, 2020, где определены основные этапы выявления, обработки инцидентов ИБ и совершенствование системы анализа рисков ИБ с учетом дополнительной возможности получения более качественных данных о различных типах угроз и связанных с ними уязвимостях.

Список литературы

1 Федеральный закон № 187-ФЗ «О безопасности критической ин-формационной инфраструктуры Российской Федерации» от 26.07.2017 [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 20.05.2020).

2 Методика оценки угроз безопасности информации. Методический документ ФСТЭК России от 5 февраля 2021 г. // Официальный сайт ФСТЭК России [Электронный ресурс]. – URL: https://fstec.ru/component/attachments/download/2919 (дата обращения 08.04.2021).

3 Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей среды / Приказ ФСТЭК России от 14 марта 2014 г. № 31 [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (дата обращения 20.05.2020).

4 Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации / Приказ ФСТЭК России от 25 декабря 2017 г. № 239 [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (дата обращения 20.05.2020).

5 Ажмухамедов И. М., Выборнова О. Н. Введение метрических характеристик для решения задачи оценки и управления рисками // Прикаспийский журнал: управление и высокие технологии. 2015. № 4. С. 10-22.

6 Ажмухамедов И.М. Динамическая нечеткая когнитивная модель влияния угроз на информационную безопасность системы // Безопасность информационных технологий. 2010. №2. С. 68–72.

7 Ажмухамедов И.М., Завьялова Е.Е., Кузнецова В.Ю. Методы автоматизации анализа текстовой информации на русском языке с целью выявления ее семантической направленности // Прикаспийский журнал: управление и высокие технологии. 2020. №. 2 (50). С. 118-126.

8 Ажмухамедов И.М., Зорин К.А., Кузнецова В.Ю. Структура программного продукта для семантического анализа текстовой информации // Прикаспийский журнал: управление и высокие технологии. 2021. № 1 (53). С. 9-17.

9 Ажмухамедов И.М., Кузнецова В.Ю., Станишевская А.В. Программный продукт для управления рисками при использовании цифровой образовательной среды // Прикаспийский журнал: управление и высокие технологии. 2021. № 3 (55). С. 72-81.

10 Вульфин, А. М. Алгоритмы нейросетевой обработки информации в задачах диагностирования инженерной сети нефтедобывающего

предприятия / А. М. Вульфин, А. И. Фрид // Нейрокомпьютеры: разработка, применение. – 2013. – № 3. – С. 036-039.

11 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.

12 Андреев Ю.С., Дергачев А.М., Жаров Ф.А., Садырин Д.С. Информационная безопасность автоматизированных систем управления технологическими процессами // Известия вузов. Приборостроение. 2019. Т. 62, № 4. С. 331–339.

13 Аникин И.В. Нечеткая оценка факторов риска информационной безопасности // Безопасность информационных технологий. 2016. Т. 23. № 1. С. 78-87.

14 Аникин И.В., Емалетдинова Л.Ю., Кирпичников А.П. Методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях // Вестник Казанского технологического университета. 2015. Т. 18. №. 6.

15 Арустамов С.А., Дайнеко В.Ю. Применение динамической байесовской сети в системах обнаружения вторжений // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 3 (79). С. 128-133.

16 Астахов А.М. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010. – 312 с.

17 Баринов А.И., Катасёва Д.В., Катасёв А.С. Использование модели нечетких нейронных сетей для формирования базы знаний по определению фишинговых сайтов // Вестник Технологического университета. 2020. Т. 23, № 10. С. 64-67.

18 Бенгфорт Б., Билбро Р., Океда Т. Прикладной анализ текстовых данных на Python. Машинное обучение и создание приложений обработки естественного языка / Пер. с англ. – СПб.: Питер, 2019. – 368 с.

19 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.

20 Бобов М. Н., Горячко Д. Г. Оценка рисков информационной безопасности с использованием стандарта CVSS 3.0. – 2017.

21 Бондарчук Д. В. Векторная модель представления знаний на основе семантической близости термов // Вестник ЮУрГУ. Серия «Вычислительная математика и информатика». 2017. Т. 6. № 3. С. 73-83. doi: 10.14529/cmse170305.

22 Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, ок-тябрь 2011 г.). – Уфа: Лето, 2011. – С. 8-13.

23 Булдакова Т.И., Миков Д.А. Методика анализа информационных рисков с применением нейро-нечеткой сети // НТИ. Сер. 2. Информационные процессы и системы. 2015. № 4. С. 13-17.
24 Булдакова Т.И., Миков Д.А. Реализация методики оценки рисков информационной безопасности в среде MATLAB // Вопросы кибербезопасности. 2015. № 4 (12).
25 Васильев В. И. и др. Система обнаружения атак в беспроводных сенсорных сетях промышленного Интернета вещей / В. И. Васильев, А. М. Вульфин, В. М. Картак [и др.] // Труды Института системного анализа Российской академии наук. – 2019. – Т. 69. – № 4. – С. 70-78. – DOI 10.14357/20790279190409.
26 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.
27 Васильев В. И., Вульфин А. М., Герасимова И. Б., Картак В. М. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт // Вопросы кибербезопасности. 2020. № 2(36). С. 11-21. doi:10.21681/2311-3456-2020-2-11-21.
28 Васильев В. И., Вульфин А. М., Гузаиров М. Б., Картак В. М., Черняховская Л. Р. Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт // Информационные технологии. 2020. Т. 26 № 4. С. 213–221. doi: 10.17587/it.26.213-221.
29 Васильев В. И., Вульфин А. М., Кучкарова Н. В. Автоматизация анализа уязвимостей программного обеспечения на основе технологии Text Mining //Вопросы кибербезопасности. – 2020. – №. 4 (38).
30 Васильев В. И., Вульфин А.М., Берхольц В. В., Кириллова А.Д., Бельский С.М. Анализ рисков обеспечения целостности телеметрической информации с использованием технологии когнитивного http://journal.ugatu.ac.ru/index.php/Vestnik/article/view/2216 (дата обращения: 15.03.2020).
31 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. DOI: 10.21681/2311-3456-2021-2-2-16
32 Васильев В.И. Интеллектуальные системы защиты информации: учеб. пособие для вузов. – 3-е изд. – М.: Инновационное машиностроение, 2017. – 201 с.
33 Васильев В.И., Вульфин А.М., Гузаиров М.Б. Оценка рисков информационной безопасности с использованием нечетких продукционных когнитивных карт // Информационные технологии. 2018. Т.24, № 4. С. 266–273.

34 Васильев В.И., Вульфин А.М., Гузаиров М.Б., Кириллова А.Д. Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт // Информационные технологии. 2018. Т. 24. № 10. С. 657-664.
35 Васильев В.И., Вульфин А.М., Кудрявцева Р.Т. Анализ и управление рисками информационной безопасности с использованием технологий когнитивного моделирования // Доклады ТУСУР, Томск. 2017. Т. 20. № 4. С. 61-66.
36 Васильев В.И., Вульфин А.М., Черняховская Л.Р. Анализ рисков инновационных проектов с использованием технологии многослойных нечетких когнитивных карт // Программная инженерия. 2020. № 3 (11). С. 142-151.
37 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.
38 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.
39 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.
40 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.
41 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.
42 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.
43 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.
44 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.

45 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.
46 Воробьева Ю.Н., Катасёва Д.В., Катасёв А.С. Кирпичников А.П. Нейросетевая модель выявления DDoS-атак // Вестник технологического университета. 2018. Т. 21, № 2. С. 94-98.
47 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.
48 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
49 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
50 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
51 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
52 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.
53 Глушенко С.А., Долженко А.И. Система поддержки принятия реше-ний нечеткого моделирования рисков информационной безопасности организации // Информационные технологии. 2015. Т. 21. № 1. С. 68-74.
54 Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А. Синтез модели машинного обучения для обнаружения компьютерных атак на основе набора данных CICIDS2017 // Труды ИСП РАН. 2020. Т. 32. № 5. С. 81–93.
55 Грачков И.А. Информационная безопасность АСУ ТП: возможные вектора атаки и методы защиты // Безопасность информационных технологий. 2018. Т. 25. № 1. С. 90-98. DOI:10.26583/bit.2018.1.09.
56 Гузаиров М. Б., Машкина И. В., Степанова Е. С. Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой

политики безопасности //Безопасность информационных технологий. – 2011. – Т. 18. – №. 2. – С. 37-49.

57 Гузаиров М.Б. Системный анализ информационных рисков с применением нечетких когнитивных карт / М.Б. Гузаиров, В.И. Васильев, Р.Т. Кудрявцева // Инфокоммуникационные технологии. – 2007. – Т. 5, – № 4, – С. 42–48.

58 Гузаиров М.Б., Васильев В.И., Кудрявцева Р.Т. Системный анализ информационных рисков с применением нечетких когнитивных карт // Инфокоммуникационные технологии. 2007. Т.5, № 4. С. 42–48.

59 Гуревич, О.С., Гольберг, Ф.Д., Селиванов О.Д. Интегрированное управление силовой установкой многорежимного самолета / Под общ. ред. О.С.Гуревича. – М. Машиностроение, 1993. – 304 с.

60 Дагаева М.В., Катасёва Д.В., Катасёв А.С. Обнаружение подмены пользователей в компьютерных системах на основе искусственной нейронной сети // Информация и безопасность. 2018. Т. 21, № 3. С. 296-301.

61 Дагаева М.В., Катасёва Д.В., Катасёв А.С., Кирпичников А.П. Нейросетевая модель динамической биометрии для обнаружения подмены пользователей в компьютерных системах // Вестник технологического университета. 2018. Т. 21, № 2. С. 115-119.

62 Диссертация «Модель прогнозирования временных рядов по выборке максимального подобия». Глава 1. Постановка задачи и обзор моделей прогнозирования временных рядов [Электронный ресурс]. URL: http://www.mbureau.ru/articles/dissertaciya-model-prognozirovaniya-vremennyh-ryadov-glava-1

63 Дойникова Е. В., Чечулин А. А., Котенко И. В. Оценка защищенности компьютерных сетей на основе метрик CVSS //Информационно-управляющие системы. – 2017. – №. 6 (91).

64 Дойникова Е.В., Котенко И.В. Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер // Информационная безопасность. 2018. № 2 (57). С. 211-240.

65 Захаров А.А. и др. Анализ информационной безопасности автоматизированных систем управления техническими процессами газодобывающего предприятия // Вестник УрФО. Безопасность в информационной сфере. 2017. № 3 (25). С. 24-33.

66 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.

67 Зегжда Д. П. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. – М.: Горячая Линия-Телеком, 2020. – 560 с.

68 Вульфин, А. М. Интеллектуальная автоматизированная система поддержки принятия решений для технологического комплекса приема-

сдачи нефти / А. М. Вульфин, А. И. Фрид // Мехатроника, автоматизация, управление. – 2011. – № 5. – С. 29-34.

69 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.

70 Исхаков С. Ю., Исхаков А. Ю., Шелупанов А. А. Алгоритм применения краткосрочного прогнозирования для выявления инцидентов информационной безопасности посредством анализа сетевого трафика //Доклады Томского государственного университета систем управления и радиоэлектроники. – 2018. – Т. 21. – №. 4. – С. 44-50.

71 Кириллова А.Д., Васильев В.И. Применение нечеткой нейронной сети для оценки рисков информационной безопасности АСУ ТП // Проблемы информационной безопасности / Материалы VII Всеросс. Заочной Интернет-конференции, 20-21 февр. 2018 г. Ростов-на-Дону: Изд-во ООО «Азов Принт», 2018. С. 138-142.

72 Козачек А.В. Математическая модель системы распознавания разрушающих программных средств на основе скрытых марковских моделей // Вестник СибГУТИ. 2012. № 3. С. 29-39.

73 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.

74 Котенко И. В., Дойникова Е. В., Чечулин А. А. Общее перечисление и классификация шаблонов атак (CAPEC): описание и примеры применения // Защита информации. INSIDE. 2012. № 4(46). С. 54-66.

75 Котенко И.В. и др. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2012. Т. 1. № 20. С. 27-56.

76 Кулинич А.А. Компьютерные системы анализа ситуаций и поддержки принятия решений на основе когнитивных карт: подходы и методы // Проблемы управления. 2011. № 4. С. 31-45.

77 Кулинич А.А. Компьютерные системы моделирования когнитивных карт: подходы и методы // Проблемы управления. М.: Изд-во ИПУ РАН им. В.А. Трапезникова. 2010. Вып. 3. С. 2–16.

78 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.

79 Лаврентьев А.М. и др. Сравнительный анализ специальных корусов текстов для задач безопасности // Вопросы кибербезопасности. 2020. № 3(37). С. 54–60.
80 Леденева Т.М., Моисеев С.А. Формализация свойств интерпретируемых лингвистических шкал и термов нечетких моделей // Прикладная информатика. 2012. № 4(40). С. 126-132.
81 Макаревич О.Б. Основные направления научных разработок кафедры бит ТТИ ЮФУ и их внедрение в НИОКР и учебный процесс // Известия ЮФУ. Технические науки. 2008. №8. URL: https://cyberleninka.ru/article/n/osnovnye-napravleniya-nauchnyh-razrabotok-kafedry-bit-tti-yufu-i-ih-vnedrenie-v-niokr-i-uchebnyy-protsess
82 Машкина И. В. и др. Использование методов системного анализа для решения проблемы обеспечения безопасности современных информационных систем //Известия Южного федерального университета. Технические науки. – 2011. – Т. 125. – №. 12. – С. 25-35.
83 Машкина И. В. Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий //Уфа: Изд-во ГОУ ВПО Уфимский государственный авиационный технический университет. – 2009.
84 Мельников П.В., Ешенко Р.А. Проблемы формирования модели угроз информационной безопасности в информационных системах // Вестник науки. 2020. № 1 (6). С. 185-189.
85 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.
86 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.
87 Милославская Н. Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. – М.: Горячая Линия-Телеком, 2021. – 432 с.
88 Вульфин, А. М. Нейросетевая модель анализа технологических временных рядов в рамках методологии Data Mining / А. М. Вульфин, А. И. Фрид // Информационно-управляющие системы. – 2011. – № 5(54). – С. 31-38.
89 Вульфин А. М., Гиниятуллин В. М., Фрид А. И. Нейросетевая модель выявления и распознавания технологических ситуаций в рамках методологии Data Mining //Optical Memory and Neural Networks (Information Optics). – 2010. – Т. 19. – №. 3. – С. 207-212.

90 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.

91 О проблеме выявления экстремистской направленности в текстах// Вестник Новосибирского государственного университета / Ананьева М.И., Кобозева М.В., Соловьев Ф.Н., Поляков И.В., Чеповский А.М.// Серия: Информационные технологии. 2016.Т.14.С.5-13.

92 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.

93 Обеспечение функциональной безопасности аппаратно-программных комплексов в условиях неопределенности среды использования / В. Е. Гвоздев, М. Б. Гузаиров, О. Я. Бежаева [и др.] // Моделирование, оптимизация и информационные технологии. – 2020. – Т. 8. – № 3(30). – С. 36-37. – DOI 10.26102/2310-6018/2020.30.3.005.

94 Основы теории нечётких и гибридных систем / Ярушкина Н.Г. // Учебное пособие, М.: Финансы и статистика, 2004. – С. 15-58.

95 Остапенко А.Г. и др. Предупреждение и минимизация последствий компьютерных атак на элементы критической информационной инфраструктуры и автоматизированные информационные системы критически важных объектов: риск-анализ и оценка эффективности защиты // Информация и безопасность. 2013. Т.16. № 2. С. 167-178.

96 Остапенко Г.А., Шершень А.Н., Калашников А.О. Концептуальный подход к расчету и регулированию рисков нарушения актуальности информации в элементах критической информационной инфраструктуры // Информация и безопасность. 2013. Т. 16. № 2. С. 239-242.

97 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.

98 Перминов Г.И., Леонова Н.В. Применение нечеткой логики для решения когнитивной карты при использовании комбинации альтернатив // Аудит и финансовый анализ, №4, 2014. С. 396-401.

99 Петренко С. А., Петренко А. С. Моделирование систем обработки больших данных кибербезопасности //Информационные системы и технологии в моделировании и управлении. 2016. С. 279-284

100 Подвесовский А.Г., Исаев Р.А. Идентификация структуры и параметров нечетких когнитивных моделей: экспертные и статистические методы // Intern. Journal of Open Information Technologies. 2019. Vol. 7, № 6. С. 35-61.

101 Применение методов автоматизации при определении актуальных угроз безопасности информации в информационных система с применением банка данных угроз ФСТЭК России / Селифанов В. В., Звягинцева П.А., Юракова Я.В., Слонкина И.С. //Интерэкспо Гео-Сибирь. 2017. Т. 8. С.202-209.

102 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.

103 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.

104 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

105 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.

106 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.

107 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.

108 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.

109 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.

110 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.

111 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.

112 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.

113 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.

114 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.

115 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.

116 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.

117 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.

118 Рахманкулова Э.М., Катасёва Д.В., Катасёв А.С., Кирпичников А.П., Хабибуллин Р.С., Хабибуллина Ю.С. Анализ и прогнозирование временных рядов на базе аналитической платформы DEDUCTOR // Вестник Технологического университета. 2018. Т. 21, № 12. С. 154-158.
119 Робертс Ф.С. Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам / Под ред. А.И. Теймана. – М.: Наука, Гл. ред. физ.-мат. лит. – 1986. – 496 с.
120 Сабиров Р.А., Увайсов С.У. Применение средств обеспечения информационной безопасности в промышленных системах управления // Север России: стратегии и перспективы развития: Материалы III Всероссийской научно-практической конференции, г. Сургут, 2017, с. 140-143.
121 Селифанов В.В., Юракова Я.В., Карманов И.Н. Методика автоматизированного выявления взаимосвязей уязвимостей и угроз безопасности информации в информационных системах // Интерэкспо Гео-Сибирь, 2018. Т.9. С.271-276.
122 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.
123 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.
124 Соловьев С. В., Мамута В. В. Применение аппарата нейросетевых технологий для определения актуальных угроз безопасности информации информационных систем //Наукоемкие технологии в космических исследованиях Земли. – 2016. – Т. 8. – №. 5.
125 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.
126 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.
127 Сравнительный анализ специальных корусов текстов для задач безопасности / Лаврентьев А.М., Рябова Д.М., Тихомирова Е.А., Фокина А.И., Чеповский А.М., Шерстинова Т.Ю. // Вопросы кибербезопасности. 2020. №3(37). С.54-60.
128 Степанова Е.С., Машкина И.В., Васильев В.И. Разработка модели угроз на основе построения нечеткой когнитивной карты для численной оценки риска информационной безопасности // Известия ЮФУ, Технические науки / Тематич. выпуск «Информационная безопасность», г. Таганрог: Изд-во ТТИ ЮФУ. №11(112), 2010. С.31-40.
129 Степанова У.С. Разработка модели угроз на основе построения нечеткой когнитивной карты для численной оценки риска нарушения

информационной безопасности / У.С. Степанова, И.В. Машкина, В.И. Васильев// Известия ЮФУ. Технические науки. – Тематич. Выпуск «Информационная безопасность». – Таганрог: ТТИ ЮФУ. – 2010. – № 11 (112), – С. 31–40.

130 Теляшев Э.Г., Арпишкин И.М., Определение характеристической вязкости полиэтилентерефталата по контролируемым параметрам насоса ISSN2071-5951 научный журнал Мир нефтепродуктов вестник нефтяных компаний 2018г.

133 Федорченко А.В., Чечулин А.А., Котенко И.В. Исследование открытых баз уязвимостей и оценка возможностей их применения в системах анализа защищенности компьютерных сетей // Информационно-управляющие системы. 2014. №5. С.72-79.

134 Федулов А.С. Нечеткие реляционные когнитивные карты // Изв. РАН. Теория и системы управления. 2005. № 1. С. 120-132.

135 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.

136 Хачатуров В.Р. и др. Системы планирования и проектирования для нефтегазобывающих регионов и месторождений: математические модели, методы, применение // Исследовано в России. 2012. № 15. С. 158.

137 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.

138 Шадькова Д.К., Коркишко А.Н. Стоимостной инжиниринг как основа управления проектом обустройства месторождения на примере компании ПАО «ГАЗПРОМ НЕФТЬ» // Фундаментальные исследования. 2017. Т. 4. № 12. С. 930-934.

139 Шелупанов А.А. Модель угроз информационной безопасности программного обеспечения компьютерных сетей на основе атрибутивных метаграфов: монография / А.К. Новохрестов, А.А. Конев, А.А. Шелупанов, Е.М. Давыдова. – Томск: В-Спектр. 2018. – 114 С.

140 Шелухин О. И. Сетевые аномалии. Обнаружение, локализация, прогнозирование. – М.: Горячая Линия-Телеком, 2020. – 448 с.

141 Abdelwahab O., Elmaghraby A. UofL at SemEval-2016 Task 4: Multi domain word2vec for Twitter sentiment classification //Proceedings of the 10th international workshop on semantic evaluation (SemEval-2016). – 2016. – С. 164-170.

142 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.

143 Ali A., Alfaycz F., Alquhayz H. Semantic Similarity Measures Between Words: A Brief Survey // Sci.Int. (Lahore), №30 (6). 2018. pp. 907-914.
144 Almomani I., Al-Kasasbeh B., Al-Akhras M. WSN-DS: A dataset for intrusion detection systems in wireless sensor networks // Journal of Sensors. 2016. Vol. 2016.
145 Alrashdi I., Alqazzaz A., Aloufi E., Alharthi R., Zohdy M., Ming H. Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning // 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). IEEE. 2019. P. 305-310.
146 Al-Shaer R., Ahmed M., Al-Shaer E. Statistical Learning of APT TTP Chains from MITRE ATT&CK. In Proc. RSA Conf. 2018. C. 1-2.
147 Alshamrani A. et al. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities // IEEE Communications Surveys & Tutorials. 2019. № 2 (21). C. 1851-1877.
148 Amancei C. Practical methods for information security risk management // Informatica Economica. 2011. T. 15. № 1. C. 151.
149 Amshinov N.M., Likhter A.M., Azhmukhamedov I.M. Methodology for improving the decision support system in order to reduce the probability of environmental accidents at gas production industry // Journal of Physics: Conference Series. IOP Publishing, 2021. Vol. 2091, no. 1. P. 012055.
150 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.
151 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
152 Anwar A. et al. Cleaning the NVD: Comprehensive Quality Assessment, Improvements, and Analyses //arXiv preprint arXiv:2006.15074. – 2020.
153 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.
154 Behnia A., Rashid R. A., Chaudhry J. A. A survey of information security risk analysis methods // SmartCR. 2012. T. 2. № 1. C. 79-94.
155 Benjamin V. et al. Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops //2015 IEEE international conference on intelligence and security informatics (ISI). – IEEE. 2015. C. 85-90.
156 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.

157 Bian X. Detecting Anomalies in Time-Series Data using Unsupervised Learning and Analysis on Infrequent Signatures // Journal of IKEEE. 2020. Vol. 24. № 4. P. 1011-1016.
158 Boutalis Y. Adaptive estimation of fuzzy cognitive maps with proven stability and parameter convergence / Y. Boutalis, Th.L. Kottas, M. Chrstodoulou // Journal IEEE Trans. On Fuzzy Systems. – 2009. – Vol. 17 – Issue 4, – P. 874–889.
159 Boutalis Y. On the existence and uniqueness of solutions for the concept values in fuzzy cognitive maps / Y. Boutalis, T. Kottas, M. Christodoulou // Decision and Control, 2008. CDC 2008. 47th IEEE Conference on. – Cancun: IEEE, – 2008. – P. 98–104.
160 Brazhuk A. Semantic model of attacks and vulnerabilities based on CAPEC and CWE dictionaries // International Journal of Open Information Technologies. 2019. № 3 (7). С. 38-41.
161 Bullock J., Parker J.T. Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework // John Wiley & Sons, 2017.
162 Carvalho J.P. Issues in the Stability of Fuzzy Cognitive Maps and Rule – Based Fuzzy Cognitive Maps / J.P. Carvalho, Y.A.B. Tome. – [Электронный ресурс]. – Режим доступа: URL: www.inesc-id.pt/indicators/Ficherois/119.pdf., свободный (дата обращения: 01.09.2017).
163 Carvalho J.P., Tome J.A.B. Rule Based Fuzzy Cognitive Maps: Fuzzy Causal Relations // Computational Intelligence for Modeling, Control and Automation: Evolutionary Computation & Fuzzy Logic for Intelligent Control, Knowledge Acquisition & Information Retrieval / Mohammadian (Ed.). – URL: www.inesc-id.pt/pt/indicadores/Ficheiros/1894.pdf (дата доступа: 24.09.2017).
164 Catterson V. M., Rudd S. E., McArthur S. D., Moss G. On-line transformer condition monitoring through diagnostics and anomaly detection // 2009 15th International Conference on Intelligent System Applications to Power Systems. IEEE. 2009. P. 1-6.
165 Cecil A. A Summary of Network Traffic Monitoring and Analysis Techniques [Электронный ресурс]. URL: https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html (дата обращения: 05.12.2021)
166 Chen H. et al. VEST: A System for Vulnerability Exploit Scoring & Timing // IJCAI, 2019. P. 6503–6505.
167 Chen S., Janeja V. P. Human perspective to anomaly detection for cybersecurity // Journal of Intelligent Information Systems. 2014. Vol. 42. № 1. P. 133-153.
168 Choi S. HAI Security Dataset. HIL-based Augmented ICS (HAI) Security Dataset // Kaggle. ICS Security Dataset [Электронный ресурс]. – URL: https://www.kaggle.com/icsdataset/hai-security-dataset (дата обращения 24.08.2021).

169 Choi S., Yun J. H., Kim S. K. A comparison of ICS datasets for security research based on attack paths // International Conference on Critical Information Infrastructures Security. Springer, Cham. 2018. P. 154-166.
170 Claroty Biannual ICS Risk & Vulnerability Report: 2H 2020. [Электронный ресурс] URL: https://security.claroty.com/biannual-ics-risk-vulnerability-report-2H-2020 (дата обращения: 10.04.2021)
171 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.
172 Cruz T., Rosa L., Proença J., Maglaras L., Aubigny M., Lev L., Simoes P. A cybersecurity detection framework for supervisory control and data acquisition systems // IEEE Transactions on Industrial Informatics. 2016. Vol. 12. № 6. P. 2236-2246.
173 Das T. K., Adepu S., Zhou J. Anomaly detection in industrial control systems using logical analysis of data // Computers & Security. 2020. Vol. 96. P. 101935.
174 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.
175 Datta P., Lodinger N., Namin S., Jones S. Cyber-Attack Consequence Prediction // Proceedings of the 3rd Workshop on Big Data Engineering and Analytics in Cyber-Physical Systems. 9 p. [Электронный ресурс]. – URL: arXiv preprint arXiv:2012.00648 (дата обращения 08.04.2021).
176 de Boer M. H. T. et al. Text Mining in Cybersecurity: Exploring Threats and Opportunities //Multimodal Technologies and Interaction. 2019. Т. 3. №. 3. pp. 62.
177 De Boom C. et al. Learning semantic similarity for very short texts //2015 ieee international conference on data mining workshop (icdmw). – IEEE, 2015. – С. 1229-1234.
178 Deng J.L. Introduction to grey systems theory // Journal on Grey Systems, 1989, No.1. – P. 1-24.
179 Detection and Remediation Method for Softwere Security / Jessoo Jurn, Taeeun Kim, Hwankuk Kim, An Automated Vulnerability // Sustainability, May 2018. №10. 1657; doi: 10?3390/ su10051652012.
180 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.
181 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

182 Doshi-Velez F., Kim B. Towards a Rigorous Science of Interpretable Machine Learning. [Электронный ресурс]. URL: https://www.arXiv:17.02.08608v2[stat.ML]2Mar.2017 – (дата обращения: 10.10.2019)

183 Doynikova E., Kotenko I. CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection. In 2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP). IEEE, 2017, pp. 346-353.

184 Doynikova E.V., Fedorchenko A.V., Kotenko I.V. Detection of Weaknesses in Information Systems for Automatic Selection of Security Actions // Automatic Control and Computer Sciences. 2019. № 8 (53). С. 1029-1037.

185 Egoshin N.S., Konev A.A., Shelupanov A.A. A Model of Threats to the Confidentiality of Information Processed in Cyberspace Based on the Information Flows Model //Symmetry. – 2020. – Т. 12. – №. 11. – С. 1-18.

186 El Hariri M. et al. A targeted attack for enhancing resiliency of intelligent intrusion detection modules in energy cyber physical systems. In 19th International Conference on Intelligent System Application to Power Systems (ISAP). IEEE, 2017, pp. 1-6.

187 Elbaz C., Rilling L., Morin C. Fighting N-day vulnerabilities with automated CVSS vector prediction at disclosure //Proceedings of the 15th International Conference on Availability, Reliability and Security. – 2020. – С. 1-10.

188 Epishkina A., Zapechnikov S. A syllabus on data mining and machine learning with applications to cybersecurity //2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC). IEEE/ 2016. pp. 194-199.

189 Espinosa M.L., Depaire B., Vanhoof K. Fuzzy Cognitive Maps with Rough Concepts // Proc. of the 9th Intern. Conf. on Artificial Intelligence Applications and Innovations (AIAI'2013), Paphos, Greece, Sept. 30 – Oct. 2, 2013. P. 527-536.

190 Fang Y. et al. FastEmbed: Predicting vulnerability exploitation possibility based on ensemble ma-chine learning algorithm //Plos one. – 2020. – Т. 15. – №. 2. – С. e0228439.

191 Fedotova A, Romanov A, Kurtukova A, Shelupanov A. Authorship Attribution of Social Media and Literary Russian-Language Texts Using Machine Learning Methods and Feature Selection //Future Internet. – 2022. – Т. 14. – №. 1. – С. 4.

192 Feutrill A. et al. The effect of common vulnerability scoring system metrics on vulnerability exploit delay //2018 Sixth International Symposium on Computing and Networking (CANDAR). – IEEE, 2018. – С. 1-10.

193 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.

194 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

195 Glykas M. (ed.). Fuzzy Cognitive Maps: Advances in theory, methodologies, tools and applications. // Springer Science & Business Media. – 2010. – Т. 247. – [Электронный ресурс]. – Режим доступа: http://www.springer.com/us/book/9783642032196, свободный (дата обращения: 01.09.2017).

196 Goh J., Adepu S., Tan M., Lee Z. S. Anomaly detection in cyber physical systems using recurrent neural networks // 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE). IEEE. 2017. P. 140-145.

197 Gómez Á. L. P., Maimó L. F., Celdran A. H., Clemente F. J. G., Sarmiento C. C., Masa C. J. D. C., Nistal R. M. On the generation of anomaly detection datasets in industrial control systems // IEEE Access. 2019. Vol. 7. P. 177460-177473.

198 Gostyunin Yu.A., Stanishevskaya Yu.A., Azhmukhamedov I.M. Formalization of the information on the condition of the electric power system in risk-based maintenance strategy // Прикаспийский журнал: управление и высокие технологии. 2019. № 1 (45). С. 211-217.

199 Gurin M.A. et al. Intrusion detection system on the basis of data mining algorithms in the industrial network // CEUR Workshop Proceedings. 2019. P. 553–565.

200 Hajeck P., Prochazka O. Interval-Valued Fuzzy Cognitive Maps for Supporting Business Decisions // Proc. of the IEEE Intern. Conf. on Fuzzy Systems, Vancouver, BC, Canada, July 2016. P. 531-536.

201 Hajek P., Froelich W., Prochazka O. Intuitionistic Fuzzy Grey Cognitive Maps for Forecasting Interval-Valued Time Series // Neurocomputing. 2020.

202 Han Z., Li X., Xing Z., LiuH., Feng Z. Learning to Predict Severity of Software Vulnerability Description // Proceedings of the 2017 International Conference on Software Maintenance and Evolution (ICSME), Shanghai, China, Nov.2017. P. 125–136.

203 Hariharan A., Gupta A., Pal T. Camlpad: Cybersecurity autonomous machine learning platform for anomaly detection // Future of Information and Communication Conference. Springer, Cham. 2020. P. 705-720.

204 Harmati I.A., Koczy L.T. On the Convergence of Fuzzy Grey Cognitive Maps // Information Technology, Systems Research, and Computational Physics. Springer Verlag. 2018. С. 74-84.

205 Hemberg E. et al. BRON--Linking Attack Tactics, Techniques, and Patterns with Defensive Weaknesses, Vulnerabilities and Affected Platform

Configurations. [Электронный ресурс]. – URL: arXiv:2010.00533 (дата обращения 08.04.2021).

206 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

207 Hwang W. S. et al. Time-series aware precision and recall for anomaly detection: considering variety of detection result and addressing ambiguous labeling // Proceedings of the 28th ACM International Conference on Information and Knowledge Management. 2019. P. 2241-2244.

208 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

209 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

210 Ismagilov I.I., Molotov L.A., Anikin I.V., Katasev A.S., Kataseva D.V. Insiders Detection in Computer Systems Based on Data Mining Technique // Helix. 2018. Vol. 8, no. 6. P. 4668-4673.

211 Jamshidi A. Risk-based maintenance of critical and complex systems. 2017.

212 Jones K. S. A statistical interpretation of term specificity and its application in retrieval //Journal of documentation. – 2004.

213 Kandasami W.B.V., Vasuki R., Thuliskkanam K. New Merged Fuzzy Cognitive Maps // Ultra Scientist. 2014. Vol. 26(3)B. P. 187-192.

214 Karimipour H., Geris S., Dehghantanha A., Leung H. Intelligent anomaly detection for large-scale smart grids // 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE). IEEE. 2019. P. 1-4.

215 Katasev A.S., Emaletdinova L.Yu., Kataseva D.V. Neural network spam filtering technology // Proceeding of 2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). IEEE, 2018. P. 1-5.

216 Keshk M., Sitnikova E., Moustafa N., Hu J., Khalil I. An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems // IEEE Transactions on Sustainable Computing. 2019. Vol. 6. № 1. P. 66-79.

217 Khan M.S., Siddiqui S., Ferens K. A cognitive and concurrent cyber kill chain model // Computer and Network Security Essentials. Springer, Cham. 2018. C. 585-602.

218 Khazaei A., Ghasemzadeh M., Derhami V. An automatic method for CVSS score prediction using vulnerabilities description //Journal of Intelligent & Fuzzy Systems. – 2016. – Т. 30. – №. 1. – С. 89-96.
219 Kiss I., Genge B., Haller P., Sebestyén G. Data clustering-based anomaly detection in industrial control systems // 2014 IEEE 10th International Conference on Intelligent Computer Communication and Processing (ICCP). IEEE. 2014. P. 275-281.
220 Knight CR.J.K. Linear and Sigmoidal Fuzzy Cognitive Maps: An Analysis of Fixed Points / CR.J.K. Knight, D.J.B. Lloyd, A.S. Penn – [Электронный ресурс]. – Режим доступа: https://pdfs.semantiescholar.org/, свободный (дата обращения: 01.09.2017).
221 Koltays A., Konev A., Shelupanov A. Mathematical Model for Choosing Counterparty When Assessing Information Security Risks //Risks. – 2021. – Т. 9. – №. 7. – С. 133.
222 Koryshev N., Hodashinsky I., Shelupanov A. Building a fuzzy classifier based on whale optimization algorithm to detect network intrusions //Symmetry. – 2021. – Т. 13. – №. 7. – С. 1211.
223 Kosko B. Bidirectional associative memories // IEEE Transactions on Systems, man, and Cybernetics. – 1988. – Т. 18. – №. 1. – С. 49-60.
224 Kosko B. Fussy Cognitive Maps // International Journal of Man-Machine Studies. – 1986. – Vol. 1, – P. 65–75.
225 Kotenko I., Doynikova E. The CAPEC based generator of attack scenarios for network security evaluation. In 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). IEEE, 2015, № 1, pp. 436-441.
226 Kotsiantis S. B. et al. Supervised machine learning: A review of classification techniques //Emerging artificial intelligence applications in computer engineering. 2007. Vol. 160. №. 1. 3-24 pp.
227 Kozachok, A.V., Kopylov, S.A., Shelupanov, A.A., Evsutin O.O. Text marking approach for data leakage prevention //Journal of Computer Virology and Hacking Techniques. – 2019. – Т. 15. – №. 3. – С. 219-232.
228 Lau J. H., Baldwin T. An empirical evaluation of doc2vec with practical insights into document embedding generation //arXiv preprint arXiv:1607.05368. – 2016.
229 Lavin E.A., Giabbanelli P.J. Analyzing and Simplifying Model Uncertainty in Fuzzy Cognitive Maps // Proc. of 2017 Winter Simulation Conference. 2017. P. 1868-1879.
230 Lavrova D. S. An approach to developing the SIEM system for the Internet of Things // Automatic control and computer sciences. 2016. Vol. 50. № 8. P. 673-681.
231 Learning to Predict Severity of Software Vulnerability Description / Han Z., Li X., Xing Z., Liu H., Feng Z. // Proceedings of the 2017 International Conference on Software Maintenance and Evolution (ICSME), Shanghai, China, Nov. 2017. pp. 125-136.

232 Lee Y., Shin S. Toward Semantic Assessment of Vulnerability Severity: A Text Mining Approach // Proceedings of ACM CIKM Workshop (EYRE' 18), 2018. [Электронный ресурс]. URL: https://www.CEUR-WS.org/Vol1-2482/papers.pdf (дата обращения 01.08.2020).
233 Legoy V. S. M. Retrieving ATT&CK tactics and techniques in cyber threat rports : дис. – University of Twente, 2019.
234 Liu L., Liu D., Zhang Y., Peng Y. Effective sensor selection and data anomaly detection for condition monitoring of aircraft engines // Sensors. 2016. Vol. 16. № 5. P. 623.
235 Marchenko A.S. Investigating Stability Analysis Issues for Fuzzy Cognitive Maps / A.S. Marchenko, I.L. Ermolov, P.P. Groumpos, Ju.V. Poduraev, Ch.D. Stylios. – [Электронный ресурс]. – Режим доступа: URL: kcc.teiep.gr/stylios/pdf/, свободный (дата обращения: 01.09.2017).
236 Mazarakis S., Matsavinos G., Groumpos P. Simulating and Forecasting Qualitative Macroeconomic Models Using Rule-Based Fuzzy Cognitive Maps // Intern. Journal on Social, Behavioral, Economic, Business and Industrial Engineering, Vol. 7, No. 1, 2013. P. 147-152.
237 McInnes L., Healy J., Melville J. Umap: Uniform manifold approximation and projection for dimension reduction //arXiv preprint arXiv:1802.03426. – 2018.
238 Meel P., Goswami A. Inverse document frequency-weighted Word2Vec model to recommend apparels //2019 6th International Conference on Signal Processing and Integrated Networks (SPIN). – IEEE, 2019. – С. 1-7.
239 Mell P., Harang R. Minimizing Attack Graph Data Structures. In the Tenth International Conference on Software Engineering Advances (Barcelona, Spain), 2015, pp. 376-385.
240 Mendsaikhan O. et al. Identification of cybersecurity specific content using the Doc2Vec language model // 2019 IEEE 43rd annual computer software and applications conference (COMPSAC). IEEE, 2019. Vol. 1. P. 396-401.
241 Miao Y., Liu Z.-Q., Siew Ch.Y. Dynamical Cognitive Network – an Extension of Fuzzy Cognitive Map // IEEE Trans. on Fuzzy Systems. Oct. 2001. Vol. 9, Issue 5. pp. 760-770.
242 Miao Y., Liu Z.-Q., Tao X.H., Shen Z., Li Ch.W. Simplification, Merging and Division of Fuzzy Cognitive Maps // Intern. Journal of Computational Intelligence and Applications. 2002. Vol. 2, № 2. P. 185-208.
243 Miciolino E.E. et al. Communications network analysis in a SCADA system testbed under cyber-attacks // 2015 23rd Telecommunications Forum Telfor (TELFOR). IEEE, 2015. pp. 341–344.
244 Mikolov T., Chen K., Corrado G. Dean J. Efficient Estimation of Word Representation in Vector Space // Proceedings of Workshop at ICLR, 2013. [Электронный ресурс]. URL: https://www.arXiv.1301.3781 (дата обращения 01.08.2020).
245 Mittal S. et al. Cybertwitter: Using twitter to generate alerts for cybersecurity threats and vulnerabilities //2016 IEEE/ACM International Conference on

Advances in Social Networks Analysis and Mining (ASONAM), IEEE. 2016. pp. 860-867.

246 Mohagheghi S. Fuzzy Cognitive Maps for Identifying Fault Activation Patterns in Automation Systems. URL: https://www.intechopen.com/books/ (дата обращения 17.08.2019).

247 Mohr S. Modelling Approaches for Multilayer Fuzzy Cognitive Maps. [Электронный ресурс]. URL: https://www.researchgate.net/publication/332158518 _Modelling_Approaches_for_Multilayer_Fuzzy_Cognitive_Maps (дата обращения 27.08.2019).

248 Mokhtari S. et al. A machine learning approach for anomaly detection in industrial control systems based on measurement data // Electronics. 2021. Vol. 10. № 4. P. 407.

249 Monshizadeh M., Khatri V., Atli B. G., Kantola R., Yan Z. Performance evaluation of a combined anomaly detection platform // IEEE Access. 2019. Vol. 7. P. 100964-100978.

250 Moore B. Gartner's top 10 IoT tech trends [Электронный ресурс] // IT Brief. URL: https://itbrief.com.au/story/gartner-s-top-10-iot-tech-trends (дата обращения: 05.12.2021)

251 Motlagh O., Papageorgiou E.I., Tang S.H., Jamaludin Z. Multivariate Relationship Modeling Using Nested Fuzzy Cognitive Map // Sains Malaysiana. 2014. N. 43(11). P. 1781–1790.

252 Moustafa N., Creech G., Sitnikova E., Keshk M. Collaborative anomaly detection framework for handling big data of cloud computing // 2017 military communications and information systems conference (MilCIS). IEEE. 2017. P. 1-6.

253 Moustafa N., Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) // 2015 military communications and information systems conference (MilCIS). IEEE, 2015. P. 1–6.

254 Munaiah N. et al. Characterizing Attacker Behavior in a Cybersecurity Penetration Testing Competition. In 2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM). IEEE, 2019, pp. 1-6.

255 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.

256 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.

257 Noel S. Interactive visualization and text mining for the CAPEC cyber attack catalog // Proceedings of the ACM Intelligent User Interfaces Workshop on Visual Text Analytics. [Электронный ресурс]. – URL:

https://csis.gmu.edu/noel/pubs/2015_CAPEC_viz.pdf (дата обращения 08.04.2021).

258 Noel S. Text Mining for Modeling Cyberattacks // Chapter 14 in the book: Handbook of Statistics. Elsevier B.V. (Part C: Applications and Linguistic Diver-sity). 2018. Vol. 38. P. 461-515. doi: 10.1016 / bs.host.2018.06.001

259 Novokhrestov A., Konev A., Shelupanov A. Model of threats to computer network software //Symmetry. – 2019. – Т. 11. – №. 12. – С. 1506.

260 Nunes E. et al. Darknet and deepnet mining for proactive cybersecurity threat intelligence //2016 IEEE Conference on Intelligence and Security Informatics (ISI). IEEE. 2016. pp. 7-12.

261 Ozesmi U., Ozesmi S.L. Ecological Models Based on People's Knowledge: a Multi-Step Fuzzy Cognitive Mapping Approach //Ecological Modelling. 2004. № 176. P. 43-64.

262 Pandit R. K., Infield D. SCADA-based wind turbine anomaly detection using Gaussian process models for wind turbine condition monitoring purposes // IET Renewable Power Generation. 2018. Vol. 12. № 11. P. 1249-1255.

263 Pang G., Shen C., Cao L., Hengel A. V. D. Deep learning for anomaly detection: A review // ACM Computing Surveys (CSUR). 2021. Vol. 54. № 2. P. 1-38.

264 Panischev O.Y., Makridin A.T., Katasev A.S., Akhmetvaleev A.M., Kataseva D.V Neural network model for detecting network scanning attacks // International Journal of Engineering Research and Technology. 2020. Vol. 13, no 11. P. 3596-3600.

265 Papageorgiou E. (ed.). Fuzzy Cognitive Maps for Applied Sciences and Engineering: From Foundations to Extensions and Learning Algorithms // Springer Science & Business Media. – 2014. – Т. 54. – [Электронный ресурс]. – Режим доступа: http://www.springer.com/us/book/9783642397387, свободный (дата обращения: 01.09.2017).

266 Papageorgiou E.I., Iakovidis D.K. Intuitionistic Fuzzy Cognitive Maps // IEEE Trans. on Fuzzy Systems. 2013. Vol. 21, № 2. P. 342-354.

267 Park S., Lee K. Improved Mitigation of Cyber Threats in IIoT for Smart Cities: A New-Era Approach and Scheme // Sensors. 2021. Vol 21. № 6. P. 1976.

268 Pereira J. Unsupervised anomaly detection in time series data using deep learning // Master's thesis, Instituto Superior Técnico, University of Lisbon, 2018.

269 Poczketa K., Yastrebov A., Papageorgiou E.I. Learning Fuzzy Cognitive Maps Using Structure Optimization Genetic Algorithm // Proc. of the Federated Conf. on Computer Science and Information Systems, ACSIS. 2015. Vol. 5. P. 547-554.

270 Quatrini E., Costantino F., Di Gravio G., Patriarca R. Machine learning for anomaly detection and process phase classification to improve safety and maintenance activities // Journal of Manufacturing Systems. 2020. Vol. 56. P. 117-132.

271 Romanov A, Kurtukova A, Shelupanov A, Fedotova A, Goncharov V. Authorship identification of a russian-language text using support vector machine and deep neural networks //Future Internet. – 2021. – Т. 13. – №. 1. – С. 1-16.
272 Rule-based token, sentence segmentation for Russian language [Электронный ресурс] URL: https://github.com/natasha/razdel (дата обращения: 10.04.2021)
273 Sabitov A., Minnikhanov R., Dagaeva M., Katasev A., Asliamov T. Text Classification in Emergency Calls Management Systems // Studies in Systems, Decision and Control. – 2021. – Vol. 350. – P. 199-210. – DOI 10.1007/978-3-030-67892-0_17.
274 Salmeron J.L. Modelling grey uncertainty with Fuzzy Grey Cognitive Maps // Expert Systems with Applications. 2010. Vol. 37. N. 12. P. 7581–7588.
275 Samala R. K. et al. Hazards of data leakage in machine learning: a study on classification of breast cancer using deep neural networks // Medical Imaging 2020: Computer-Aided Diagnosis. International Society for Optics and Photonics. 2020. Vol. 11314. P. 1131416.
276 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
277 Sarkar S., Vinay S., Maiti J. Text mining based safety risk assessment and prediction of occupational accidents in a steel plant //2016 International Conference on Computational Techniques in Information and Communication Tech-nologies (ICCTICT). – IEEE, 2016. – С. 439-444.
278 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.
279 Shapiro A.F., Koissi M.–C. Risk Assessment Applications of Fuzzy Logic, March 2015. URL: https://www.casact.org/education/annual/2015/presentations/C-13-Shapiro.pdf (дата доступа: 24.09.2017)
280 Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization // ICISSp. 2018. Vol. 1. P. 108–116.
281 Shelupanov A, Evsyutin O, Konev A, Kostyuchenko E, Kruchinin D, Nikiforov D. Information Security Methods—Modern Research Directions //Symmetry – 2019. – Т. 11. – №. 2. – С. 150.
282 Shin H. K. et al. HAI 1.0: HIL-based Augmented ICS Security Dataset // 13th USENIX Workshop on Cyber Security Experimentation and Test (CSET'20). Santa Clara, CA, 2020.

283 Siddiqui M. A., Stokes J. W., Seifert C., Argyle E., McCann R., Neil J., Carroll J. Detecting cyber attacks using anomaly detection with explanations and expert feedback // ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE. 2019. P. 2872-2876.

284 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

285 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.

286 Spanos G., Angeis L., Toloudis D. Assessment of Vulnerability Severity using Text Mining // Proceedings of the 21st Pan-Hellenic Conference, Sept.2017, Larissa, Greece. pp. 1-6.

287 Srinivasa-Desikan B. Natural Language Processing and Computational Linguistics: A practical guide to text analysis with Python, Gensim, spaCy, and Keras. – Packt Publishing Ltd, 2018.

288 Strom B.E. et al. Finding cyber threats with ATT&CK-based analytics // The MITRE Corporation, Bedford, MA, Technical Report № MTR170202. 2017.

289 Stula M., Stipanicev D., Bodrozic L. Intelligent Modeling with Agent-based Fuzzy Cognitive Map // Intern. Journal on Intell. Systems. 2010. Vol.25, N.10. P. 981–1004.

290 Stylios C.D., Groumpos P.P. Fuzzy Cognitive Maps Multi-Model for Complex Manufacturing Systems // IFAC Large Scale Systems: Theory and Applications. Bucharest, Romania, 2001. P. 61–66.

291 Szwed P., Skrzynski P.A. New Lightweight method for security risk assessment based on Fuzzy Cognitive Maps // Intern. Journal on Appl. Math. Comput. Sci. 2014. Vol. 24, N. 1. P. 213–225.

292 Tao Wen, Yuquing Zhang, Gang Yang. A Novel Automatic Severity Vulnerability Assessment Framework // Journal of Communications, Vol. 10. №5. May 2015. pp. 320-329.

293 Tartakovsky A. G., Polunchenko A. S., Sokolov G. Efficient computer network anomaly detection by changepoint detection methods // IEEE Journal of Selected Topics in Signal Processing. 2012. Vol. 7. № 1. P. 4-11.

294 Tavallaee M. et al. A detailed analysis of the KDD CUP 99 data set // 2009 IEEE symposium on computational intelligence for security and defense applications. IEEE, 2009. P. 1–6.

295 Teixeira M.A. et al. SCADA system testbed for cybersecurity research using machine learning approach // Future Internet. 2018. Vol. 10. № 8. C. 76.

296 Ten C. W., Hong J., Liu C. C. Anomaly detection for cybersecurity of the substations // IEEE Transactions on Smart Grid. 2011. Vol. 2. № 4. P. 865-873.

297 Ten C. W., Manimaran G., Liu C. C. Cybersecurity for critical infrastructures: Attack and defense modeling // IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans. 2010. Vol. 40. № 4. P. 853-865.

298 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.

299 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

300 Tobarra L. et al. A Cybersecurity Experience with Cloud Virtual-Remote Laboratories // Multidisciplinary Digital Publishing Institute Proceedings. 2019. Vol. 31. № 1. C. 3.

301 Tuor A., Kaplan S., Hutchinson B., Nichols N., Robinson S. Deep learning for unsupervised insider threat detection in structured cybersecurity data streams // Workshops at the Thirty-First AAAI Conference on Artificial Intelligence. 2017.

302 Urbanska M., Ray I., Home A.E., Roberts M. Structuring a Vulnerability Description for Comprehensive Single System Security Analysis / RMCWiC`2012. [Электронный ресурс]. URL: www.cs.colostate.edu/psysec/papers/urbanskaRMCWiC`2012.pdf. (дата обращения: 01.12.2020).

303 Vallido A., Martin-Guerrero J.D., Lisboa P.J.G. Making Machine Learning Models Interpretable // Proc. of European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, 25-27 April 2012, Bruges, Belgium. P. 163-172.

304 Van der Maaten L., Hinton G. Visualizing data using t-SNE //Journal of machine learning research. – 2008. – Т. 9. – №. 11.

305 Vulfin A.M. et al. Algorithms for detecting network attacks in an enterprise industrial network based on data mining algorithms // Journal of Physics: Conference Series. IOP Publishing, 2021. Vol. 2001. № 1. C. 012004.

306 Vulfin A.M. et al. Network traffic analysis based on machine learning methods // Journal of Physics: Conference Series. IOP Publishing, 2021. Vol. 2001. № 1. P. 012017.

307 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.

308 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.
309 Wåreus E., Martin H. Automated CPE Labeling of CVE Summaries with Machine Learning. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment // 17th International Conference. Lisbon, 2020. Vol. 12223. P. 3-22. doi:10.1007/978-3-030-52683-2_1.
310 Word2Vec: как работать с векторными представлениями слов // Neurohive (Базовый курс). [Электронный ресурс]. – URL: https://neurohive.io/ru/osnovy-data-science/word2vec-vektornye-predstavlenija-slov-dlja-mashinnogo-obuchenija/ (дата обращения 08.04.2021).
311 Wu K. et al. Online Fuzzy Cognitive Map Learning // IEEE Transactions on Fuzzy Systems. 2020. С. 1
312 Xiao H. et al. Embedding and Predicting Software Security Entity Relationships: A Knowledge Graph Based Approach // International Conference on Neural In-formation Processing. Springer, Cham, 2019. P. 50-63.
313 Yadav T., Rao A.M. Technical aspects of cyber kill chain // International Symposium on Security in Computing and Communication. Springer, Cham. 2015. С. 438-452.
314 Yebjah–Bouteng E.O. Using fuzzy cognitive maps (FCMs) To evaluate the vulnerabilities with ICT assets disposal policies // Intern. Journal on Electrical & Computer Sciences IJECS–IJENS. – 2012. – Vol. 12, № 05. – P. 20–31.
315 Yoon B.S., Jetter A.J. Comparative Analysis for Fuzzy Cognitive Mapping // Proc. of 2016 Portland Intern. Conf. on Management of Engineering and Technology (PICMET). 2016. P. 1897-1908.
316 Zhang J.Y., Liu Z.Q., Zhou S. Quotient FCMs – A Decomposition Theory for Fuzzy Cognitive Maps // IEEE Trans. on Fuzzy Systems. Oct. 2003. Vol. 11, No. 5. P. 593-604.
317 Zhang Y. et al. Power system reliability evaluation with SCADA cybersecurity considerations // IEEE Transactions on Smart Grid. 2015. № 4 (6). С. 1707-1721.
318 Актуальные киберугрозы: IV квартал 2020 года // Отчет Positive Technologies [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q4/ (дата обращения 08.04.2021).
319 Информационная безопасность интернета вещей (Internet of Things) [Электронный ресурс]. URL: www.tadviser.ru/index.php/Статья:Информационная_безопасность_интернета_вещей_(Internet_of_Things) (дата обращения 20.05.2020).
320 Информационная безопасность интернета вещей: кто вещь, а кто хозяин? [Электронный ресурс]. URL:

http://vvsklyar.blogspot.com/2018/11/blog-post.html (дата обращения 20.05.2020).

321 Калинин Н., Шерварлы В., Петухов А. Общий обзор классификаций угроз безопасности: OWAPS, CWE, CAPEC, WASC [Электронный ресурс]. – URL: https://safe-surf.ru/specialists/article/5210/595970/ (дата обращения 08.04.2021).

322 Кибербезопасность промышленных предприятий под угрозой [Электронный ресурс]. URL: http://www.iksmedia.ru/news/5394915-Kiberbezopasnost-promyshlennyx-pred.html (дата обращения: 12.03.2018).

323 Ландшафт угроз для систем промышленной автоматизации. 2019 год // Kaspersky ICS CERT [Электронный ресурс]. – URL: http: // www.cert.kaspersky.ru (дата обращения 08.04.2021).

324 Лукацкий А. Применимость стандартов NERC CIP в России / Без-опасность инфраструктуры энергоснабжения [Электронный ресурс]. URL: http://www.rza-expo.ru/images/2017/history/2013/day4/C.5-7.pdf (дата обращения 20.05.2020).

325 Обзор стандарта безопасности промышленных систем управления NIST SP 800-82 Rev. 2 [Электронный ресурс]. URL: https://www.ussc.ru/news/id/254 (дата обращения 20.05.2020)

326 Сапожников А. Общий обзор реестров и классификаций уязвимостей (CVE, OSVDB, NDV, Secunia) [Электронный ресурс]. – URL: https://safe-surf.ru/specialists/article/5228/607311/ (дата обращения 08.04.2021).

327 Современные технологии аналитики в кибербезопасности // Газинформ-сервис [Электронный ресурс]. – URL: https://habr.com/ru/company/gaz-is/blog/480980/ (дата обращения 24.08.2021).

328 СПИИРАН. Лаборатория проблем компьютерной безопасности [Электронный ресурс]. URL: http://www.spiiras.nw.ru/ru/scientific-activity/research-units/laboratory-of-problems-of-computer-security.html (дата обращения 20.05.2020).

329 Ярушевский Д. Кибербезопасность АСУ ТП – что это и зачем? Пресс-центр «ДиалогНаука». URL: https://www.dialognauka.ru/press-center/article/13226/ (дата обращения 17.08.2019).

330 Ярушевский Д. Обеспечение безопасности АСУ ТП – краткий обзор семейства стандартов IEC 62443 // Information Security/Информационная безопасность. 2014. № 3 [Электронный ресурс]. URL: http://www.itsec.ru/articles2/Oborandteh/obespechenie-bezopasnosti-asu-tp-kratkiy-obzor-semeystva-standartov-iec-62443 (дата обращения 20.05.2020).

Приложение А. Перечень основных нормативно правовых актов и документов, регламентирующих вопросы обеспечения безопасности объектов КИИ

Основной документ — ФЗ № 187 «О Безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017.

Связанные нормативные документы:

1. Постановление Правительства Российской Федерации от 08.02.2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
2. Постановление Правительства Российской Федерации от 11.07.2018 г. № 808 «О внесении изменения в Правила организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса».
3. Постановление Правительства Российской Федерации от 17.02.2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
4. Указ Президента Российской Федерации от 25.11.2017 г. № 569 «О внесении изменений в Положение о ФСТЭК».
5. Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации — *Концепция утверждена Президентом РФ 12.12.2014 № К 1274.*
6. Постановление Правительства РФ №452 от 13.04.2019 «О внесении изменений в постановление ПП-127 от 08.02.2018».
7. Постановление Правительства РФ №743 от 08.06.2019 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи РФ для обеспечения функционирования значимых объектов КИИ».

Приказы ФСТЭК:

1. Приказ ФСТЭК от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» — *вступил в силу 20.02.2018*.
2. Приказ ФСТЭК России от 11.12.2017 № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» — *вступил в силу 8.01.2018*.
3. Приказ ФСТЭК от 21.12.2017 №235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».
4. Приказ ФСТЭК от 22.12.2017 №236 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».
5. Приказ ФСТЭК от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
6. Приказ ФСТЭК от 26.04.2018 №72 «О внесении изменений в регламент ФСТЭК».
7. Приказ ФСТЭК России №138 от 09.08.2018 «О внесении изменений в Требования к обеспечению ЗИ в АСУ П и ТП на КВО, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК №31, и в Требования по обеспечению безопасности ЗО КИИ РФ, утвержденные приказом ФСТЭК №239».
8. Приказ ФСТЭК России №59 от 21.03.2019 «О внесении изменений в форму направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденную приказом ФСТЭК №236 от 22.12.2017».

9. Приказ ФСТЭК России №60 от 26.03.2019 «О внесении изменений в Требования по обеспечению безопасности значимых объектов КИИ РФ, утвержденные приказом ФСТЭК №239 от 25.12.2017».
10. Информационное сообщение ФСТЭК России №240/22/2339 от 04.05.2018 «О методических документах по вопросам обеспечения безопасности информации в КСИИ РФ».
11. Информационное сообщение ФСТЭК России №240/25/3752 от 24.08.2018 «По вопросам представления перечней объектов КИИ, подлежащих категорированию, и направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».
12. Методический документ ФСТЭК «Меры защиты информационных и автоматизированных систем и содержащейся в них информации» – Документ включит в себя общие положения, рекомендации по выбору мер защиты информации, содержание мер защиты информации. Методический документ будет единым для 17/21/31 приказов. Примерно в это же время ФСТЭК планирует привести приказы и КИИ к единой нумерации требований.

Документы ФСБ:

1. Приказ ФСБ РФ от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам.»
2. Приказ ФСБ РФ от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.»
3. Приказ ФСБ РФ от 24.07.2018 N 368 Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области

реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения.

4. Приказ ФСБ РФ от 06.05.2019 № 196 «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.»
5. Приказ ФСБ РФ от 19.06.2019 № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации.»
6. Приказ ФСБ РФ от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации.»

Ответственность:

Федеральный закон №193-ФЗ от 26.07.2017 «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О безопасности КИИ РФ».

Федеральный закон №194-ФЗ от 26.07.2017 «О внесении изменений в УК РФ и УПК РФ в связи с принятием ФЗ «О безопасности КИИ РФ».

Стандарты:

– ГОСТ Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. – М.: Стандартинформ, 2019;

- ГОСТ Р ИСТО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Стандартинформ, 2011;
- ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. – М.: Стандартинформа, 2018;
- ГОСТ Р 56205-2014 IEC/TS 62443-1-1-2009. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели. – М.: Стандартинформ, 2020;
- ГОСТ Р МЭК 62443-2-1-2015. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики. – М.: Стандартинформ, 2015;
- ГОСТ Р 59547-2021. Защита информации. Мониторинг информационной безопасности. Общие положения (утв. 27.07.2021)
- ГОСТ Р 57700.37-2021. Цифровые двойники изделий;
- ГОСТ Р 57412-2017. Компьютерные модели в процессах разработки, производства и эксплуатации изделий;
- ГОСТ Р 59277-2020 Системы искусственного интеллекта. Классификация систем искусственного интеллекта;
- ГОСТ Р 57700.25-2020. Компьютерные модели и моделирование;
- ГОСТ Р ИСО/МЭК 29161-2019. Информационные технологии. Структура данных. Уникальная идентификация для интернета вещей;
- ГОСТ Р ИСО/МЭК 20546-2021. Информационные технологии. Большие данные. Обзор и словарь;
- ПНСТ 420-2020. Предварительный национальный стандарт Российской Федерации. Информационные технологии. Интернет вещей промышленный. Типовая архитектура

Приложение Б. Результаты анализа структуры формализованных текстовых описаний угроз и уязвимостей

Предварительный анализ корпуса текстов позволит оценить структуру корпуса и возможности применения моделей для построения предикторов. С помощью библиотеки Gensim выполним частотный анализ и оценку длины отдельных текстовых документов (рисунок Б.1).

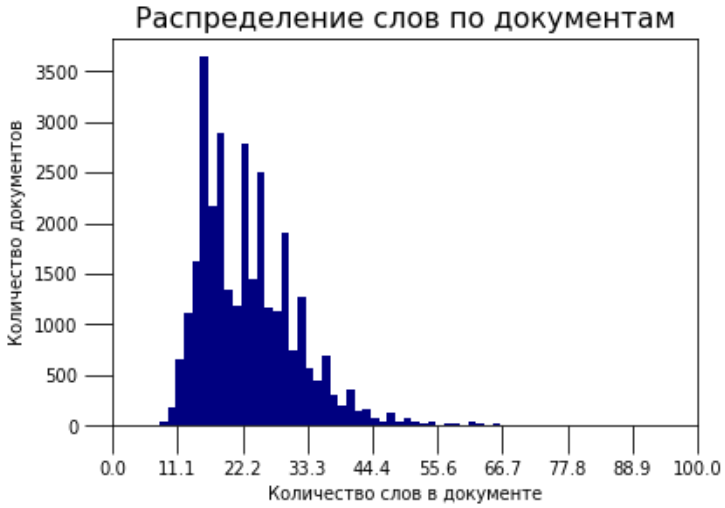


Рисунок Б.1 – Распределение количества слов в документах

Далее выполним тематическое моделирование на основе алгоритма латентного размещения Дирихле (LDA), которое позволит оценить возможность представления текстовых документов в виде смеси автоматически выделенных тем, и привязкой каждого слова к одной из них. Тематическая модель позволяет оценить структурированность текстов и потенциал их группировки по степени семантической близости. Используются значения матрицы близости, основанной на частотных характеристиках документов и лексических единиц для первых четырех выделенных тем, что позволяет оценить словарный состав и частотное распределение слов для каждой из них (рисунок Б.2).

Сложность (обобщающую способность) модели LDA составляет 5,926, а ее когерентность (мера интерпретируемости – оценка согласованности темы) 0,459, что позволяет сделать вывод о наличии структуры у корпуса текстов и возможности построения предикторов, реализующих задачу классификации по компонентам вектора метрики CVSS 2.0/3.0. С помощью t-distributed stochastic neighbor embedding, (стохастическое вложение соседей с распределением Стьюдента t-SNE) выполним понижение размерности признакового пространства и

визуализацию в пространстве двух переменных распределения документов по первым 4 темам (рисунок Б.2).

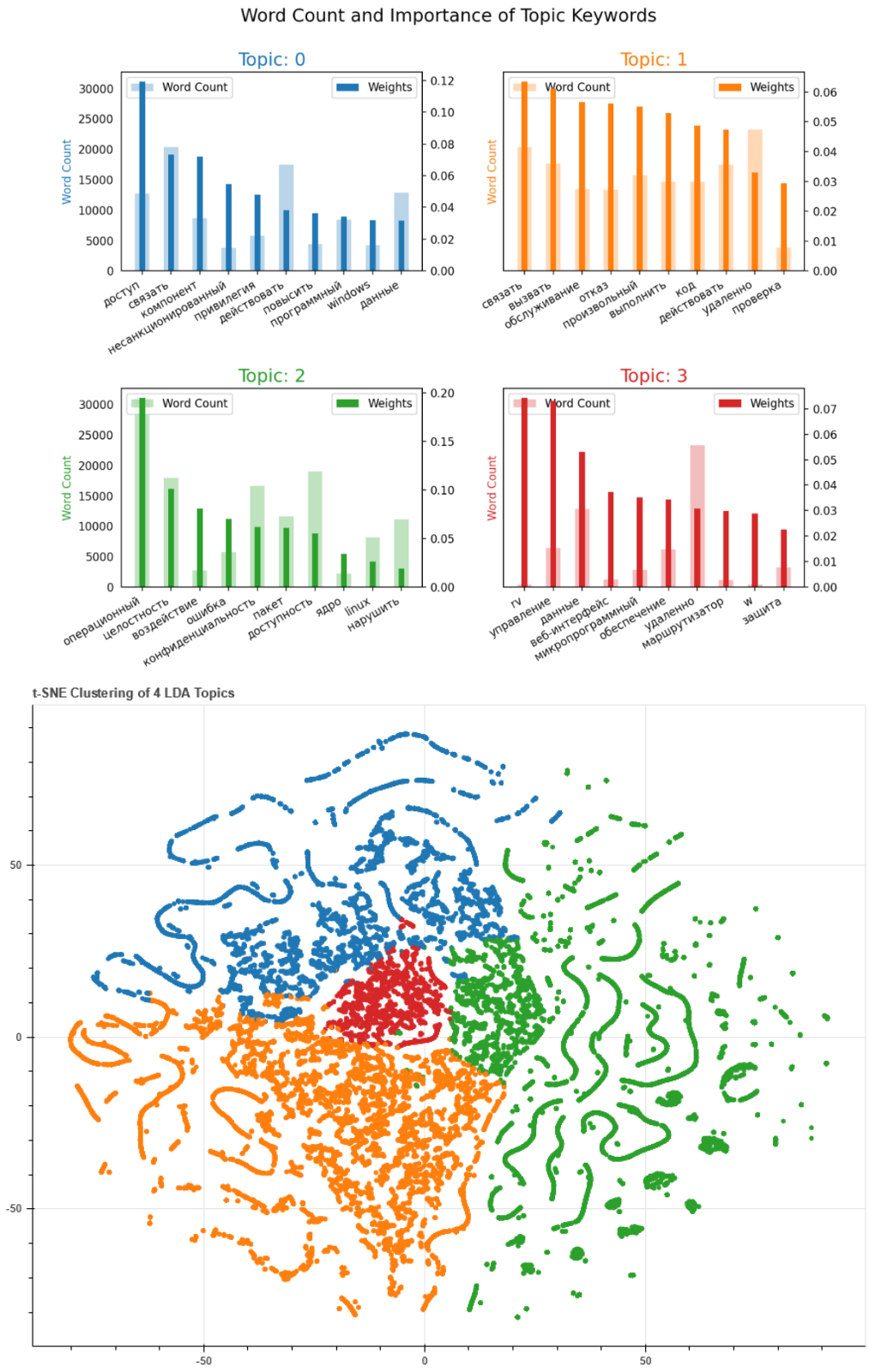


Рисунок Б.2 – Частотные характеристики первых четырех выделенных тем (вверху) и t-SNE визуализация распределения (внизу)

Компактные группы объектов хорошо отделимы друг от друга, однако, наличие характерных выбросов у каждой группы требует дальнейшего анализа

и изменения алгоритма постфильтрации на основе расширяемого стоп-словаря, но не препятствует построению предикторов.

Наличие потенциальной структуры формализованных текстовых описаний уязвимостей на основе модели вложений оценим с помощью алгоритмов кластеризации со случайной расстановкой центроидов с помощью алгоритма k-means++ (рисунок Б.3) с 25 перезапусками.

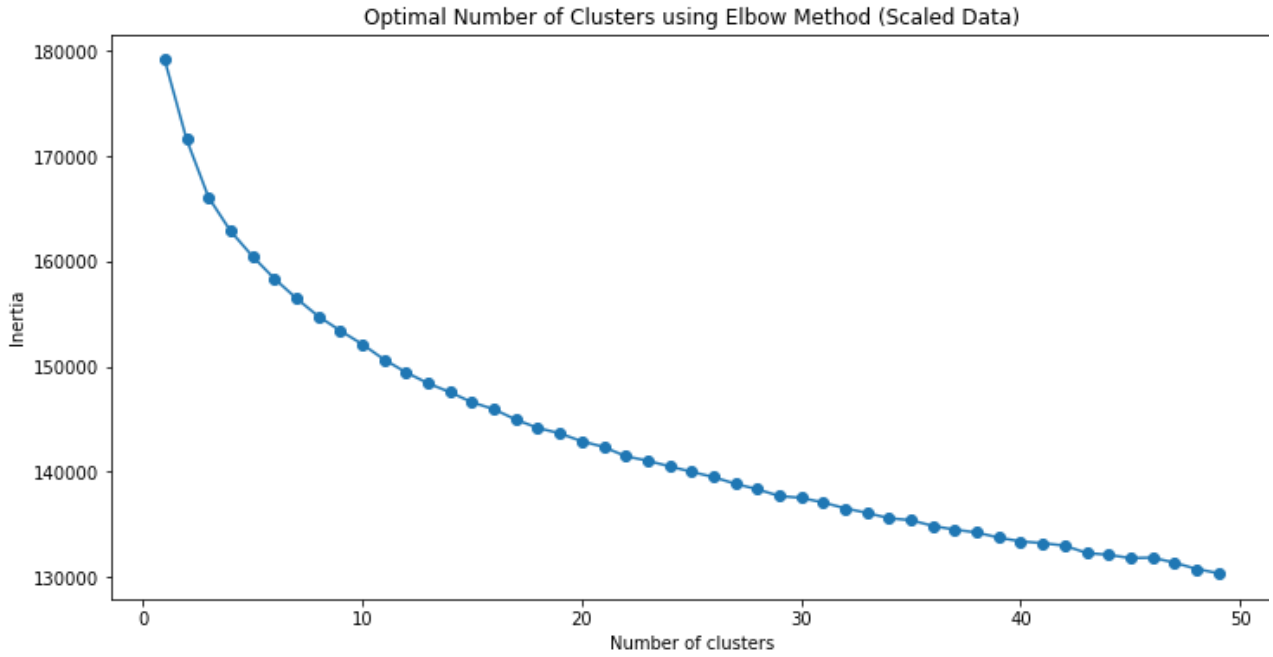


Рисунок Б.3 – Зависимость оценки суммарного квадратичного отклонения точек кластеров от центров этих кластеров (ось ординат) от количества заданных кластеров (ось абсцисс)

При количестве кластеров $k > 15$ наблюдаются устойчивые группы объектов – семантически близких описаний уязвимостей. Для каждого найденного кластера может быть вычислен индекс качества кластеризации – «ширина силуэта»:

$$s_s = \frac{b(i) - a(i)}{\max[b(i), a(i)]}, \quad \text{(Б.1)}$$

где $a(i)$ – среднее расстояние между объектами i-го кластера, $b(i)$ – среднее расстояние от объектов i-го кластера до другого кластера, самого близкого к i-му. При $k > 15$ значение KMeans Scaled Silhouette Score составляет 0,019.

В ходе анализа групп объектов воздействия **ТО** сформирован список из 22 позиций (таблица Б.1)

Таблица Б.1 – Группы объектов воздействия и сформированные для них векторы признаков

Тип	Описание	Токены	Doc2Vec	W2Vec
1	аппаратное обеспечение Аппаратное обеспечение ...	[аппаратный, обеспечение, аппаратный, обеспече...	[0.1193, 0.3398, 0.1125, -0.3715...	[0.2952, 1.6905, -0.86...
2	виртуальная машина Виртуальная машина виртуаль...	[виртуальный, машина, виртуальный, машина, вир...	[0.0019, 0.3936, -0.3379, 0.1901...	[-1.2085, 0.9354, -0.8...
3	Вычислительный узел суперкомпьютера грид-систе...	[вычислительный, узел, суперкомпьютер, грид-си...	[0.4652, 0.1887, 0.0395, -0.3640...	[0.6453, -2.0265, -0.5...
5	информационная система Информационная система ...	[информационный, информационный, информационны...	[0.7289, 0.5184, -0.2491, 0.0358...	[-0.8232, -0.6953, -1....
6	защищаемые данные Информационные ресурсы Инфор...	[защищаемые, данные, информационный, ресурс, х...	[0.3606, 0.3618, -0.4091, 0.2415...	[-0.3120, -0.3690, -0...
…				

Формализованные векторы признаков {D2V; W2V} текстовых описаний объектов воздействия **ТО** зададим как центроиды для алгоритма k-means (рисунок Б.4).

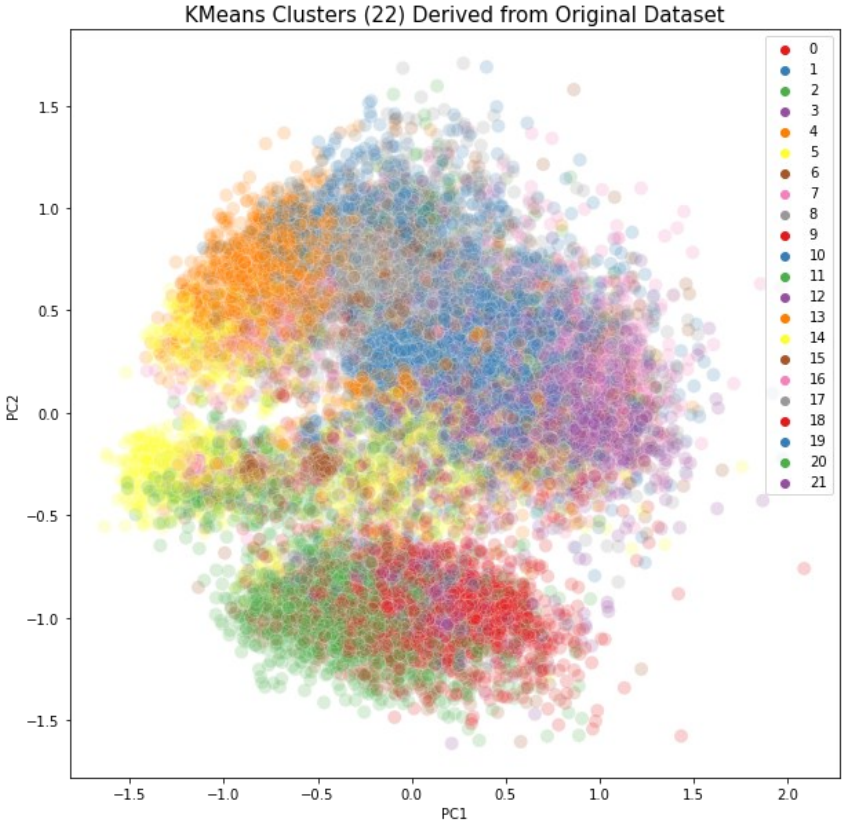


Рисунок Б.4 – Проекция на первые две главные компоненты (PCA) структуры кластеров с заданными центроидами

Значение KMeans Scaled Silhouette Score в этом случае составляет 0,016, что позволяет считать полученное разбиение обоснованным.

Визуализация структуры кластеров с заданными центрами на основе UMAP [237] – взвешенного графа отношений исходных объектов и его приближения с помощью инструментов нечеткой логики и минимизации дивергенций Кульбака-Лейблера – показана на рисунке Б.5. Наличие структуры разбиения подтверждается, но форма кластеров оставляет вопрос о необходимости дальнейшей ручной фильтрации текстовых описаний и пополнения стоп-словарей.

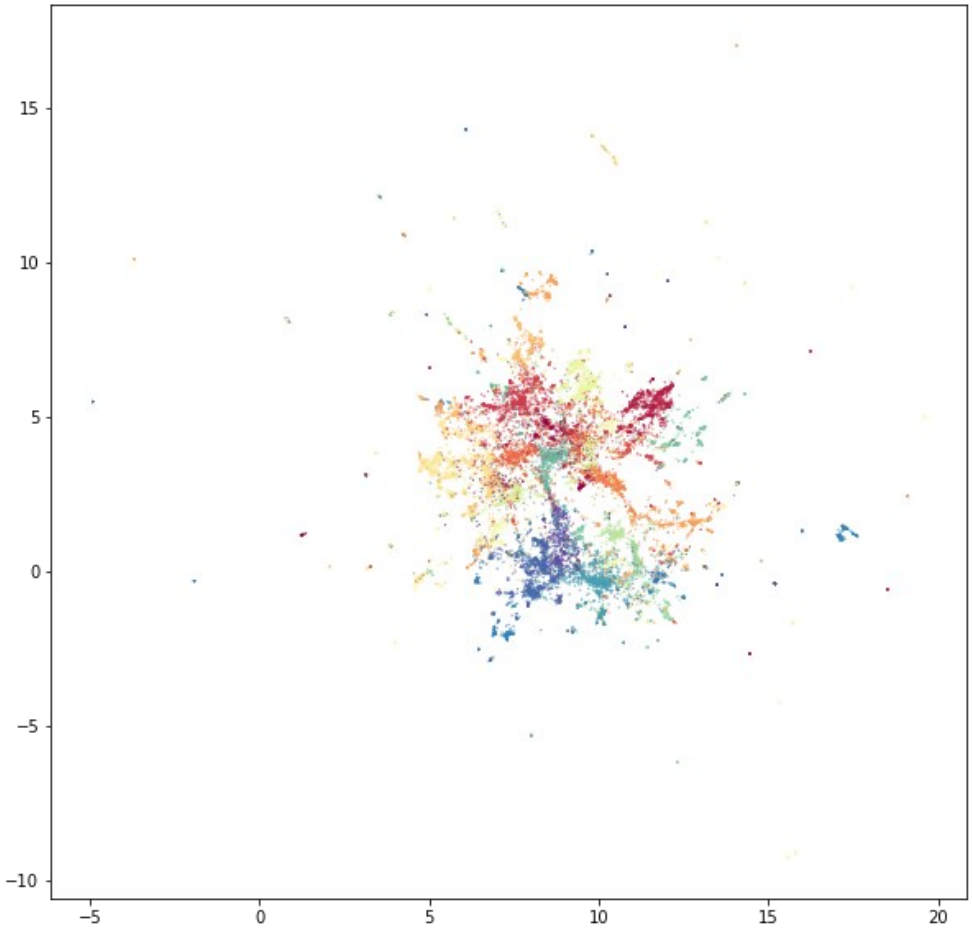


Рисунок Б.5 – Оценка кластерной структуры с помощью UMAP

Понижение размерности пространства признаков с помощью метода главных компонент (PCA) и стохастического вложения соседей с t-распределением (t-distributed Stochastic Neighbor Embedding, t-SNE) [304] не позволяют существенно сократить размерность вектора признаков (рисунок Б.6, рисунок Б.7).

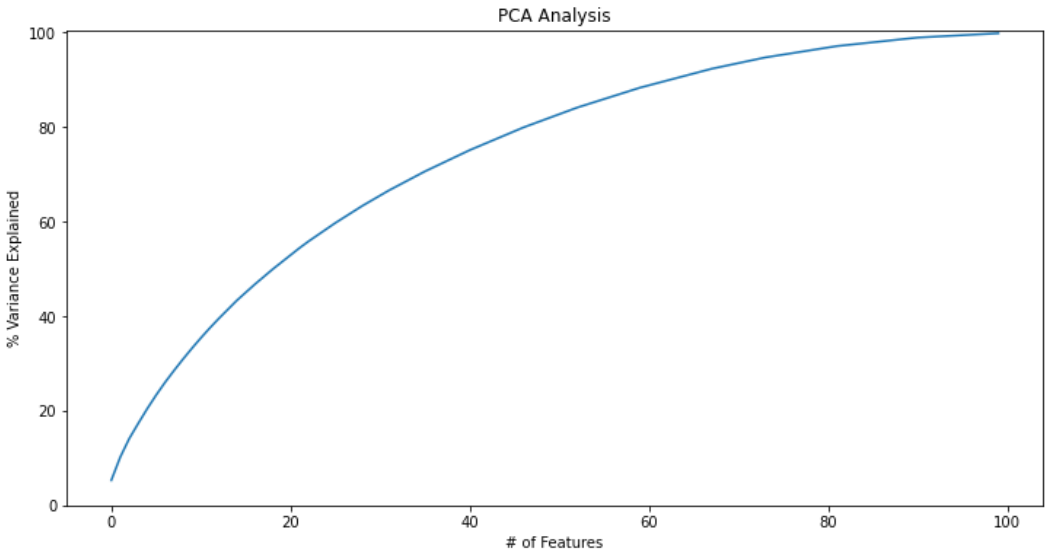


Рисунок Б.6 – Зависимость доли объясняемой дисперсии от количества главных компонент в PCA для вектора D2V

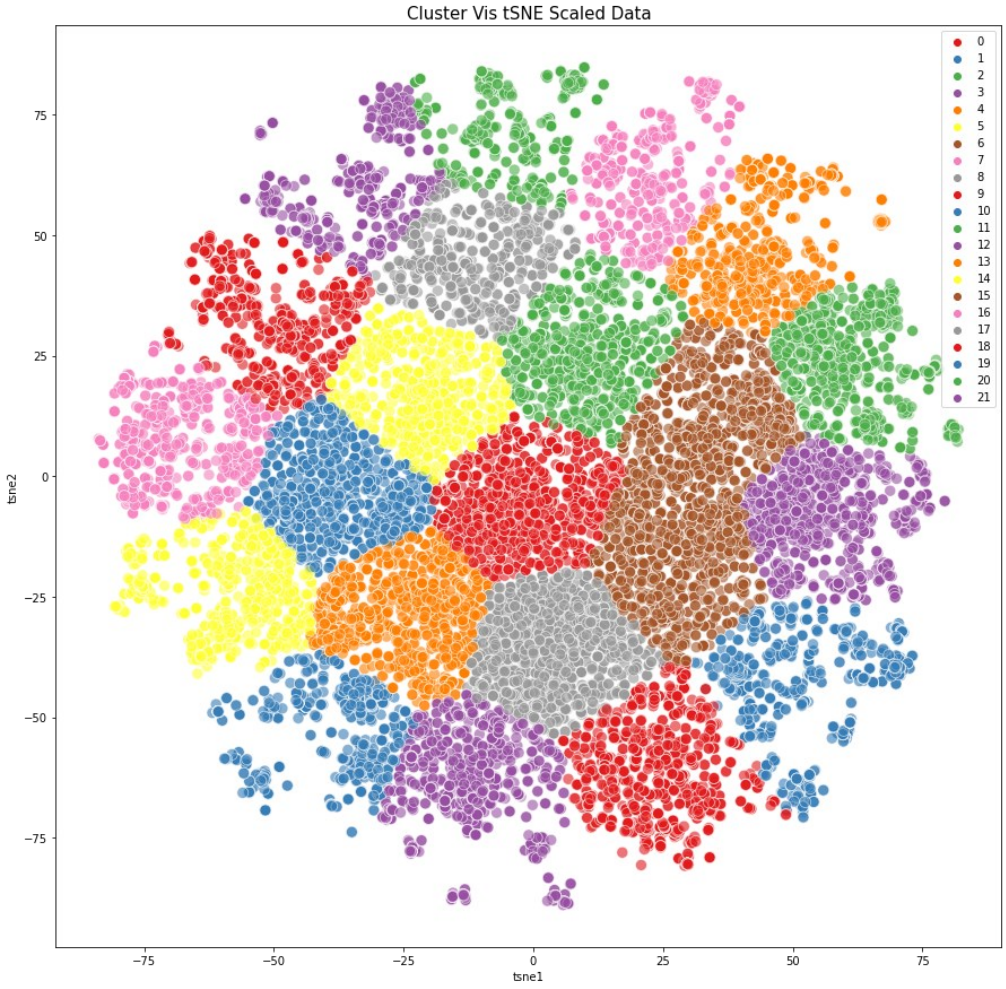


Рисунок Б.7 – Визуализация структуры кластеров для пониженной до 2 с помощью метода t-SNE размерности пространства признаков. Оценка KMeans tSNE Scaled Silhouette Score: 0.347

Приложение В. Общая схема построения нечеткой когнитивной модели оценки рисков ИБ объекта КИИ

Допустим, что необходимо проанализировать последствия от реализации вирусной атаки на некоторый информационный ресурс, располагаемый на рабочей станции (АРМ оператора). Тогда, в соответствии с 3-факторной формулой оценки риска [16], можно воспользоваться схемой НКК, приведенной на рисунке В.1.

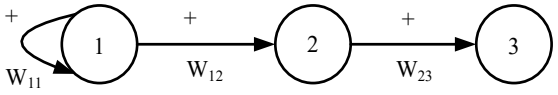


Рисунок В.1 – Нечеткая когнитивная карта для оценки риска

Здесь: 1 – концепт C_1, представляющий собой угрозу (вирусную атаку); 2 – концепт C_2, характеризующий уязвимость (например, отсутствие обновлений антивирусного ПО); 3 – концепт C_3, характеризующий ущерб от нарушения целостности информации вследствие реализации угрозы C_1 через уязвимость C_2.

Переменные состояния: X_1 – вероятность возникновения угрозы; X_2 – вероятность успешной реализации уязвимости; X_3 – величина ущерба от воздействия угрозы (в относительных единицах).

Рассмотрим 2 варианта представления НКК:

а) в виде знакового орграфа;

б) в виде взвешенного графа.

В первом случае будем полагать, что все веса НКК на рисунке В.1 принимают одинаковые значения, равные +1: $W_{11}=W_{12}= W_{23}=1$ (положительные связи). Наличие цикла положительной обратной связи для концепта C_1 указывает на то, что данный концепт выступает в качестве независимого входа (источника), характеризующего воздействие на соседние концепты со стороны внешней среды (в [220] подобные концепты названы *драйверами*). Матрица смежности в данном случае принимает вид:

$$\mathbf{W}=\begin{Vmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{Vmatrix} \qquad \text{(В.1)}$$

С целью анализа устойчивости НКК составим характеристическое уравнение

$$|\mathbf{A} - \lambda \cdot \mathbf{I}| = \begin{vmatrix} 1-\lambda & 1 & 0 \\ 0 & -\lambda & 1 \\ 0 & 0 & -\lambda \end{vmatrix} = \lambda^2 (1-\lambda) = 0, \quad \text{(B.2)}$$

корни которого (т.е. собственные числа матрицы **W**) в данном случае принимают значения $\lambda_{1,2} = 0$; $\lambda_3 = 1$. Следовательно, в соответствии с приведенным выше Утверждением 1, данный орграф является импульсно (абсолютно) устойчивым.

Переходя к взвешенному орграфу (рисунок В.1), предположим, что эксперт назначил следующие значения весов связей НКК: W_{11}=1, W_{12}=W_{23}=0,8 (т.е. связи между концептами C_1, C_2 и C_3 – «сильные»). Введение цикла положительной обратной связи для концепта C_1 (W_{11}=1) позволяет принудительно «удерживать» его начальное состояние $X_1(0)$=1 в последующие моменты времени, принимая в дальнейшем $X(t)$=1 для всех t=1,2,… .Воспользовавшись уравнениями состояния (5)-(6) для начальных условий $X(0)$=(1,0,0), находим установившееся (равновесное) значение переменной X_3, т.е. риска; X_3^*=R=0,63. Таким образом, максимальное значение ущерба от реализации угрозы (вирусной атаки) при отсутствии специальных мер защиты составляет 0,63, т.е. 63% от максимальной границы возможного ущерба R_{max}=1.

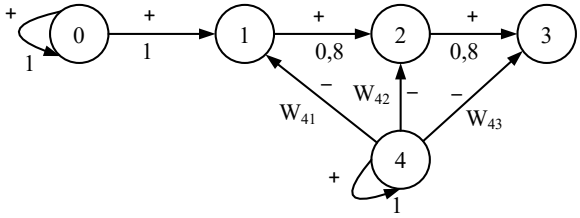
Потребуем, чтобы за счет принятия дополнительных контрмер риск снизился до некоторого минимального (допустимого) уровня. При этом можно воспользоваться следующими рекомендуемыми способами управления риском [16]:

- уменьшение вероятности воздействия угрозы на информационные ресурсы;

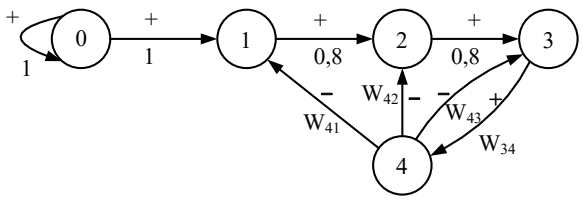
- уменьшение вероятности использования уязвимости;

- уменьшение возможного ущерба путем обнаружения нежелательных событий, реагирования и восстановления ресурса.

Рассмотрим два варианта управления риском, реализующих указанные способы (рисунке В.2): а) «жесткое» (централизованное) управление; б) «мягкое» (адаптивное) управление.



а)



б)

Рисунок В.2 – Схемы НКК для управления риском

На рисунке В.2: C_1 – угроза (вирусная атака); C_2 – уязвимость (отсутствие обновления антивирусного ПО); C_3 – ущерб от реализации угрозы; C_4 – контрмеры по защите информации. Дополнительно введенные отрицательные связи с весами W_{41}, W_{42}, W_{43} характеризуют соответственно влияние контрмер на основные факторы, определяющие уровень риска:

- $C_4 \to C_1$: распознавание и блокирование вируса на ранней стадии;
- $C_4 \to C_2$: обновление антивирусного ПО;
- $C_4 \to C_3$: частичное или полное восстановление искаженной информации.

Дополнительно введенный концепт C_0 выполняет функцию драйвера, обеспечивая значение вероятности «исходной» угрозы X_0 (t) =1 для всех t =0,1,2,…. Переменная X_1 характеризует вероятность «модифицированной» угрозы с учетом влияния концепта C_4. Переменная X_4 в обоих случаях (рисунок В.2, а-б) определяет ресурсы, выделенные на реализацию мер защиты информации. Дополнительная связь $C_3 \to C_4$ с весом W_{34} характеризует учет результатов контроля (мониторинга) за состоянием защищаемой информации C_4. Различие между 2-мя указанными выше вариантами состоит в том, что в 1-ом случае (рисунок В.2, а) ресурсы концепта-драйвера C_4 жестко выделяются в фиксированном объеме и затем перераспределяются по выполняемым функциям защиты, а во 2-ом случае (рисунок В.2, б) величина этих ресурсов зависит от фактического состояния защищенности информации (ущерба) C_3 и может варьироваться в определенных пределах.

НКК на рисунок В.2, а имеет 2 контура положительной обратной связи ($C_0 \to C_0$, $C_4 \to C_4$) для драйверов C_0 и C_4, а НКК на рисунок В.2, б – 1 контур положительной обратной связи ($C_0 \to C_0$) и 3 контура отрицательной обратной связи ($C_4 \to C_3 \to C_4$; $C_4 \to C_2 \to C_3 \to C_4$; $C_4 \to C_1 \to C_2 \to C_3 \to C_4$). Матрицы смежности для обоих вариантов запишутся соответственно как

$$\mathbf{W_а}=\begin{Vmatrix}1 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 0\\ 0 & -1 & -1 & -1 & 1\end{Vmatrix};\ \mathbf{W_б}=\begin{Vmatrix}1 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1\\ 0 & -1 & -1 & -1 & 0\end{Vmatrix}, \qquad (В.3)$$

откуда получаем характеристические уравнения: $|\mathbf{W_а} - \lambda\cdot\mathbf{I}| = \lambda^2(1-\lambda)^3 = 0$; $|\mathbf{W_б} - \lambda\cdot\mathbf{I}| = \lambda^2(1-\lambda)(\lambda^2-\lambda+1)$. Учитывая, что корни этих уравнений принимают значения $\lambda_{1,2}=0$; $\lambda_{3,4,5}= 1$ (для варианта а) и $\lambda_{1,2}= 0$; $\lambda_3=1$; $\lambda_{4,5} = \frac{1}{2}\pm j\frac{\sqrt{3}}{2}$ (для варианта б), можно сделать вывод о том, что оба этих варианта НКК импульсно (абсолютно) устойчивы.

Допустим далее, что изначально заданные значения весов связей $W_{12}=W_{23}=0{,}8$ сохраняются, а значения весов W_{41}, W_{42}, W_{43}, W_{34} назначаются экспертом (соответствующие варианты задания весов для каждой из 2-х схем, приведенных на рисунке В.2, а-б, представлены в таблице). Легко проверить, что условие устойчивости (8) во всех случаях выполняется (веса связей-драйверов $W_{00}=W_{01}=1$ и $W_{44}=1$ в данном случае не учитываются [162, 163]). Таким образом, оператор в правой части уравнений (5) является оператором сжатия и, следовательно, для заданных начальных условий $X(0)= (1,0,0,0,1)^т$ – для схемы на рисунке В.2,а и $X(0) = (1,0,0,0,0)^т$ – для схемы на рисунке В.2,б достигается установившееся (равновесное) состояние $X^*=(X_0^*, X_1^*, X_2^*, X_3^*, X_4^*)^т$. Результаты моделирования, полученные с помощью разработанного авторами автоматизированного пакета FCMBuilder [111], приведены в таблице В.1.

Таблица В.1 – Результаты моделирования

№ варианта	W_{41}	W_{42}	W_{43}	W_{34}	X_1^*	X_2^*	$X_3^*=R$	X_4^*
а -1	-0,8	-0,5	-0,5	0	0,55	0,49	0,47	1
а -2	-0,5	-0,8	-0,5	0	0,62	0,43	0,46	1
а -3	-0,8	-0,8	-0,5	0	0,55	0,41	0,46	1
а -4	-0,8	-0,8	-0,8	0	0,55	0,41	0,38	1
б -1	-0,8	-0,5	-0,5	0,5	0,63	0,56	0,55	0,57
б -2	-0,5	-0,8	-0,5	0,5	0,67	0,52	0,53	0,57
б -3	-0,8	-0,8	-0,5	0,5	0,63	0,51	0,53	0,57
б -4	-0,8	-0,8	-0,8	0,5	0,63	0,51	0,48	0,59

Приложение Г. Оценка рисков ИБ системы сбора, хранения и обработки ТМИ о состоянии подсистем ЛА с помощью серых когнитивных карт

Разработанная в [19, 30, 66, 73, 116, 117, 125, 135] автоматизированная информационная система (АИС) наземных служб технического обслуживания представляет собой набор программных и аппаратных средств, необходимых для приема, хранения и обработки информации о параметрах состояния сложных технических изделий (СТИ) на борту ЛА. АИС является территориально распределенной системой, объединяющей инфраструктуру информационных систем наземных станций технического обслуживания и информационную систему ПИ посредством защищенных каналов связи. Получение ТМИ реализовано посредством считывания журнала состояния СТИ на борту ЛА при проведении технического осмотра и обслуживания на наземных станциях с помощью беспроводных и/или проводных сенсорных сетей.

Анализ основных отдельных аспектов построения защищенной системы сбора, хранения и обработки ТМИ наземными службами технического обслуживания рассмотрен в работах автора [117, 125, 135, 153].

АИС решает основные задачи, связанные с приёмом ТМИ о состоянии бортовых систем ЛА. Основные способы получения данных:

1. Непосредственно с борта ЛА по организованному защищенному радиоканалу;
2. Посредством считывания журнала состояния СТИ на протяжении всего предыдущего периода эксплуатации при проведении технического осмотра и обслуживания ЛА на наземной станции [47, 153].
3. Внесение данных журнала событий оператором в базу хранимой ТМИ на ПИ в автоматизированном режиме через защищенное соединение с помощью Web-приложений [47].

Обобщенная структура территориально распределенной модульной системы сбора, хранения и обработки ТМИ, поступающей с ЛА, разработана в [66] и представлена на рис. Г.0. Защищенная система сбора, хранения и обработки ТМИ о состоянии бортовых подсистем ЛА строится исходя из модульного принципа и содержит достаточно крупные подсистемы с высокой степенью связности компонент внутри и достаточной степенью автономности на уровне взаимодействия самих подсистем. Каждый уровень и подсистемы строятся на основе

организационных принципов, характерных для специфики решаемой задачи, и регламентируются существующими нормативными документами.

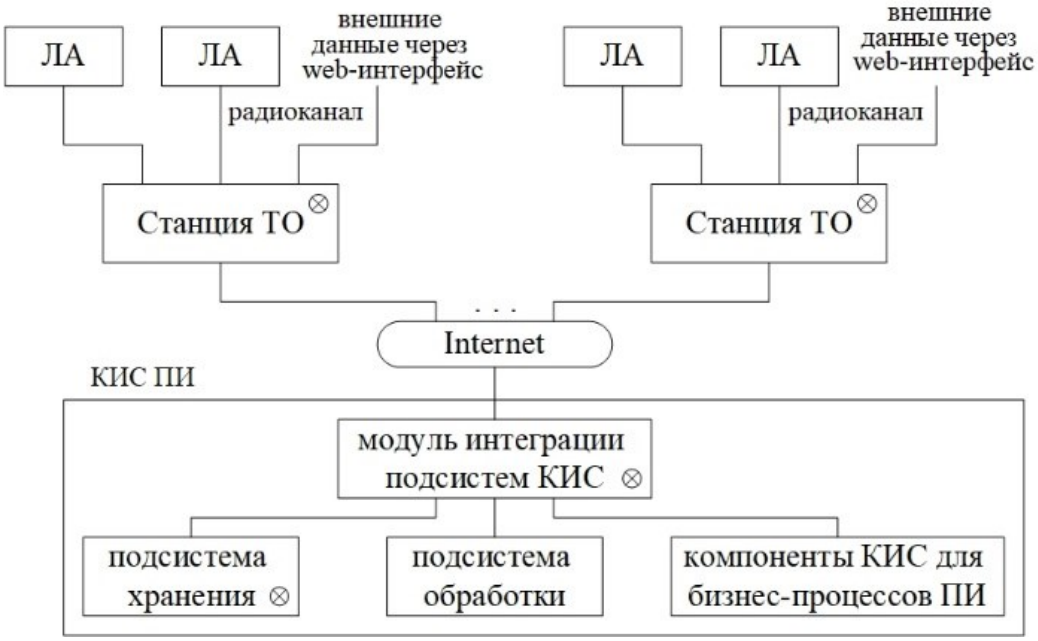


Рисунок Г.0 – Обобщенная структурная схема защищенной системы сбора, хранения и обработки ТМИ (⊗ – зоны воздействия внешних и внутренних угроз)

Уровень сбора ТМИ систем наземных станций технического обслуживания ЛА представляет собой реализацию гетерогенной (с проводным и беспроводным сегментом) сенсорной сети первичного сбора ТМИ с выходных интерфейсов бортовых систем ЛА.

На уровне первичного накопления и подготовки ТМИ к передаче в часть сети предприятия изготовителя реализуется предварительное хранение накапливаемых данных, мониторинг и диагностика состояния системы сбора.

На уровне передачи накопленных данных реализовано создание защищенного канала через глобальные инфокоммуникационные сети и передача ТМИ в сеть АИС ПИ для последующего хранения и обработки. Система сбора, хранения и обработки ТМИ использует комплекс средств защиты информации (СЗИ), направленных на обеспечение безопасности информации ПИ. Криптошлюз «Континент» позволяет создавать VPN-канал между сетями предприятия в соответствии с криптоалгоритмом ГОСТ 28147-89 (L3 VPN-сети).

В составе корпоративной информационной сети (КИС) ПИ выделяется уровень, включающий подсистемы хранения и обработки ТМИ, а также сегмент, предназначенный для поддержки и реализации бизнес-процессов ПИ. Для обеспечения защищенности подсистем, реализующих первые два уровня

предлагаемой структуры были учтены требования нормативных документов международного и федерального стандарта. При проектировании подсистемы беспроводной сенсорной сети сбора ТМИ руководствовались требованиям стандартов.

Физическая архитектура подсистемы сбора и хранения ТМИ на наземных станциях обслуживания ЛА построена в соответствии с NIST 800-82 и ISA/IEC 62443 (рис. Г.1).

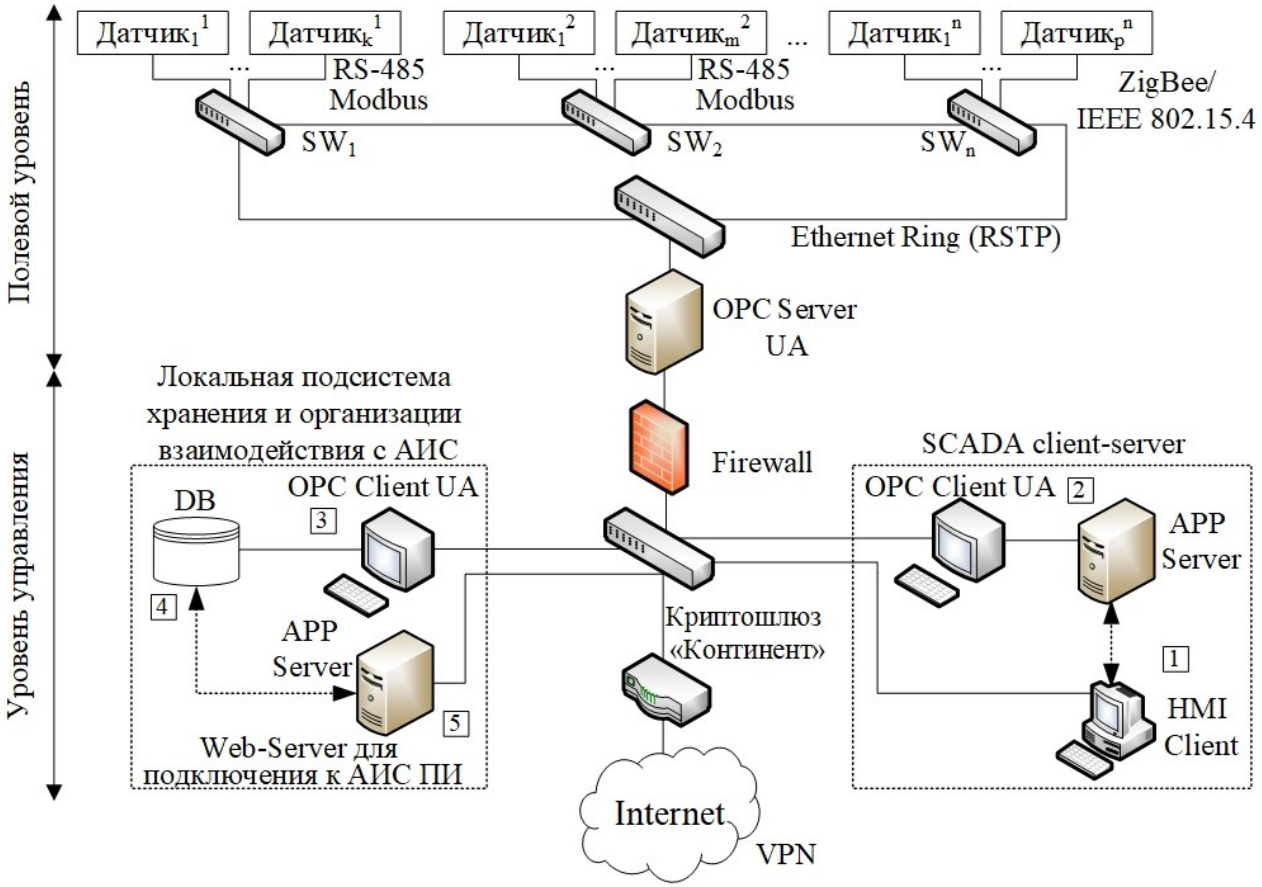
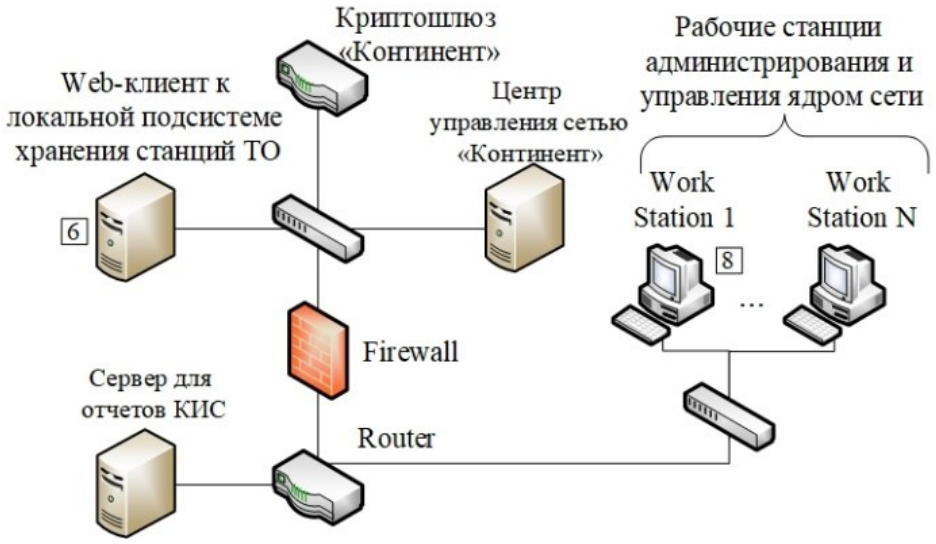


Рисунок Г.1 – Структура подсистемы сбора и хранения данных на станциях обслуживания

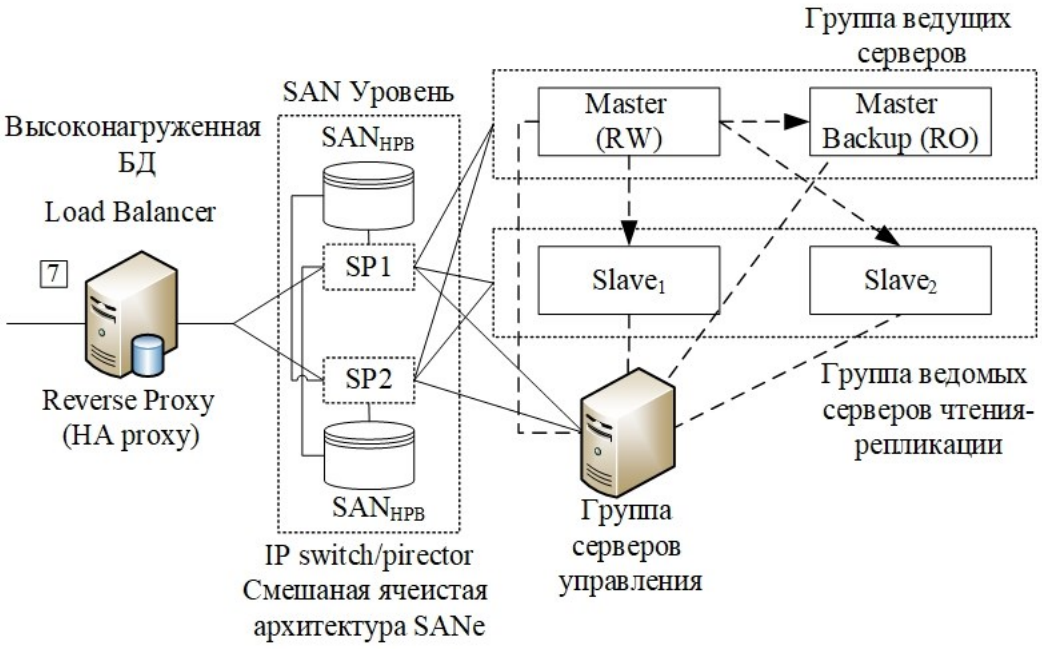
Ядро сети КИС ПИ представлено на рис. Г.2, а.

Web-client обеспечивает подключение к удаленным серверам станций обслуживания и передачу информации в хранилище ПИ. Корневой маршрутизатор реализует объединение подсистемы хранения, подсистемы обработки и КИС ПИ. Станции обслуживания WS_1-WS_N предназначены для администрирования сервисов ядра сети и основных подсистем. Сервер отчетов позволяет обращаться пользователям КИС для построения отчетов о текущем анализе параметров рассогласования модельных и натурных данных ТМИ СТИ на станциях технического обслуживания.

Для обеспечения хранения ТМИ и эффективного доступа к накапливаемым объемам данных необходимо построение отказоустойчивой системы хранения на основе использования механизмов репликации СУБД MySQL (рис. Г.2, б).



а)



б)

Рисунок Г.2. а – ядро КИС предприятия-изготовителя; б – структура подсистемы хранения ТМИ с функциями отказоустойчивости

Состав и основные элементы подсистем описаны в таблице 1 (где C_i^j – элемент подсистемы, i – номер элемента в подсистеме, j – номер подсистемы).

Таблица Г.1 –**Элементы подсистем защищенной системы сбора, хранения и обработки ТМИ**

Подсистема сбора и хранения данных на станциях обслуживания	
Firewall[1]	Межсетевой экран для организации DMZ, разграничивающей Field Network и Control Network станции обслуживания
Криптошлюз «Континент»[1]	Создание VPN-канала между сетями предприятия; Межсетевой экран для организации DMZ, разграничивающей Control Network станции обслуживания и сеть Internet Маршрутизатор для реализации опорной сети станции обслуживания
HMI $Client_1$[1]	ПК, предоставляющий возможность запуска в браузере клиентской части SCADA системы на основе Web-приложения.
APP $Server_2$[1]	Сервер приложений, предназначенный для запуска серверной части SCADA системы
OPC Client UA_3[1]	Клиент для взаимодействия с сервером OPC на основе спецификации Unified Architecture [20]
DB_4[1]	СУБД и хранилище данных для размещения оперативных данных телеметрии, накапливаемых на объекте.
APP $Server_5$[1]	Сервер приложений, предназначенный для запуска серверной части системы передачи данных в хранилище данных ПИ на основе Web-приложения
Подсистема хранения ТМИ с функциями отказоустойчивости	
Reverse Proxy (HA $proxy)_7$[2]	Узел, обеспечивающий доступ к распределенному хранилищу данных ТМИ на ПИ
Модуль интеграции подсистем КИС	
Криптошлюз «Континент»[0]	Маршрутизатор пограничный для сети ПИ и сети провайдера Межсетевой экран для организации DMZ, разграничивающей клиентский модуль для организации доступа к удаленному серверу APP $Server_5$[1] станции обслуживания и опорной сети КИС ПИ
Router[0]	Маршрутизатор опорной сети ПИ для обеспечения изоляции подсети хранения, КИС, подсети обработки информации.
Firewall[0]	Межсетевой экран для организации DMZ, разграничивающей клиентский модуль для организации доступа к удаленному серверу APP $Server_5$[1] станции обслуживания и опорной сети КИС ПИ
Web $Client_6$[0]	Клиентский модуль для организации доступа к удаленному серверу APP $Server_5$[1] станции обслуживания с целью передачи накопленных оперативных данных ТМИ в хранилище ПИ
Work $Station_8$[0]	АРМ администратора и обслуживающего персонала опорной сети КИС ПИ
Центр управления сетью «Континент»	Обеспечивает управление защищенными каналами связи с удаленными станциями ТО и ядром КИС ПИ
Сервер для отчетов КИС	Предоставляет сервис для пользователей КИС ПИ для построения отчетов о текущем анализе параметров рассогласования модельных и натурных данных ТМИ СТИ на станциях ТО.

Угрозы, связанные с нарушением целостности телеметрических данных, способны привести к получению ПИ неверных данных о состоянии ЛА. Автором предложена [73] концепция системы мониторинга целостности ТМИ, реализующей постоянный мониторинг и моделирование параметров СТИ для выявления значимых отклонений от выделенных шаблонов режимов работы, которые, в свою очередь, будут указывать на возможные действия внешних и внутренних угроз на ТМИ.

Приведен перечень угроз несанкционированного доступа (НСД) к отдельным узлам распределенной системе сбора, передачи, хранения и обработки ТМИ с применением программных и программно-аппаратных средств, которые могут быть реализованы с целью нарушения целостности информации:

1) Угроза воздействия на программно-аппаратные узлы АИС:

- Угроза воздействия на программное обеспечение с высокими привилегиями;
- Угроза изменения системных и глобальных переменных;
- Угроза нарушения технологии обработки информации;
- Угроза некорректного использования функционала программного и аппаратного обеспечения;
- Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;
- Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства;
- Угроза несанкционированного управления синхронизацией и состоянием;
- Угроза повышения привилегий;
- Угроза несанкционированного воздействия на средство защиты информации;
- Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения;
- Угроза перехвата управления информационной системой.

2) Угроза воздействия на узлы сетевой инфраструктуры АИС:

- Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети.

Анализ объекта защиты с точки зрения наличия уязвимостей обеспечивает максимальную полноту описания возможных угроз.

Можно выделить следующие классы уязвимостей рассматриваемой системы:

- уязвимости системного и прикладного ПО;
- уязвимости аппаратного обеспечения;
- уязвимости протоколов сетевого взаимодействия.

Исходя из рассматриваемых классов уязвимостей и на основании Банка данных угроз безопасности информации ФСТЭК, построен декомпозированный список уязвимостей, потенциально имеющихся у основных программно-аппаратных узлов АИС, эксплуатация которых ведет к нарушению целостности ТМИ:

- Уязвимости механизма проверки входных данных и команд API, а также мер по разграничению доступа;
- Уязвимости механизма контроля доступа к разделяемой памяти, а также уязвимостями программных модулей приложений, реализующих контроль целостности внешних переменных;
- Уязвимости виртуальной машины, обеспечивающей изолированность адресного пространства;
- Уязвимость механизма управления синхронизацией и состоянием;
- Уязвимости в средствах разграничения доступа к памяти и контроля целостности содержимого ячеек памяти;
- Уязвимости программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации);
- Уязвимость механизма проверки целостности обрабатываемых файлов и корректности, содержащихся в них данных;
- Уязвимости программной среды управления средством защиты информации.

В зависимости от наличия права постоянного или разового доступа в контролируемую зону, в пределах которой размещается оборудование системы, рассматриваются внешние и внутренние нарушители. Общая классификация рассматриваемых нарушителей в зависимости от предоставленных и прав доступа с описанием способов реализации угроз представлена далее.

Внешний нарушитель

В качестве внешнего нарушителя ИБ рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящихся в пределах контролируемой зоны в силу принятых на предприятии мероприятий по ограничению доступа посторонних лиц в контролируемую зону.

Внешний нарушитель может осуществлять следующие действия по нарушению целостности ТМИ:

1) подмену базовой и/или абонентской радиостанции – подавление сигнала базовой/абонентской радиостанции и поднятие на частоте ее радиообмена собственной радиостанции, передающей поддельную информацию;

2) отправку поддельной информации в радиоканал – создание пакета данных с поддельной телеметрической информацией и отправка его базовой/абонентской радиостанции;

3) повторную отправку ранее перехваченной в радиоканале информации – перехват легитимного сообщения, передаваемого по радиоканалу, и его повторная отправка участнику движения через некоторый период времени.

Внутренний нарушитель

Внутренний нарушитель представляет собой сотрудника организации, который обладает определенными правами доступа к техническим средствам и ресурсам системы, находящихся в пределах контролируемой зоны

К внутренним нарушителям могут относиться:

1. Администраторы подсистем и БД:

- Администратор сегмента полевого уровня станции ТО ЛА. Решает задачи конфигурирования и управления распределенной сетевой инфраструктурой гетерогенной сети сбора ТМИ с бортовых систем ЛА, получаемых по радиоканалу, либо с помощью организации проводного подключения к бортовым системам на станции ТО. Точками потенциального воздействия на систему с целью нарушения целостности ТМИ является НСД к OPC-серверу.
- Администратор сегмента управления станции ТО ЛА. Решает задачи конфигурирования и управления сетевой инфраструктурой предварительного хранения ТМИ. Управляет параметрами взаимодействия с полевым уровнем посредствам конфигурирования OPC-сервера. Поддерживает работоспособность программно-аппаратных средств клиент-серверной SCADA-системы. Управляет

работой оперативного хранилища ТМИ на станции ТО ЛА. Управляет работой серверной частью Web-приложения для организации удаленного доступа к оперативному хранилищу из АИС ПИ. Точками потенциального воздействия на систему с целью нарушения целостности ТМИ является НСД к SCADA системе, параметрам оперативного хранилища ТМИ, параметрам серверной части Web-приложения.

- Администратор подсистемы высоконагруженной системы хранения ТМИ в составе АИС ПИ (SAN). Обеспечивает конфигурирование и работу высоконагруженной БД хранения ТМИ. Точками потенциального воздействия на систему с целью нарушения целостности ТМИ является НСД к параметрам конфигурационного сервера хранилища и серверам SAN.
- Администратор подсистемы обработки данных ТМИ с помощью иерархии математических моделей СТИ (Apache Spark, Hadoop). Управляет работой вычислительного кластера, предназначенного для обеспечения работоспособности моделей СТИ. Примененная схема виртуализации на основе построения легковесных контейнеров с встроенными средствами криптозащиты не допускает необнаруживаемого несанкционированного изменения параметров самой модели.

Таким, образом администратор обладает полной информацией о системе (сети), имеет доступ ко всем техническим средствам обработки информации и данным, к средствам защиты информации и протоколирования, обладает правами конфигурирования и административной настройки, конфигурирования и распределения ключевой документации между пользователями. На него возложены задачи администрирования программно-аппаратных средств и БД системы для интеграции и обеспечения взаимодействия различных подсистем. Они потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищенной информации, обрабатываемой и хранимой в системе, а также к техническим и программным средствам, включая средства защиты.

2. Персонал по техническому обслуживанию, сопровождению ПО на защищаемом объекте:

- Специалист по обслуживанию полевой сетевой инфраструктуры станции ТО ЛА. Поддерживает работоспособность полевой инфраструктуры.

- Оператор АРМ сегмента управления станции ТО ЛА. Выполняет мониторинг работы технического процесса сбора данных телеметрии с бортовых систем ЛА. Точка доступа с целью нарушения целостности ТМИ является НСД к узлу, реализующему поддержку HMI SCADA-клиента.
- Специалист обслуживания высоконагруженной системы хранения ТМИ в составе АИС ПИ (SAN). Точка доступа с целью нарушения целостности ТМИ является НСД к конфигурационному серверу хранилища и серверам SAN.
- Специалист обслуживания подсистемы обработки данных ТМИ с помощью иерархии математических моделей СТИ (Apache Spark, Hadoop).

Таким образом, персонал по техническому обслуживанию и сопровождению ПО обладает возможностями внесения закладок в технические средства системы на стадии их внедрения и сопровождения. Они могут обладать любыми фрагментами информации о топологии системы и технических средствах обработки и защиты информации в системе. Обладает частичной информацией об алгоритмах и программах обработки информации, протоколах, реализуемых и используемых в конкретных подсистемах и системе в целом, а также о применяемых принципах и концепциях безопасности, обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО.

3. Начальник сегмента управления:

Обладает всеми возможностями администратора системы. Располагает конфиденциальной информацией, к которой имеет доступ.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в системе конкретные режимные и организационно-технические меры. Таким образом, объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно, поэтому рассматриваются категории внутренних нарушителей только с максимальными правами доступа.

Сценарии поведения внутреннего и внешнего нарушителя отображаются через построение графов атак.

Графы атак являются инструментом топологического анализа защищенности информационной системы и позволяют учитывать взаимосвязь и свойства объектов информационной системы на основе результатов сканирования сети, модели нарушителя и данных о конфигурации сети (правила фильтрации

межсетевого экрана, маршрутизации, обнаружения атак, достижимости хостов и т.д.). Классификация представления графов атак приведена в таблице Г.2.

Для формирования рассуждений в условиях неопределенности в соответствии с оценками вероятностей событий и связи между событиями удобным является построение на основе ориентированного на условия зависимостей графа сетевой модели в виде сети Байеса.

Таблица Г.2 – **Классификация графов атак**

Название	Описание
граф перечисления состояний	вершинам соответствуют тройки (*s*, *d*, *a*), где *s* – источник атаки, *d* – цель атаки, *a* – элементарная атака; дуги обозначают переходы из одного состояния в другое
граф ориентированных на условия зависимостей	вершинам соответствуют результаты атак, а дугам – элементарные атаки, приводящие к таким результатам
граф зависимости эксплойтов	вершины соответствуют результатам атак или элементарным атакам, дуги отображают зависимости между вершинами – условия, необходимые для выполнения атаки и следствие атаки

Рассмотрим уровень сбора ТМИ систем наземных станций технического обслуживания ЛА, который представляет собой реализацию сенсорной сети первичного сбора ТМИ с выходных интерфейсов бортовых систем ЛА с помощью проводных и беспроводных датчиков. На уровне первичного накопления и подготовки ТМИ к передаче в часть АИС ПИ реализуется предварительное хранение накапливаемых данных, мониторинг и диагностика состояния системы сбора.

Целью атаки являются:

- Оперативные данные ТМИ, которые могут быть модифицированы злоумышленником до внесения в БД на узлах SCADA клиент-серверного типа;
- БД хранения оперативных данных ТМИ, которые могут быть модифицированы злоумышленником;
- Накопленные в БД данные, передаваемые через Web-приложение в КИС ПИ.

Граф атак для подсистемы сбора и хранения ТМИ представлен на рис. Г.3 и позволяет проиллюстрировать уязвимости, используемые злоумышленником в ходе реализации угрозы для достижения цели атаки (конечного узла графа атак).

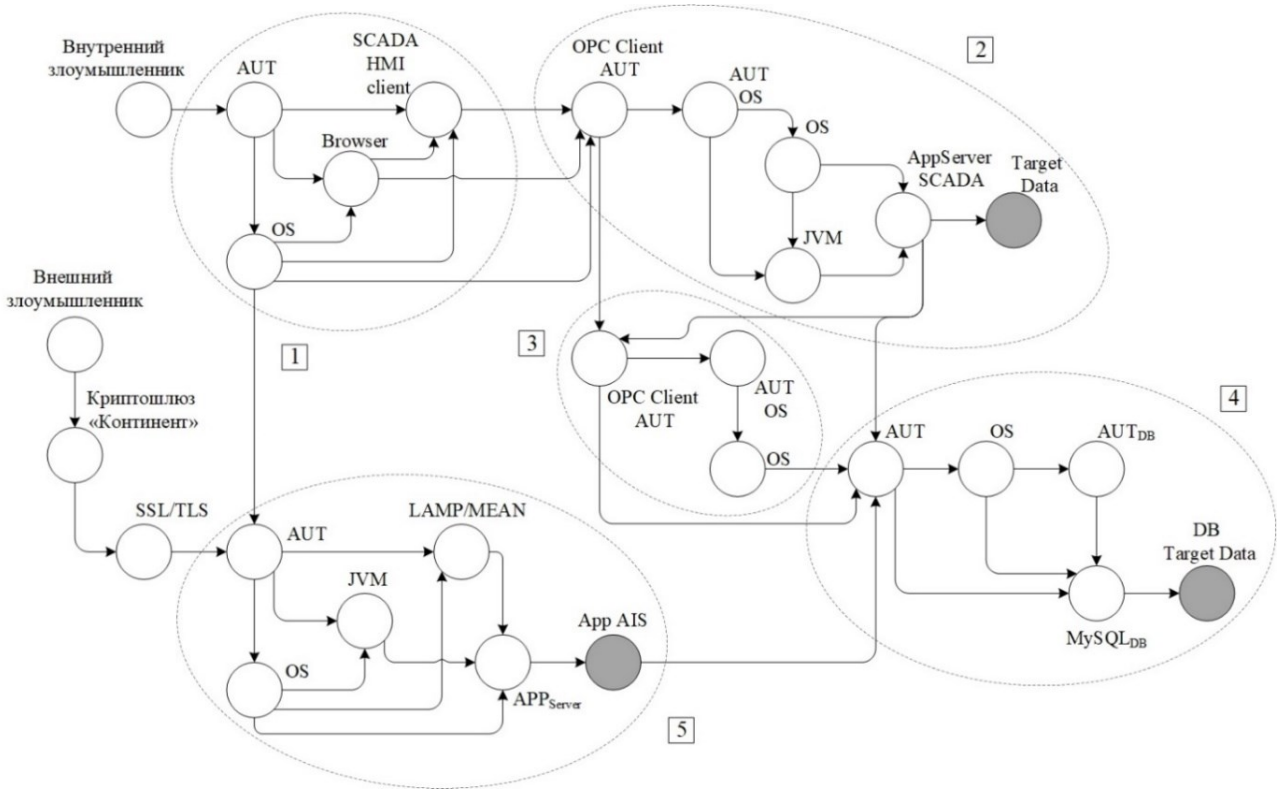


Рисунок Г.3 – Граф реализации угроз для подсистемы сбора и хранения ТМИ на наземных станциях обслуживания ЛА

Описание рассмотренных выше уязвимостей с привязкой к программно-аппаратным элементам системы представлено в таблице Г.3.

Таблица Г.3 – **Уязвимости в составе графа атак для подсистемы сбора и хранения ТМИ на наземных станциях обслуживания ЛА**

1. HMI Client$_1$[1]	
AUT	Эксплуатация уязвимости системы авторизации пользователя ОС (уязвимости механизма проверки входных данных, и мер по разграничению доступа к разделяемой памяти)
SCADA HMI client	Эксплуатация уязвимости прикладного ПО web-клиента SCADA HMI (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
Browser	Эксплуатация уязвимости браузера ОС для запуска клиентской части SCADA HMI (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
OS	Уязвимость доступа к памяти ОС (уязвимость механизма разграничения доступа к памяти)
2. APP Server$_2$[1]	
OPC Client AUT	Эксплуатация уязвимости системы авторизации клиентской части ПО OPC Client UA
AUT OS	Эксплуатация уязвимости системы авторизации основного пользователя ОС (уязвимости механизма проверки входных данных, и мер по разграничению доступа к разделяемой памяти)
OS	Эксплуатация уязвимости доступа к памяти ОС (уязвимость механизма разграничения доступа к памяти)

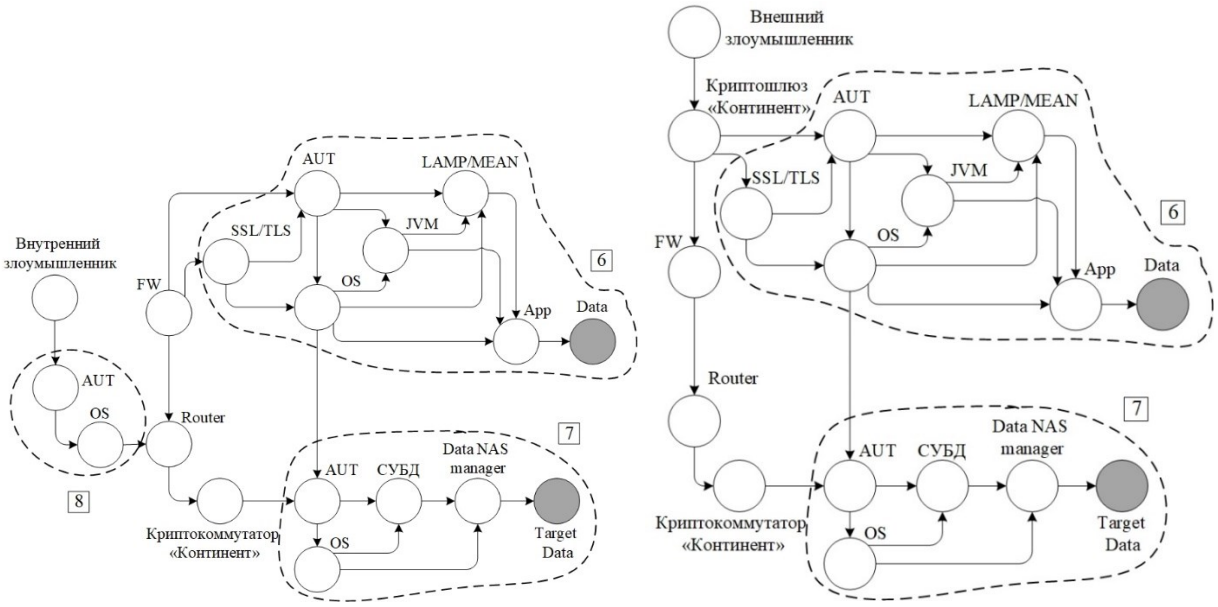
JVM	Эксплуатация уязвимости виртуальной машины Java (уязвимости виртуальной машины, обеспечивающей изолированность адресного пространства)
App Server SCADA	Эксплуатация уязвимости системного ПО сервера приложений для запуска серверного Web-приложения SCADA системы (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
Target Data	Оперативные данные ТМИ, которые могут быть модифицированы злоумышленником до внесения в БД на узлах SCADA client-server type
3. OPC Client UA_3[1]	
OPC Client AUT	Эксплуатация уязвимости системы авторизации клиентской части ПО OPC Client UA (уязвимости механизма проверки входных данных, и мер по разграничению доступа к разделяемой памяти)
AUT OS	Эксплуатация уязвимости системы авторизации основного пользователя ОС (уязвимости механизма проверки входных данных, и мер по разграничению доступа к разделяемой памяти)
OS	Эксплуатация уязвимости доступа к памяти ОС (уязвимость механизма разграничения доступа к памяти)
4. DB_4[1]	
AUT	Эксплуатация уязвимости системы авторизации основного пользователя ОС (уязвимости механизма проверки входных данных, и мер по разграничению доступа к разделяемой памяти)
OS	Эксплуатация уязвимости доступа к памяти ОС (уязвимость механизма разграничения доступа к памяти)
AUT_{DB}	Эксплуатация уязвимости системы авторизации основного пользователя СУБД (уязвимости механизма проверки входных данных, и мер по разграничению доступа к разделяемой памяти)
$MySQL_{DB}$	Эксплуатация уязвимости доступа к памяти СУБД (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
DB Target Data	БД хранения оперативных данных ТМИ, которые могут быть модифицированы злоумышленником
5. APP $Server_5$[1]	
AUT	Эксплуатация уязвимости системы авторизации основного пользователя ОС (уязвимости механизма проверки входных данных, и мер по разграничению доступа к разделяемой памяти)
LAMP/ MEAN	Эксплуатация уязвимости системного ПО, реализующего работу связки сервера веб-приложений Apache, СУБД MySQL, среды исполнения PHP для поддержки интерактивных Web-страниц (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
OS	Эксплуатация уязвимости доступа к памяти ОС (уязвимость механизма разграничения доступа к памяти)
JVM	Эксплуатация уязвимости доступа к памяти виртуальной машины Java (уязвимости виртуальной машины, обеспечивающей изолированность адресного пространства)
App Server	Эксплуатация уязвимости ПО сервера приложений (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
App AIS	Эксплуатация уязвимости Web-приложения для запуска модуля доступа к БД оперативного хранения ТМИ на станциях обслуживания ЛА (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)

Крип-тошлюз «Конти-нент»	Эксплуатация уязвимости программной среды управления маршрутизатора Эксплуатация уязвимости программной среды управления средством защиты информации – межсетевого экрана
SSL/TLS	Эксплуатация уязвимости системного ПО, реализующего создание защищенного сетевого канала

Далее с помощью графа атак проиллюстрирована последовательность эксплуатации уязвимостей, позволяющая нарушить целостность данных в подсистеме хранения ТМИ и в подсистеме ядра КИС ПИ, осуществляющей взаимодействие со станциями ТО посредствам Web-приложения (рис. Г.4, табл. Г.4).

Целью атаки являются:

- ТМИ из оперативного хранилища станций ТО ЛА, получаемые посредством доступа по защищенному каналу к станциям обслуживания ЛА;
- ТМИ в долгосрочном хранилище.



а) б)

Рисунок Г.4 – Граф реализации угроз в подсистеме хранения ТМИ и в подсистеме ядра КИС ПИ (а) внешний злоумышленник; б) внутренний злоумышленник)

Таблица Г.4 – **Уязвимости в составе графа атак для в подсистемы хранения ТМИ и подсистемы ядра КИС ПИ**

6. Web Server$_6^0$	
Криптошлюз «Континент»	Эксплуатация уязвимости программной среды управления маршрутизатора Эксплуатация уязвимости программной среды управления средством защиты информации – межсетевого экрана
AUT	Эксплуатация уязвимости системы авторизации основного пользователя ОС

LAMP/ MEAN	Эксплуатация уязвимости системного ПО, реализующего работу связки сервера веб-приложений Apache, СУБД MySQL, среды исполнения PHP для поддержки интерактивных Web-страниц
SSL/TLS	Эксплуатация уязвимости системного ПО, реализующего создание защищенного сетевого канала (уязвимость сетевых протоколов)
OS	Эксплуатация уязвимости доступа к памяти ОС
JVM	Эксплуатация уязвимости доступа к памяти виртуальной машины Java
App	Эксплуатация уязвимости ПО сервера приложений для организации удаленного защищенного доступа к БД оперативного хранения ТМИ на станциях ТО ЛА (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
Data	ТМИ из оперативного хранилища станций ТО ЛА
7. Reverse Proxy (HA proxy)$_7^2$	
AUT	Эксплуатация уязвимости системы авторизации основного пользователя ОС конфигурационного сервера БД (уязвимости механизма проверки входных данных, и мер по разграничению доступа к разделяемой памяти)
OS	Эксплуатация уязвимости доступа к памяти ОС (уязвимость механизма разграничения доступа к памяти)
СУБД	Эксплуатация уязвимости доступа к памяти СУБД (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
Data NAS manager	Эксплуатация уязвимости доступа к памяти конфигурационного сервера сетевого хранилища (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
Target Data	ТМИ в долгосрочном хранилище
8. Work Station$_8^0$	
AUT	Эксплуатация уязвимости системы авторизации основного пользователя ОС (уязвимости механизма проверки входных данных, и мер по разграничению доступа к разделяемой памяти)
OS	Эксплуатация уязвимости доступа к памяти ОС (уязвимость механизма разграничения доступа к памяти)
Router	Эксплуатация уязвимости программной среды управления маршрутизатора
FW	Эксплуатация уязвимости программной среды управления средством защиты информации – межсетевого экрана

В результате анализа структуры защищенной системы сбора, хранения и обработки ТМИ о состоянии подсистем ЛА выявлены основные угрозы и уязвимости, затрагивающих обеспечение целостности передаваемых и накапливаемых данных ТМИ. На основе результатов анализа разработаны сценарии реализации угроз на основе инструментов топологического анализа защищенности системы, которые позволяют учитывать взаимосвязь и свойства объектов системы на основе результатов анализа уязвимостей, модели нарушителя и данных о конфигурации сети. Разработанные графовые модели является необходимым этапом для последующей оценки рисков ИБ с помощью когнитивного моделирования.

В составе АИС (рис. Г.5) при этом можно выделить следующие подсистемы (зоны), объединяемые по принципу единства выполняемых функций и требований к безопасности их реализации:

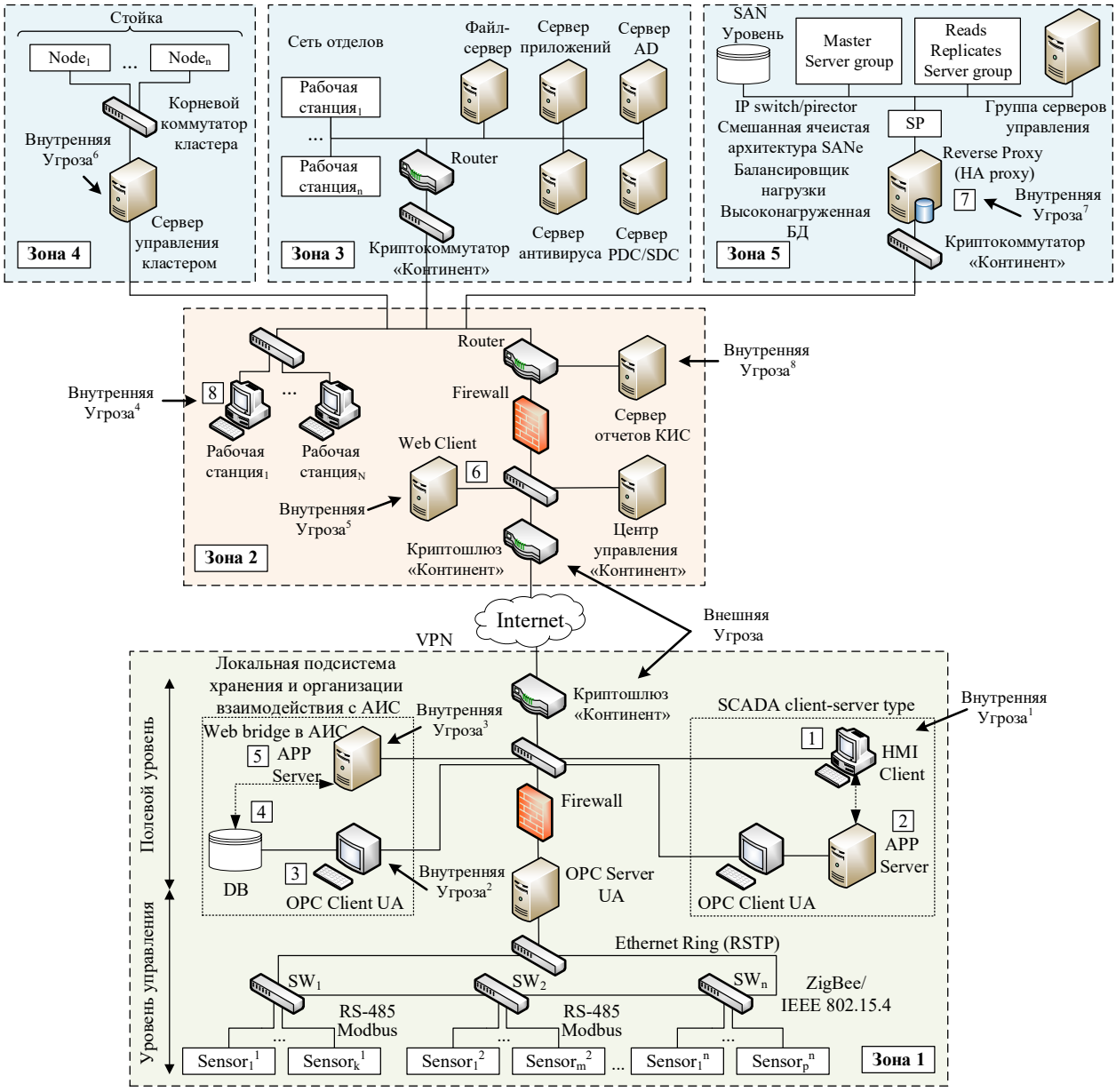


Рисунок Г.5 – Структурная схема АИС сбора, хранения и обработки ТМИ

1) *подсистема сбора и хранения первичных данных на станциях технического обслуживания* (зона 1), в состав которой входят:

– элемент 1 – клиентская часть Web-base SCADA системы;

– элемент 2 – серверная часть Web-base SCADA системы;

– элемент 3 – OPC UA клиент;

– элемент 4 – временное хранилище для размещения оперативных данных телеметрии, накапливаемых на объекте;

элемент 5 – серверная часть системы передачи накопленных данных в хранилище предприятия-изготовителя (ПИ) авиационной техники;

2) *ядро корпоративной информационной сети (КИС)* ПИ (зона 2), где:

– элемент 6 – клиентская часть для организации доступа к серверу станции обслуживания с целью передачи накопленных оперативных данных ТМИ в хранилище ПИ;

– элемент 8 – АРМ администратора и обслуживающего персонала ядра КИС ПИ;

3) *подсистема хранения ТМИ с функциями обеспечения отказоустойчивости* (зона 3), где:

– элемент 7 – узел доступа к хранилищу данных ТМИ на ПИ;

– Cluster management server – сервер управления вычислительным кластером и консоль управления системой мониторинга целостности;

– Core switch – базовый коммутатор вычислительного кластера;

4) *подсистема обработки данных ТМИ с помощью иерархии математических моделей* изделий авиационной техники (зона 4);

5) *подсистема поддержки и реализации бизнес-процессов ПИ* (зона 5).

Соответствующие подсистемы (зоны безопасности) связаны между собой на рисунке Г.5 с помощью каналов телекоммуникаций (трактов).

Будем полагать, что целью моделирования с помощью НСКК является анализ эффективности распределения ресурсов применяемых контрмер (рис. Г.6), а также оценка особенностей их интеграции в существующую информационную систему организации и последующее сопровождение на всех этапах жизненного цикла.

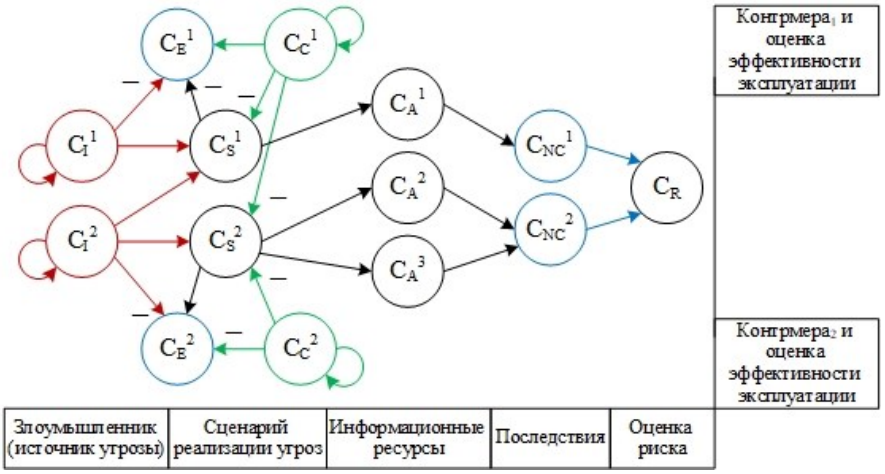


Рисунок Г.6 – НСКК для оценки эффективности распределения ресурсов контрмер

Значение концепта C_R НСКК на рис. Г.6 определяет итоговую оценку X_R риска ИБ для моделируемых сценариев C_S^1 и C_S^2. Значения весовых коэффициентов $W_{C_C^1,C_S^1}, W_{C_C^1,C_S^2}, W_{C_C^2,C_S^2}$ характеризуют распределение ограниченных ресурсов контрмер C_C^1 и C_C^2 при моделировании сценариев реализации угроз нарушения кибербезопасности. Установившиеся значения концептов C_E^1 и C_E^2 позволяют оценить эффективность интеграции и использования каждой контрмеры.

Таким образом, возможна следующая формальная постановка задачи оптимизации:

$$\Phi\left(W_{C_C^i,C_S^j}\right) = X_R \to min,$$

где $\Phi(\cdot)$ – целевая функция, X_R – установившееся значение концепта C_R, $W_{C_C^i,C_S^j}$ – настраиваемые параметры, характеризующие распределение ограниченных ресурсов контрмеры C_C^i для снижения вероятности реализации сценариев угроз C_S^j.

На параметры $W_{C_C^i,C_S^j}$ накладывается ряд условий, связанных со спецификой определения весов в базисе «серых» чисел:

$$\forall W_{C_C^i,C_S^j}: \begin{cases} \overline{W_{C_C^i,C_S^j}},\ \underline{W_{C_C^i,C_S^j}} \in [0;\ 1] \\ \overline{W_{C_C^i,C_S^j}} > \underline{W_{C_C^i,C_S^j}} \\ \sum_i \left[\overline{W_{C_C^i,C_S^j}} + \underline{W_{C_C^i,C_S^j}}\right] < \Theta \end{cases}$$

Для применения классических реализаций алгоритмов оптимизации с ограничениями целевую функцию представим как норму вектора компонент серого числа X_R с дополнительным заданием штрафной компоненты, обеспечивающей корректное определение области значений $\overline{X_R},\ \underline{X_R} \in [0;\ 1]$:

$$\Phi\left(W_{C_C^i,C_S^j}\right) = \left\|\overline{X_R}, \underline{X_R}\right\| + \alpha f\left(\overline{X_R}, \underline{X_R}\right),$$

$$f\left(\overline{X_R}, \underline{X_R}\right) = \begin{cases} 1, \overline{X_R} < 0, \underline{X_R < 0} \\ 0, \text{otherwise} \end{cases}$$

Для оптимизации весовых коэффициентов когнитивной карты возможно использовать генетический алгоритм (ГА).

Анализ соотношения полученных оценок рисков и затрат на мероприятия по их снижению позволяет определить механизмы управления защищенностью целевых ресурсов системы и поддерживать ее необходимый уровень, а также оценивать требуемые при этом затраты на интеграцию и сопровождение

контрмер. В результате работы ГА будет получен набор весовых коэффициентов НСКК, отражающих оптимальное распределение затрат на реализацию мер по снижению риска нарушения кибербезопасности АСУ ТП.

Применение ГА позволяет формулировать задачу многокритериальной оптимизации, например, в следующей постановке:

$$\Phi\left(W_{C_C^i, C_S^j}\right) = X_R \to min, \quad \sum X_R^i \to min,$$

$$\Phi\left(W_{C_C^i, C_S^j}\right) = \left\|\overline{X_R}, \underline{X_R}\right\| + \sum_i \left\|\overline{X_C^i}, \underline{X_C^i}\right\| + \alpha f\left(\overline{X_R}, \underline{X_R}\right) + \beta f\left(\overline{X_C^i}, \underline{X_C^i}\right),$$

учитывающей одновременную минимизацию и оценки риска, и суммарной оценки эффективности использования контрмер в различных сценариях моделирования.

Результаты моделирования показывают, что оценки риска ИБ для целевых концептов C_{11} и C_{12} после оптимизации распределения ресурсов контрмеры уменьшились как в отношении разброса («серость»), так и в отношении центрального значения оценок («белизна») на 75%. Отметим, что возросла оценка эффективности эксплуатации контрмеры (состояние концепта X_{15}) и уменьшилась оценка стоимости эксплуатации контрмеры несмотря на то, что в целевую функцию оптимизация этих параметров заложена не была. Следовательно, предложенный подход демонстрирует эффективность в выборе наиболее эффективных вариантов средств защиты при минимальных затратах и позволяет оптимизировать распределение ресурсов системы защиты информации для минимизации рисков нарушения кибербезопасности.

Приложение Д. Моделирование атаки внешнего злоумышленника на АСУ ТП ТТН на основе традиционного подхода с использованием графовых моделей

Рассмотрим процесс моделирования атаки внешнего злоумышленника на АСУ ТП ТТН на основе традиционного подхода с использованием графовых моделей. При построении графа атак вначале выполняется анализ профиля вероятного злоумышленника, наиболее вероятных атак и наиболее уязвимых ресурсов предприятия. Исходя из экспертного анализа базовой модели архитектуры АСУ ТП ТТН и возможных последствий воздействия злоумышленника, рассмотрим ряд возможных сценариев (рисунке Д.1).

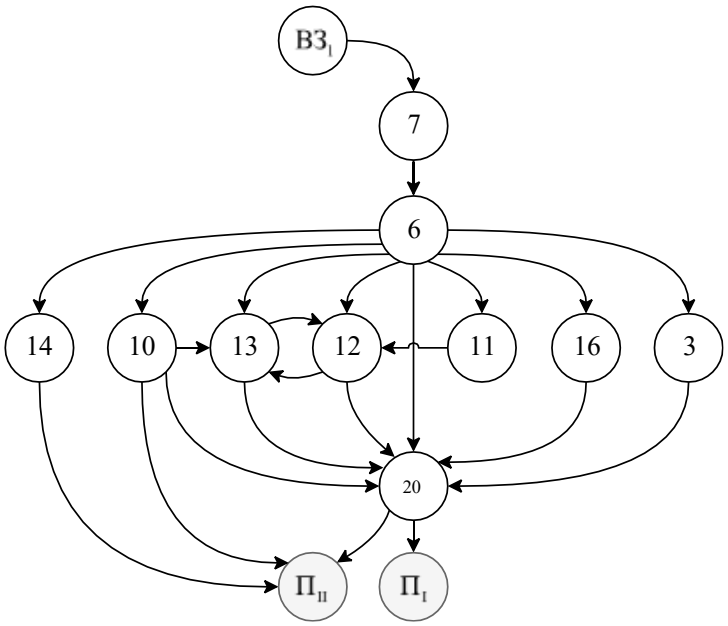


Рисунок Д.1 – Граф атак на промышленную сеть АСУ ТП

Номера узлов графа соответствуют номерам устройств на рисунке 3.25.

$ВЗ_1$ – внешний злоумышленник, реализующий атаку на компоненты АСУ ТП.

Последствия реализации атаки:

$П_I$ – отключение насоса;

$П_{II}$ – нарушение целостности исторических данных, что ведет к искажению технико-экономических показателей системы баланса материальных потоков.

Возможные последовательности действий злоумышленника (цепочки – эксплуатация последовательности уязвимостей элементов базовой архитектуры АСУ ТП – рисунок 3.25) для реализации атаки (таблицы Д.1-Д.2) построены на основе экспертного анализа БДУ ФСТЭК и иных баз угроз и уязвимостей (CAPEC, CVE, NVD, CWE).

Таблица Д.1 – Эксплуатируемые уязвимости компонент базовой архитектуры АСУ ТП ТТН

Компонент	Уязвимость
3	Уязвимость прикладного ПО управления версиями прошивок
6	Уязвимость ПО организации удаленного доступа в ЛВС
7	Уязвимость VPN-сервера
10	Уязвимость прикладного ПО сервера NTP
11	Уязвимость прикладного ПО SCADA клиента
12	Уязвимость прикладного ПО SCADA сервера
13	Уязвимость OPC-сервера
14	Уязвимость системного ПО сервера хранения исторических данных
16	Уязвимость коммутационного оборудования сети
20	Уязвимость механизмов авторизации ПЛК

Таблица Д.2 – Последовательность действий злоумышленника для реализации атаки

Цепочка перемещений по элементам базовой архитектуры системы	Результат реализации
7 → 6 → 13 → 20	Передача команды на программируемый логический контроллер (ПЛК) для отключения насоса через OPC-сервер
7 → 6 → 12 → 20	Передача команды на ПЛК для отключения насоса через SCADA сервер
7 → 6 → 16 → 20	Подмена сетевого трафика между 11 и 12, 12 и 13, 13 и 20
7 → 6 → 14	Нарушение целостности накопленных исторических данных на сервере 14 и искажение ТЭП ТП
7 → 6 → 11 → 12 → 13	Нарушение корректной визуализации данных о ходе ТП на 11 и срабатывание защитного контура / команда оператора
7 → 6 → 10	Нарушение работы сервера NTP и нарушение целостности данных в 14
7 → 6 → 10 → 13 → 12	Задержка команд и сигналов из-за нарушения работы 10
7 → 6 → 3 → 20	Изменение работы сервера обновления прошивок ПЛК и технологического оборудования
7 → 6 → 20	Использование недостатков механизмов аутентификации и авторизации ПЛК (пароль и логин по умолчанию) для изменения режима работы ПЛК и искажения передаваемых данных

Для более подробного описания шагов злоумышленника, реализующего атаку, направленную на перехват управления АСУ ТП, и автоматизации моделирования вектора атаки, воспользуемся меташаблонами атак из CAPEC. Вектор атак представляет собой последовательность действий, совокупность способов, методов и средств, при помощи которых злоумышленник достигает поставленной цели воздействия на каждом этапе проведения атаки.

Тактики из проекта Методики, описывающие пошагово действия внешнего злоумышленника, а также соответствующие этим тактикам меташаблоны атак из CAPEC, представлены в таблице Д.3.

Для анализа возможностей злоумышленника на каждом этапе реализации построим граф атак для каждого меташаблона атаки, объединяющего в себе стандартные шаблоны. Стандартные шаблоны атак ориентированы на конкретную методологию или технику, используемую для осуществления атаки. Они необходимы для представления эксплуатации конкретной техники и достижения желаемой цели. Подробный шаблон атаки обеспечивает больший уровень детализации, используя конкретную технику, нацеленную на конкретную технологию.

Таблица Д.3 – Тактики и соответствующие им меташаблоны атак

Тактики / Методика	**Меташаблоны атак / CAPEC**
1) сбор информации о системах и сетях	1) CAPEC-169: Footprinting. Включает в себя различные методы сбора информации для подготовки к атаке. Позволяет узнать о составе, конфигурации, механизмах безопасности системы и сети (рис. 3).
2) получение первоначального доступа к компонентам систем и сетей	2) CAPEC-560: Use of Known Domain Credentials. Злоумышленник угадывает или получает законные учетные данные для аутентификации и выполнения санкционированных действий под видом аутентифицированного пользователя (рис. 4).
3) закрепление в системах и сетях	
4) повышение привилегий по доступу к компонентам систем и сетей	3) CAPEC233: Privilege Escalation. Злоумышленник использует уязвимость, позволяющую ему повысить свои привилегии и выполнить действия, которые ему не разрешено выполнять (рис. 5).
5) неправомерный доступ и воздействие на информационные ресурсы или компоненты систем и сетей, приводящее к негативным последствиям	4) CAPEC-176: Configuration / Environment Manipulation. Злоумышленник манипулирует файлами и настройками, которые влияют на поведение приложения (рис. 6).

Отметим, что построенный выше граф атак на промышленную сеть (рисунок Д.1) опирается на исчерпывающие сведения специалистов информационной безопасности об анализируемой системе: архитектуре, внутренних ресурсах, их значимости и т.п. Внешний злоумышленник не обладает всей полнотой информации о системе и выполняет атаку на основе имеющихся у него сведений. Следовательно, для моделирования его возможных действий достаточно рассмотреть последовательность связанных меташаблонов, раскрывающих узлы 7 и 6 экспертного графа атак и соответствующих применению техник и тактик Методики. На основе графов атак меташаблонов конструируется вектор атак в виде цепочки вероятностных переходов между узлами графа атаки (рисунок Д.2).

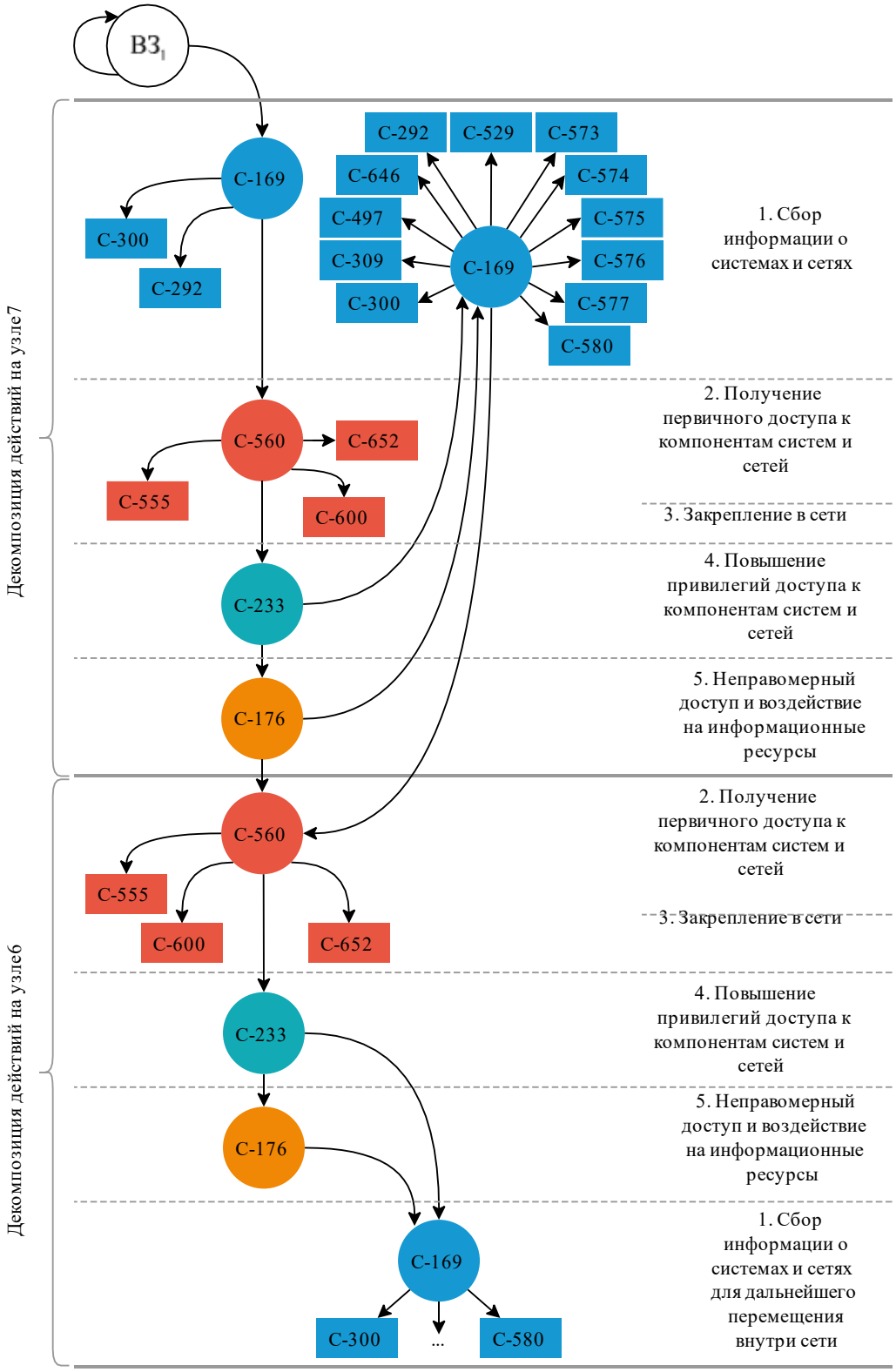


Рисунок Д.2 – Применение сценарного подхода к моделированию сложной атаки на основе шаблонов атак CAPEC для фрагмента графа атак

Для оценки вероятностей переходов можно использовать соответствующие элементу меташаблона уязвимость и уровень ее опасности (оценка CVSS [183, 184]). Если конкретная уязвимость отсутствует в системе, то переход к

соответствующему элементу графа металшаблона невозможен (весовой коэффициент, характеризующий вероятность перехода к следующей вершине, равен нулю).

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 металшаблона.

Возможны два варианта анализа графа атаки, соответствующего металшаблону:

1) граф строится поэтапно, с моделированием по матрицам потенциальных переходов между вершинами и выбором возможных переходов при наличии уязвимостей и слабостей;

2) полный граф редуцируется – отсекаются нереализуемые переходы и вершины с нулевыми связями.

Описанный подход частично реализован в инструментах анализа защищенности информационных систем, использующих симуляцию векторов атак (Cymulate), сценарии автоматической эксплуатации уязвимостей (PenTera, Core Security, Rapid 7 Metasploit [161]), аналитическое тестирование на проникновение (CyBot). В то же время, если формируемый автоматически граф атак становится достаточно большим, это затрудняет его практический анализ экспертом.

Приложение Е. Результаты эксперимента по контролю целостности наблюдаемых параметров ТП на основе технологий интеллектуального анализа данных

Для обучения НС были взяты данные о ходе ТП производства полиэтилентерефталата за год, а именно вязкость, сила тока, скорость вращения ротора и давление всасывания – $y(t), u_1(t), u_2(t), u_3(t)$.

На рисунке 5.8 изображен в графическом виде технологический временной ряд для входных параметров $u_1(t)$ – сила тока, $u_2(t)$ – скорость вращения ротора, $u_3(t)$ – давление всасывания и выходной параметр $y(t)$ – вязкость полиэтилентерефталата.

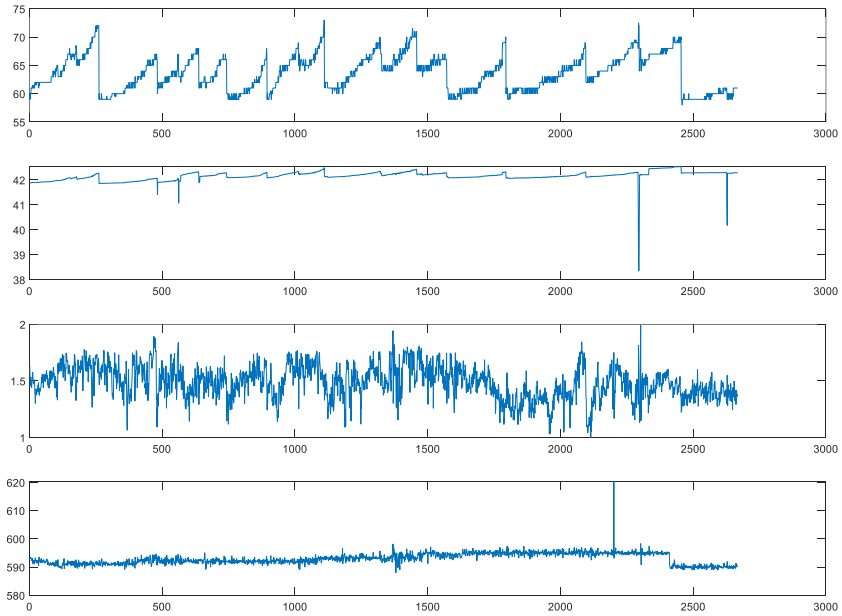


Рисунок 5.8 – ТВР входных – $u_1(t), u_2(t), u_3(t)$ и выходных характеристик ТОУ, $y(t)$

Подбор количества сегментов ТВР для каждого из параметров ТВР реализован по критерию поиска точки перегиба на графике зависимости суммарной невязки модели и натурных данных $y(t), u_1(t), u_2(t), u_3(t)$ (рисунок 5.9).

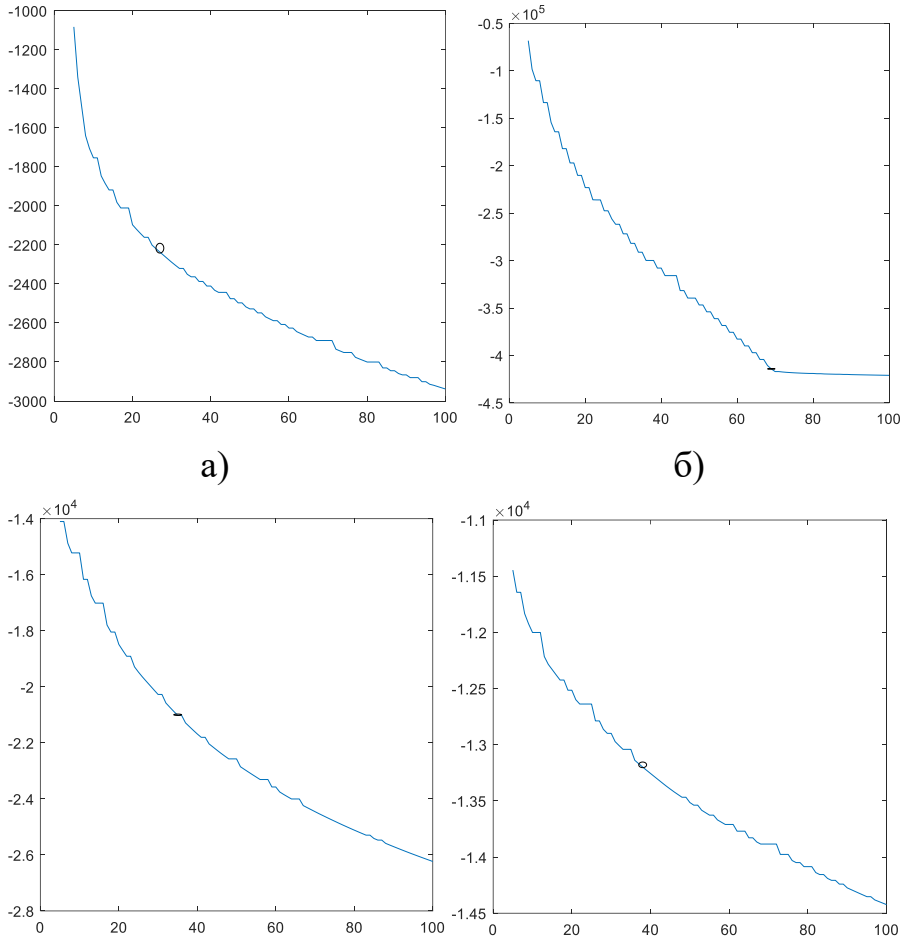


Рисунок 5.9 – Зависимость суммарной невязки модели и натурных данных y(t) от количества сегментов (ось X) по критерию поиска точки перегиба (knee of curve) (а) k = 27, б) k = 69, в) k = 35, г) k = 38)

Для проверки правильности нахождения количества сегментов с помощью модели NARX, был проведен анализ для каждого из параметров (рисунки 5.10, 5.11). По результатам сводного анализа выбирается значение количества сегментов k = 27, что совпало с результатами NARX модели.

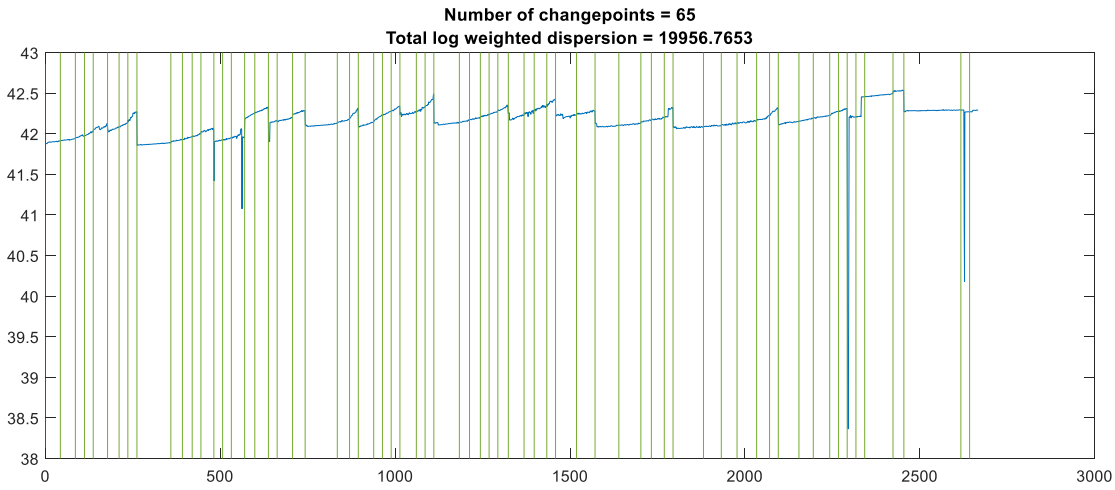
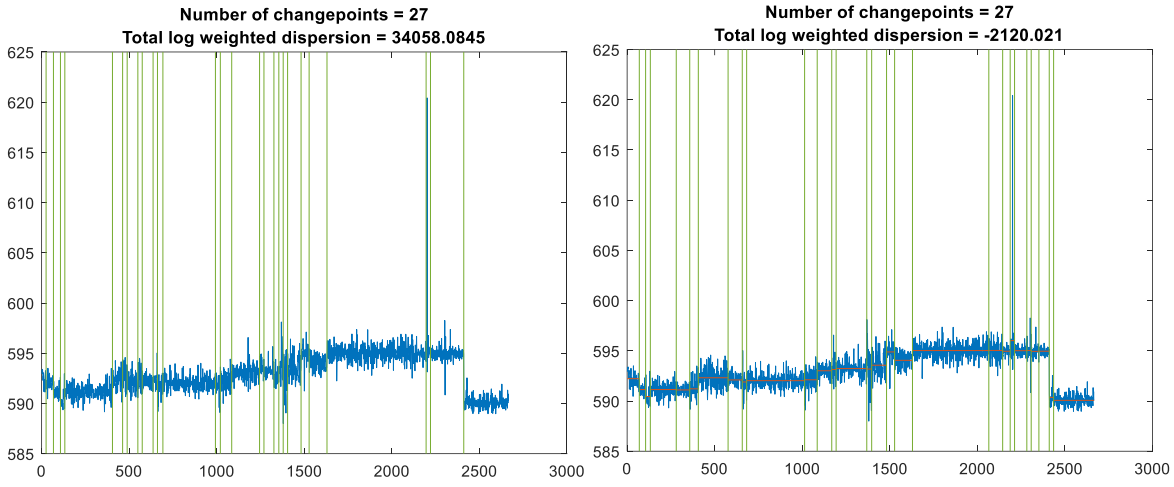
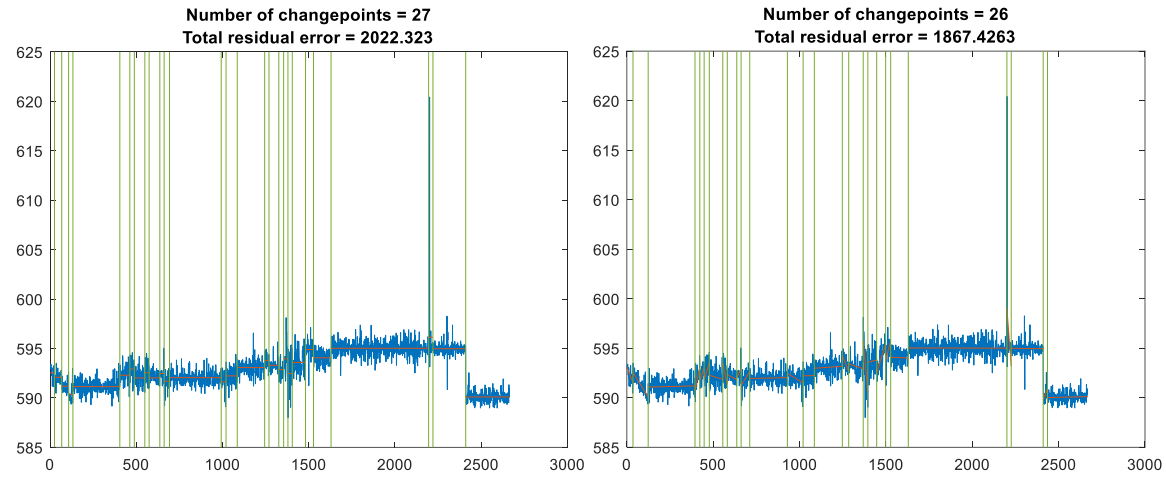


Рисунок 5.10 – Границы адаптивных сегментов по u_1(t) – RMS



а) б)



в) г)

Рисунок 5.11 – Границы адаптивных сегментов по y(t) (а) RMS; б) STD; в) MEAN; г) LINEAR)

RMS – обнаружение резких изменений среднеквадратичного значения отсчетов временного ряда в скользящем окне;

STD – обнаружение значительных изменений среднеквадратичного значения отсчетов временного ряда, рассчитанного для скользящего окна;

MEAN – обнаружение резких изменений среднего значения отсчетов временного ряда в скользящем окне;

LINEAR – обнаружение линейных изменений.

Полученные сегменты объединяем по «схожим» типам динамики с помощью реализованного алгоритма кластеризации в пакете MATLAB, а именно метода кластеризации k-means по критерию Calinski-Harabasz (см. рисунок 5.12).

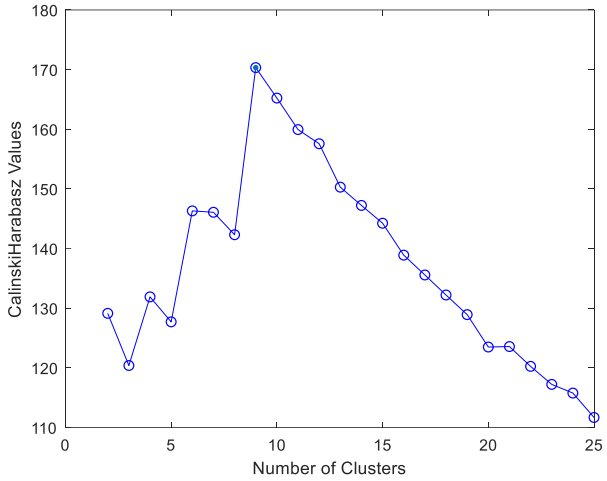


Рисунок 5.12 – Оптимальное количество кластеров для алгоритма k-means по критерию Calinski-Harabasz. По оси абсцисс – количество кластеров, по оси ординат – значение критерия качества кластеризации

Итоговое количество кластеров после объединения похожих сегментов составило 9. На рисунках 5.13 и 5.14 видна разница до кластеризации сегментов. В результате кластеризации 27 адаптивных сегментов были поделены на 9 классов динамики ТВР, что значительно упростит обучение нейронной сети для классификации события, происходящего на объекте, по типу сегмента ТВР.

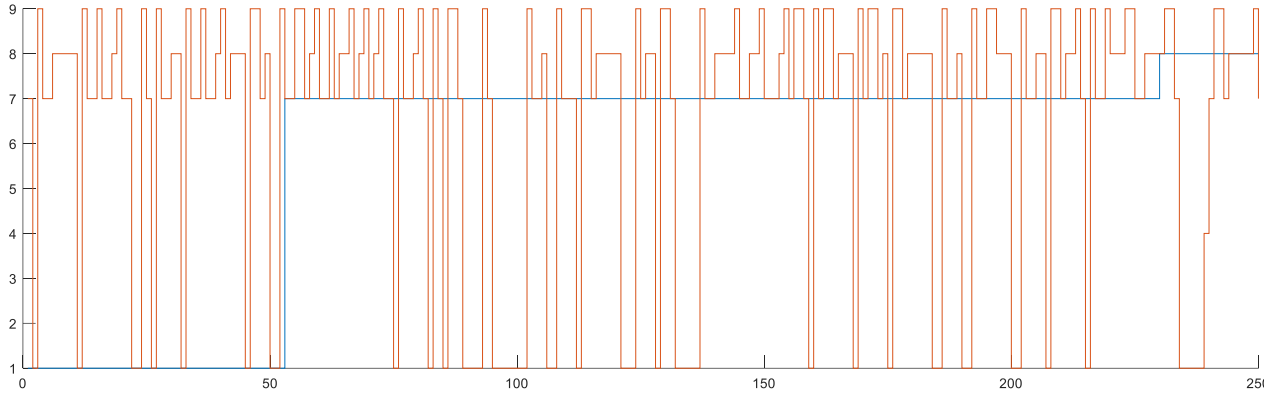


Рисунок 5.13 – Первые 250 отсчетов ТВР, отнесенные к выделенным кластерам. Оранжевая линия – без слияния соседних, синяя – с учетом значения соседей. Ось X – номер отсчета, ось Y – номер класса

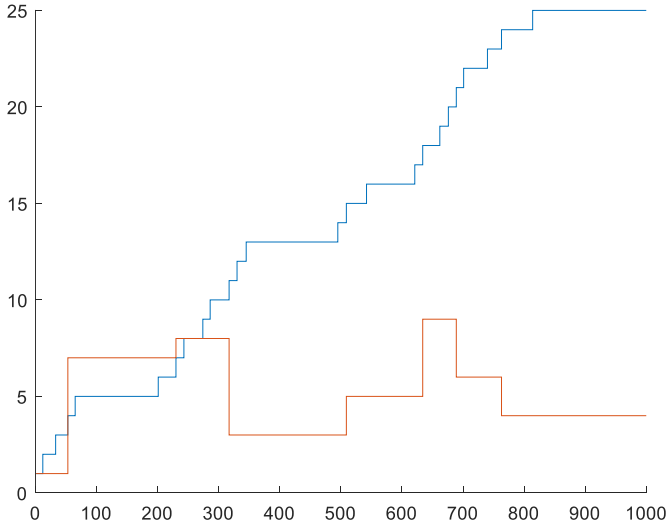


Рисунок 5.14 – Отсчеты ТВР, отнесенные к выделенным кластерам. Синяя линия – исходная нумерация кластеров (27 адаптивных сегментов), оранжевая линия – с учетом значения соседей (9 типов сегментов). Ось X – номер отсчета, ось Y – номер класса

Для реализации классификатора, который будет анализирует динамику ТП и принимать решение о типе технологического состояния ТО, была выбрана модель многослойного персептрона. Для обучения НС было взято 1330 примеров по 10 отсчетов в скользящем окне с шагом перекрытия 2 и 9 классов динамики, выборка была разбита в соотношении 75 на 25. Для скрытого слоя в ходе экспериментов подобрано количество нейронов, равное 30. Для обучения было выбрано 5000 эпох, функция активации – гиперболический тангенс. Для оценки ошибки сети использовалась среднеквадратичная ошибка. В качестве алгоритма

обучения использован алгоритм сопряженных градиентов. Целевая ошибка обучения goal = 1e-3 была достигнута за 2740 итераций.

Для обучающей выборки специфичность и чувствительность равны:

Sensitivity = 1;

Specificity = 0.9987.

Точность классификатора на обучающей выборке составила 99,79%.

Для тестовой выборки специфичность и чувствительность равны:

Sensitivity = 0.8387;

Specificity = 0.9815.

Отсюда точность классификатора на тестовой выборке составила 87,99%.

Количество ошибок отдельных классификаторов для тестовой выборки представлено на рисунке 5.15.

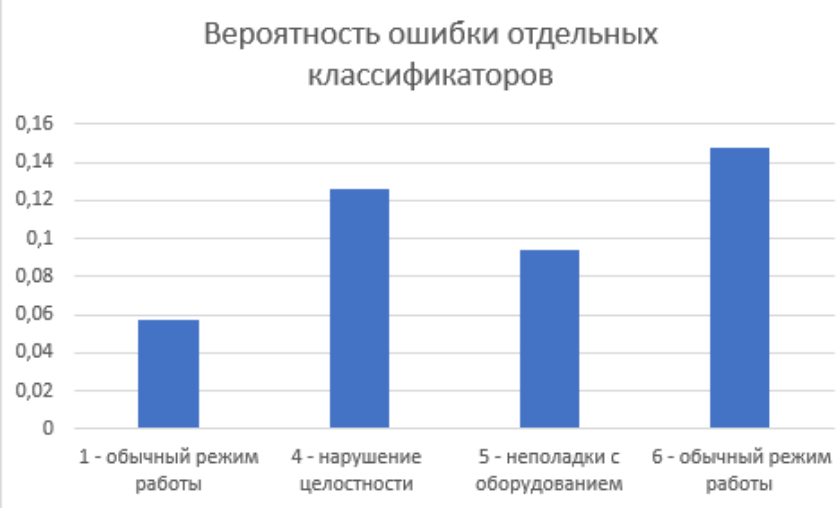


Рисунок 5.15 – Ошибки классификаторов

Таким образом, для тестовой выборки точность классификатора составила 87,99%, а вероятность ошибки отдельных классификаторов типов не превышает 14%.

Можно сделать вывод, что реализация данной системы мониторинга ТП на основе технологии искусственного интеллекта повысит степень защищённости результатов измерений от несанкционированной модификации в базах данных информационных систем промышленного предприятия.

Приложение Ж. Результаты эксперимента по оценке рисков ИБ КФО на основе прогнозирования и обнаружения аномалий их состояния

Предложенный исследователями из Южной Кореи (Institute of ETRI, Daejeon, South Korea) [168, 282] набор данных собран в ходе эксплуатации стендовой АСУ ТП и дополнен результатами программно-аппаратного моделирования (HIL) генерации энергии паровой турбиной и процесса гидроаккумулирования.

Технологические процессы на испытательном стенде (рисунок Ж.1):

- процесс котла (P1);
- процесс турбины (P2);
- процесс водоподготовки (P3);
- HIL-моделирование (P4) сценариев выработки тепловой энергии и генерации гидроаккумулирования энергии.

Процессы котла и турбины используются для моделирования тепловой электростанции, а процесс очистки воды используется для моделирования гидроаккумулирующей электростанции.

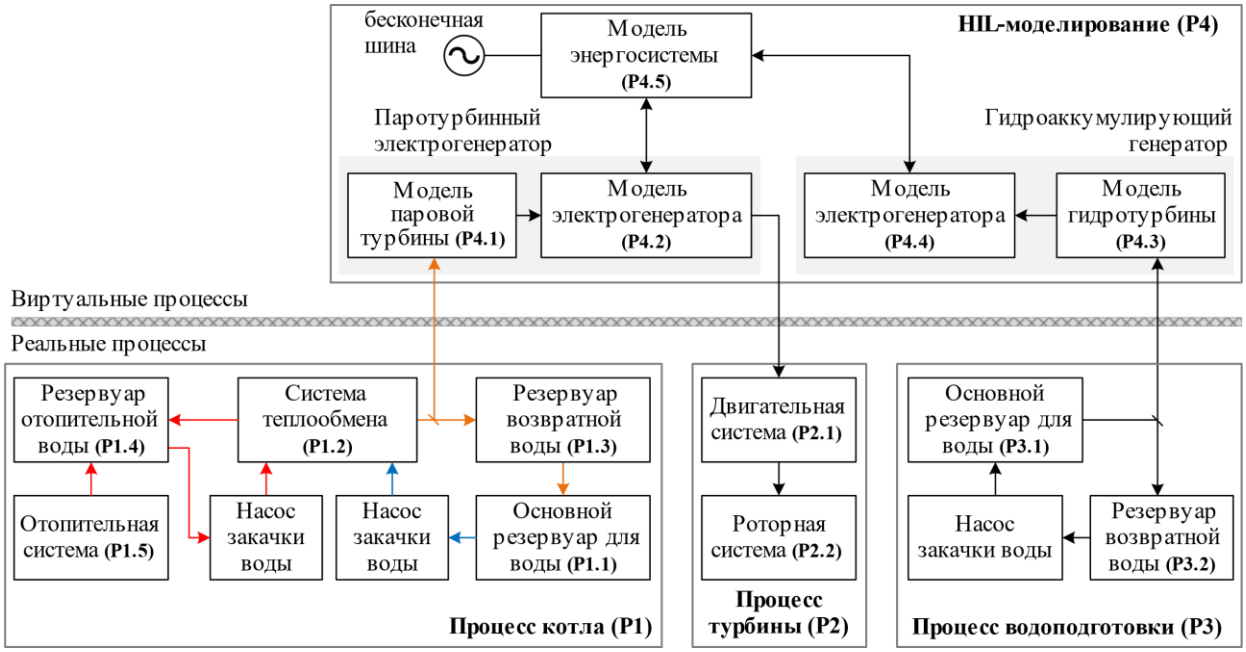


Рисунок Ж.1 – Технологическая схема анализируемого стенда

Управление нагревателем в котле контролируется системой DCS Emerson Ovation. Для управления скоростью вращения и мониторинга вибрации турбины используется контроллер DCS Mark VIe компании General Electric. Процесс водоподготовки контролируется с помощью ПЛК Siemens S7-300, который управляет уровнем воды и работой насоса. В испытательном стенде HAI

моделирование HIL проводилось с использованием системы dSPACE® SCALEXIO, сопряжённой с со стендом с помощью ПЛК S7-1500, ПЛК (Siemens) и с устройствами удаленного ввода-вывода ET200 (рисунок Ж.2).

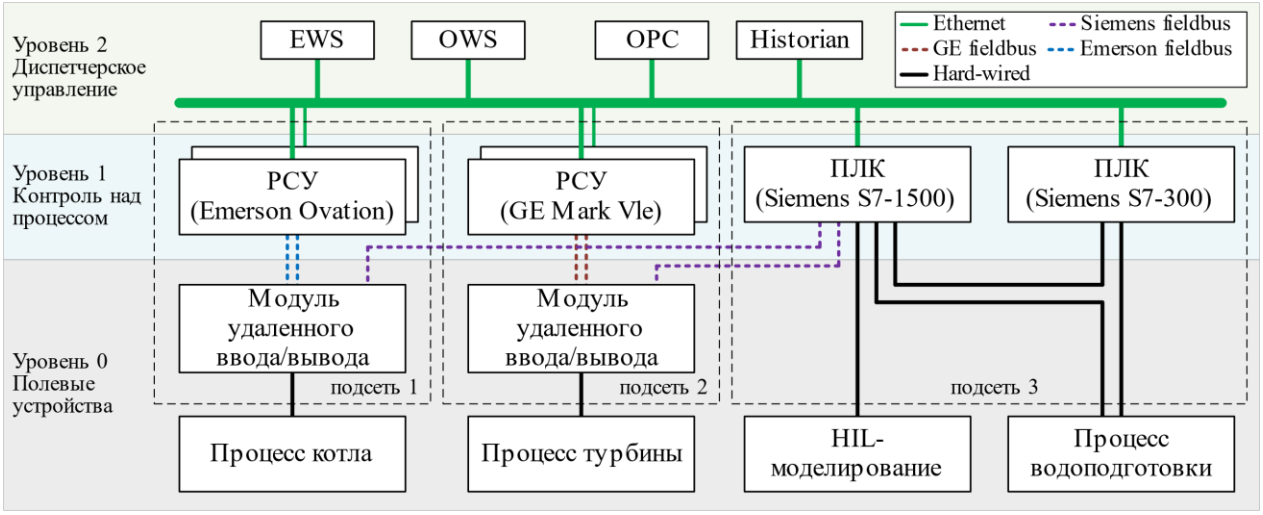


Рисунок Ж.2 – Тестируемые компоненты и поток данных управления по уровням

Сценарии работы системы задаются с помощью четырех переменных замкнутого контура управления, а именно: уставок (SPs), параметров процесса (PVs), управляющие воздействия (CVs) и параметров управления (CPs) (рисунок Ж.3).

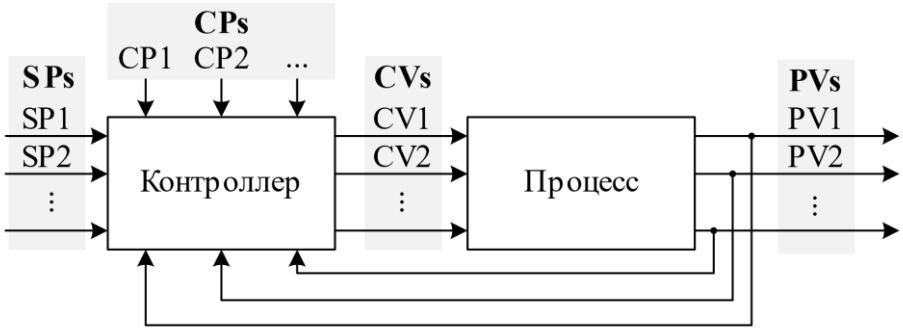


Рисунок Ж.3 – Модель контура управления

При нормальной работе системы предполагается, что оператор управляет объектом в обычном режиме через HMI и что переменные симулятора, связанные с выработкой электроэнергии в HIL-симуляторе, изменяются. Оператор отслеживает значения PV, фиксируемые датчиками и отображаемые с помощью HMI, и задает SP для контролируемых устройств.

Планировщик задач HMI используется для периодической установки SPs и переменных HIL-симулятора на случайные или предопределенные значения в пределах нормального диапазона для имитации вариантов штатного сценария.

Нормальные диапазоны значений SP определены путем экспериментального изменения значения каждого SP. Аномальное поведение возникало, когда некоторые параметры выходили за пределы нормального диапазона или находились в неожиданном состоянии вследствие атак, сбоев или отказов.

Было проведено 50 атак, включая 25 примитивов атак и 25 комбинированных атак при одновременном выполнении сразу двух примитивов атаки. Сценарии атак реализуются с учетом цели атаки, времени атаки и метода для каждого контура управления с обратной связью. Примеры примитивов атак:

- закрыть клапан контроля давления, а затем вернуться в нормальное состояние и пытаться поддержать предыдущее значение датчика;
- уменьшить значение расхода воды в баке отработанной воды (P1_B3005), а затем восстановить его (скрывая изменения в HMI);
- открыть клапан контроля уровня, а затем восстановить его в виде трапециевидного профиля и пытаться поддержать предыдущее значение датчика;
- кратковременная атака, при которой на несколько секунд открывается клапан контроля уровня и восстанавливается нормальное состояние. Повторяется несколько раз.

Описание полей набора данных. Обучающая выборка содержит 921603 примера без аномалий (атаки не проводились, нормальный режим работы системы) и 309604 примеров тестовых данных с тремя типа одиночных и комбинированных атак. Применяется нормализация количественных признаков – приведение к нулевому среднему и единичному стандартному отклонению, и выполняется преобразование категориальных переменных в количественные. Далее основной задачей является анализ взаимосвязи признаков.

Корреляционная матрица исходных временных рядов. С помощью попарной корреляции Пирсона для переменных обучающей выборки построена тепловая карта, позволяющая оценить параметры с сильной линейной зависимостью. Удаление зависимых переменных позволит существенно ускорить обучение моделей обнаружения аномалий.

Удаление признаков. Выполняется поиск и удаление константных (22 признака), квазиконстантных (с порогом вариабельности (дисперсия) за период анализа (обучающая выборка) 0,005 удаляется 6 признаков) и коррелирующих признаков (с порогом 0,9 на основе матрицы попарной корреляции Пирсона –

удаляются 23 признака) позволяет последовательно сократить количество анализируемых признаков до 28.

Генерация оконных признаков для детекторов. Скользящее окно длиной 90 отсчетов (экспертная оценка, являющаяся компромиссом для обнаружения длительных и кратковременных аномалий) с шагом 1 перемещается по каждому из ТВР 28 признаков. Для отсчетов, попавших в текущее скользящее окно анализа, рассчитываются следующие признаки:

- max – минимальное значение отсчета в окне;
- min – максимальное значение отсчета в окне;
- mean – среднее значение отсчетов в окне;
- std – среднеквадратичное отклонение отсчетов в окне.

Удаляются строки, содержащие неверные форматы данных или пропуски. Остается 1231118 записей, содержащих оконные признаки, определенные по описанной выше схеме, и элементы исходных ВР признаков – 147 признаков на каждую запись. В обучающей выборке окончательно содержится 921514 примеров, в тестовой – 309604 примеров.

Генерация оконных признаков для автоенкодера на основе LSTM. Для 28 ТВР с глубиной погружения в 32 отсчета строится с помощью скользящего окна с шагом 1 множество примеров обучающей и тестовой выборок.

Построение ансамбля детекторов аномалий. Исходный обучающий набор не содержит аномалий, вызванных действиями злоумышленника. Тестовый набор включает 6770 примеров, связанных с действиями злоумышленника (аномалии).

Объединенный набор данных содержит 1224315 примеров нормальной работы (отсчеты исходных 28 ВР и рассчитанные для каждого ВР признаки в скользящих окнах – по 5 признаков).

Детектор аномалий на основе изолирующего леса. Параметры детекторов для каждого из ТВР приведены в (таблице Ж.1 и Ж.2).

Таблица Ж.1 – Параметры модели детектора аномалий на основе изолирующего леса (IsolationForest, IFO) и на основе модели оценки локального уровня выброса (LocalOutlierFactor, LOF)

Параметр	Значение
Количество базовых оценок в ансамбле	128
Доля выбросов в наборе данных (используется при подгонке для определения порога оценки образцов) (contamination)	auto
Параметр	Значение

Параметр	Значение
Количество соседей, используемых по умолчанию для запросов	16

Построение детектора аномалий на основе автоенкодера. Параметры детектора на основе нейросетевого автоенкодера приведены в таблице Ж.3. Процесс обучения нейронной сети показан на рисунок Ж.1.

Таблица Ж.2 – Архитектура многомерного нейросетевого автоенкодера LSTM

Слой	Функция активации	Размеры слоя	Регуляризация
Input	–	32, 28	–
LSTM (L1)	relu	32, 128	L2
LSTM (L2)	relu	64	–
RepeatVector (L3)	–	32, 64	–
LSTM (L4)	relu	32, 64	–
LSTM (L5)	relu	32, 128	–
Output	–	32, 28	–

Начальное обучение сети выполняется за 25 эпох, обучающая выборка делится на пакеты (батчи) размером 512 примеров.

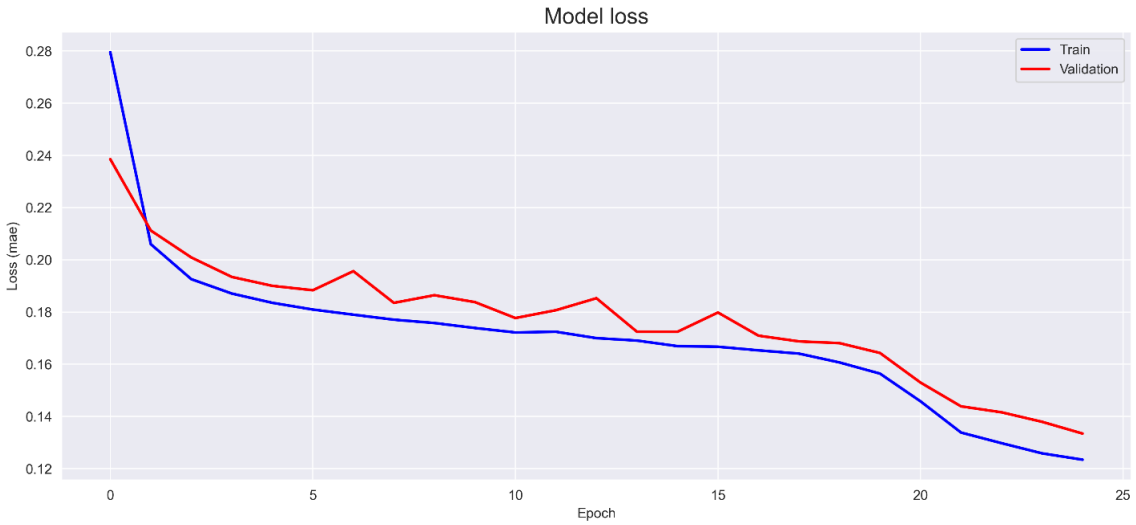


Рисунок Ж.4 – Процесс начального обучения автоенкодера LSTM; по оси абсцисс – эпохи обучения, по оси ординат средняя абсолютная ошибка

Абсолютная ошибка (*MAE*) раскрывает ошибку восстановления образа с помощью автоенкодера по отношению к среднему значению расстояния между прогнозируемым моделью значением $f(x)$ и истинным значением y:

$$MAE = \frac{\sum_{i=1}^{n} \left| f(x_i) - y_i \right|}{n}.$$

Ошибка восстановления образа (Loss_mae) к концу начального обучения продолжает уменьшаться. Дообучение происходит 25 эпох, набор данных делится на пакеты (батчи) размером 2048. Итоговая гистограмма распределения

ошибок восстановления образов с помощью автоенкодера приведена на рисунке Ж.5.

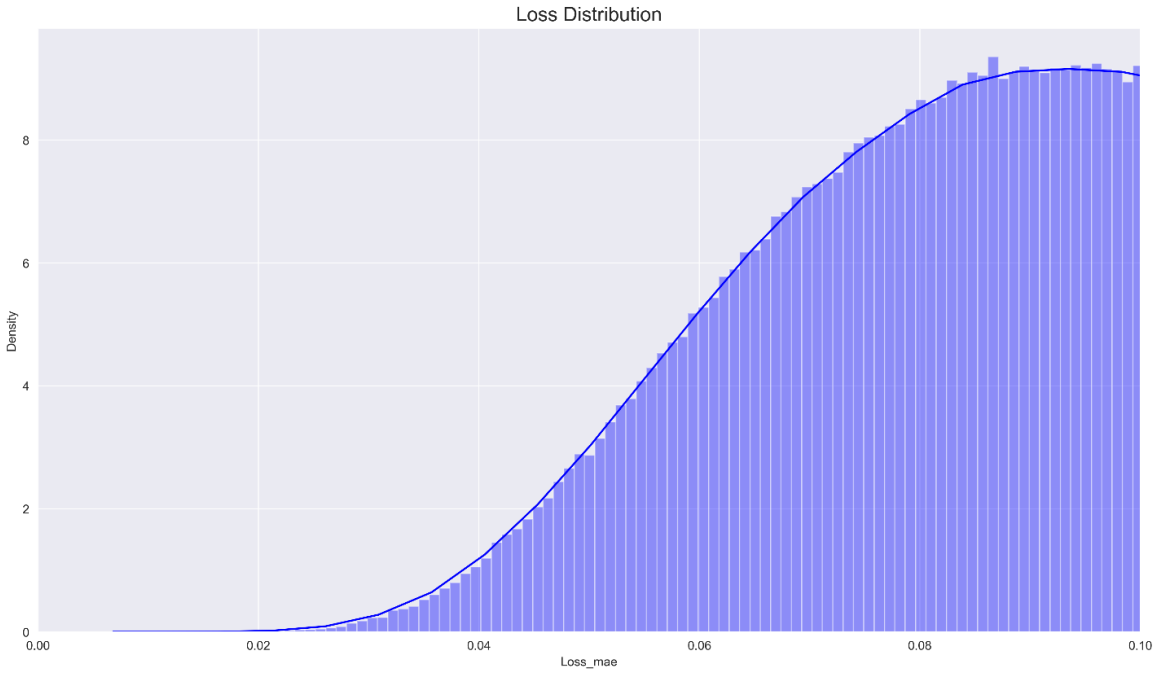


Рисунок Ж.5 – Гистограмма распределения ошибок восстановления образа с помощью автоенкодера

Анализ результатов и оценка эффективности предложенного решения

Результаты разметки отсчетов ВР, попадающих в скользящие окна анализа для полного набора данных, включающего обучающую и тестовую выборки, приведены на рисунке Ж.6. Указана доля отсчетов, отнесенных к аномалиям, по отношению к общему числу отсчетов, определенная каждым детектором по каждой переменной.

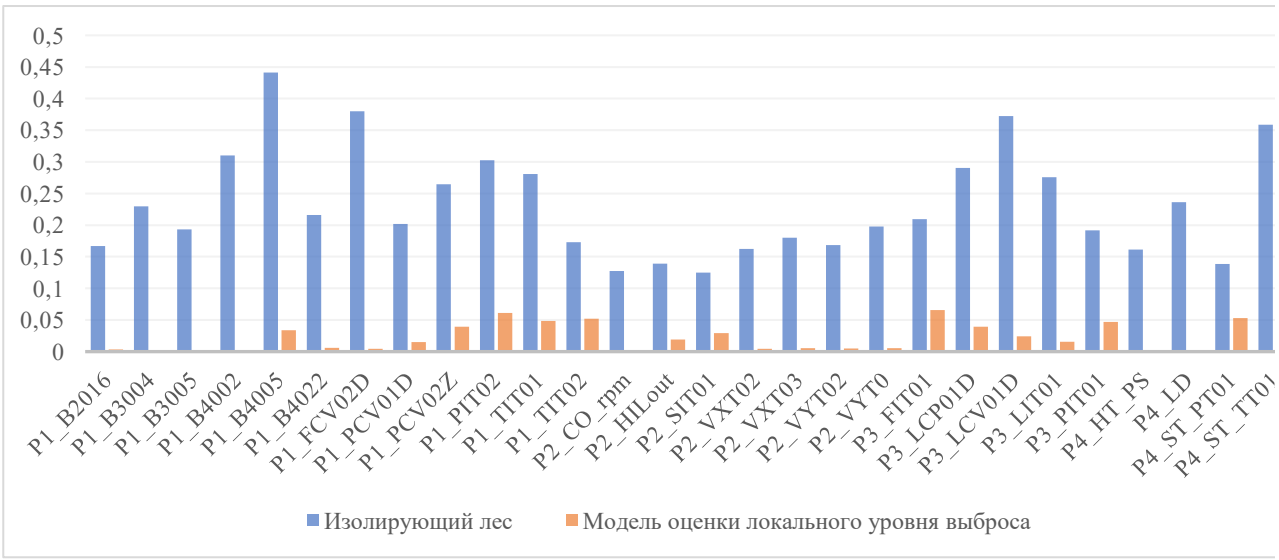


Рисунок Ж.6 – Результаты разметки отсчетов детекторами на основе изолирующего леса и модели оценки локального уровня выброса: доля примеров (ось ординат), отнесенных к аномальным, по каждому параметру (ось абсцисс)

Из рисунка Ж.6 видно, что детекторы на основе изолирующего леса значительно чаще относят примеры данных к аномальным, напротив, избирательность детекторов на основе LOF существенно лучше. Распределение суммарных оценок детекторов на основе изолирующего леса приведено на рисунке Ж.7.

Рисунок Ж.7 – Распределение суммарных оценок детекторов на основе изолирующего леса при оценке одномерных ТВР (ось абсцисс – суммарная оценка детекторов о принадлежности образца к классу аномалий «-1» или классу нормальной работы «1»; ось ординат – количество образцов)

Ключевым этапом является подбор порога чувствительности ансамбля детекторов. Определим порог для оценки принадлежности окна анализа к аномальному. Подбор оптимального значения порога для минимизации пропусков аномалий реализуем как поиск порога чувствительности и специфичности модели в диапазоне от $\Theta \in [10;29]$ с шагом 0,1. Исходный диапазон поиска определяется из рисунка 15 как отсечка, показывающая степень согласованности детекторов по каждому ВР при отнесении текущего образца к нормальному или аномальному режиму работы.

Зависимость метрик качества детектора от установленного порога показана на рисунок Ж.8. Анализ чувствительности и F1-меры, взвешенных количеством примеров в каждом из классов оценок, позволяет выбрать приемлемое значение порога фильтрации аномалий и уменьшить количество ложных срабатываний.

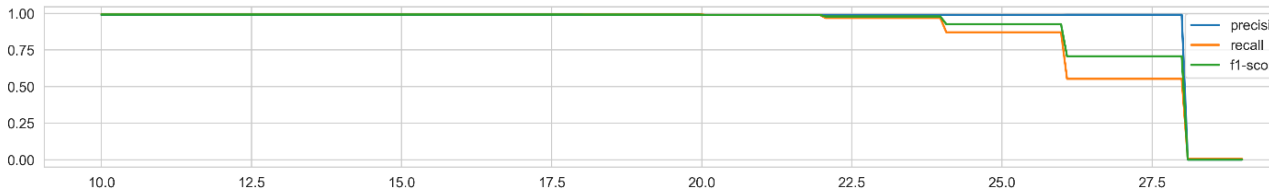


Рисунок Ж.8 – Зависимость метрик качества (взвешенные оценки) детектора от установленного порога (ось абсцисс)

Далее проанализируем гистограмму распределения ошибок восстановления образа с помощью автоенкодера (Глава 2). Из рисунка видно, что значение порога обнаружения аномалий может быть задано как значение в интервале (0,1-0,3). Подбор порога для оптимизации количества выявленных аномалий с помощью автоенкодера реализуем перебором по сетке: стартовое значение составляет 0,1, конечное – 0,35, шаг подбора – 0,05. Взвешенное значение метрик качества детектора на основе автоенкодера от установленного порога (рисунок Ж.5).

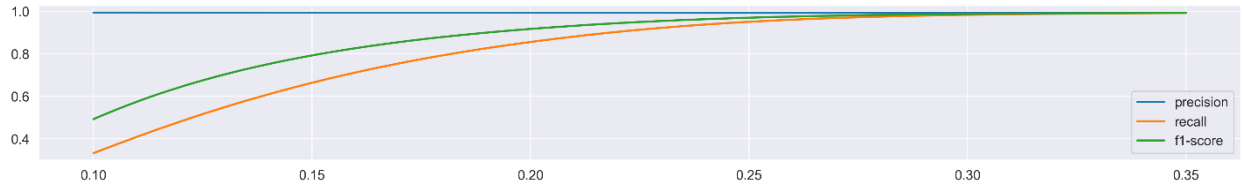


Рисунок Ж.9 – Взвешенное значение метрик качества детектора на основе автоенкодера от установленного порога (ось абсцисс)

Подобранное значение порога составляет 0,21. С установленным порогом качественно оценим распознавание аномалий каждого типа.

Стоит отметить, достаточно большое количество ложно положительных срабатываний ансамбля детекторов, для снижения которого необходимы дополнительные фильтры срабатываний на основе оценки временных аспектов реализации атак: минимальной длительности, потенциальной периодичности, минимального интервала времени между реализацией разных типов атак.

Сводная оценка качества работы детектора по обнаружению аномалий приведена в таблице Ж.3. Итоговая оценка TaPR для композиции детекторов: TaR = 0,993, TaP = 0,915.

Таблица Ж.3 – Сводная таблица оценки качества работы детектора по обнаружению аномалий без постфильтрации

	Все атаки		Первая атака		Вторая атака		Третья атака	
	F1-мера	количество	F1-мера	количество	F1-мера	количество	F1-мера	количество
Нормальная работа	0,97	1224315	0,97	1225819	0,97	1229746	0,97	1230487

	Все атаки		Первая атака		Вторая атака		Третья атака	
Аномалия, вызванная атакой	0,13	6770	0,10	5266	0,03	1339	0,02	598
Доля правильных классификаций (Accuracy)	0,95	1231085	0,95	1231085	0,95	1231085	0,95	1231085
Accuracy weighted avg (взвешенная количеством примеров доля правильных классификаций)	0,97	1231085	0,97	1231085	0,97	1231085	0,97	1231085
FP	58365		59395		61721		62288	
FN	2364		1890		289		115	
F_beta(0,5)	0,9835		0,9847		0,9882		0,9888	

В работе [248] рассмотрен подход к обнаружению аномалий на основе решения задачи классификации состояний объекта с помощью методов машинного обучения. Этапы предобработки, анализа значимости и отбора признаков завершаются построением классификаторов: k ближайших соседей, комитета деревьев решений, и решающего дерева. Особенностью является объединение обучающей (примеры нормального функционирования объекта, не содержащие атак) и тестовой выборок (смесь нормальной работы и примеров, характеризующих реализованные атаки) с последующим исправлением дисбаланса количества примеров в классах нормальной и аномальной работы с помощью алгоритма увеличения числа примеров миноритарного класса (класс аномалий) SMOTE (Synthetic Minority Oversampling Technique). Далее аугментированная выборка разбивается на обучающую и тестовую в соотношении 70% и 30%. Итоговые характеристики качества классификации достигают оценки F1-меры на уровне 0,9976.

К недостаткам рассмотренного подхода стоит отнести следующее:

1) использование моделей, обучаемых с учителем, требует размеченного набора данных и первоначального объединения обучающей и тестовой выборок, предложенных разработчиками набора данных, – обучающая выборка в первоначальном варианте включает только данные, характеризующие нормальный режим работы объекта;
2) не в полной мере учитывается временная упорядоченность отсчетов данных о состоянии объекта – выполнена классификация изолированных временных отсчетов;

3) построенные модели позволяют с очень высокой точностью характеризовать отдельные последовательности отсчетов, без учета начала и завершения временного интервала, в течение которого реализуется атака злоумышленника, приводящая к изменениям параметров функционирования объекта. Т.е., невозможно оценить метрику TaP (насколько точно обнаруживается каждая аномалия).

В работе [267] также предложен подход, основанный на применении моделей, обучаемых с учителем:

- машина опорных векторов;
- комитет решающих деревьев;
- решающее дерево;
- классификатор k ближайших соседей;
- ансамбль стохастического градиентного бустинга (light gradient boosting machine, LightGBM).

На этапе конструирования новых признаков использован подход на основе вычисления статистических характеристик (среднее значение параметра, разброс, минимальное и максимальное значения) в скользящем окне анализа переменной длины. Существенным преимуществом предлагаемого решения при построении моделей классификации является принятие временной упорядоченности отсчетов параметров, характеризующих состояние объекта, и анализ влияния длины скользящего окна на итоговое качество классификации. Дальнейшая процедура перекрестной проверки также реализована для временных рядов параметров.

Характеристики качества классификации F1-меры находятся на уровне 0,9987. К сожалению, невозможно оценить метрику TaP (насколько точно обнаруживается каждая аномалия).

Однако, при построении моделей, обучаемых с учителем, необходима разметка примеров, поэтому авторы вновь объединяют исходные обучающую и тестовую выборки с последующим новым разбиением, что приводит к так называемой проблеме утечки данных [275].

В работе [157] предложено построение модели детектора аномалий на основе стекирования двунаправленных рекуррентных нейронных сетей (bidirectional Gated Recurrent Unit (GRU)), позволяющих учитывать временную природу анализируемых данных и частично решающих проблемы длительного и ресурсоемкого обучения нейронных сетей LSTM. Применение алгоритма

автоматического подбора порога чувствительности на основе эвристик позволяет повысить качество итогового обнаружения аномалий. Полученная оценка взвешенной меры F1 составляет для тестовой выборки 0,977 (исходная выборка, предложенная создателями набора данных), рассчитаны значения метрик TaP = 0,968 и TaR = 0,805. Однако, для тестовой выборки сделаны предположения, что отдельные реализации одной атаки и вызванные ими аномалии в параметрах состояния объекта разделены временным интервалом не менее чем в 500 секунд. Атаки разных классов разделены интервалом более 2000 секунд. Предложенные допущения на порядок снижают количество ложно положительных срабатываний детектора.

Анализ таблицы Ж5.3 показывает, что количество ложноположительных срабатываний детектора существенно превышает общее количество примеров, связанных с реализацией атаки. Приняв во внимание дополнительные временные ограничения по возможности реализации злоумышленником атаки, предложенные в работе [157], добавим временной фильтр, позволяющий существенно снизить количество ложных срабатываний, лишь незначительно уменьшив количество корректно распознанных аномалий. Примем, что атаки разделены временным интервалом $t_1 = 350$ с, класс атаки меняется с интервалом не менее $t_2 = 1500$ с (таблица Ж.4).

Таблица Ж.4 – Сводная таблица оценки качества работы детектора по обнаружению аномалий с применением постфильтрации ложноположительных срабатываний

Постфильтрация	Показатель		Все атаки		Первая атака		Вторая атака		Третья атака	
Нет	TP	FP	1165950	58365	1166424	59395	1168025	61721	1168199	62288
	FN	TN	2364	4406	1890	3376	289	1050	115	483
	F1-мера (по классам)		0,975	0,127	0,974	0,099	0,974	0,033	0,974	0,015
Есть	TP	FP	1220425	3890	1222329	3490	1226867	2879	1225941	4546
	FN	TN	2399	4371	2007	3259	358	981	128	470
	F1-мера (по классам)		0,997	0,582	0,998	0,542	0,998	0,377	0,998	0,167

Количество ложноположительных срабатываний детектора удается снизить в 10-15 раз. Стоит отметить, что значительная доля атак каждого класса обнаруживается детектором достаточно уверенно, количество ложноотрицательных случаев (пропусков атак) для 2 и 3 типа атак находится на приемлемом

уровне. Практическое применение подобной системы возможно в составе комплекса средств защиты промышленной сети, выступающих в качестве источников событий безопасности для системы сбора и корреляции событий информационной безопасности. Дальнейший анализ больших массивов гетерогенных данных о событиях безопасности и обнаружения инцидентов и угроз безопасности является основной, наиболее ресурсоемкой операцией, которая выявляет причинно-следственные связи между поступающими на обработку событиями. Операция корреляции позволяет выявлять вредоносную и аномальную активности, определять источник и цель атаки на основе анализа комплекса показателей, но не единичных инструментов и детекторов, и отсеивать значительное количество ложноположительных срабатываний за счет сопоставления признаков атаки из разных источников.

Приложение З Применение алгоритмов анализа сетевого трафика в задаче обнаружения сетевых атак в промышленных сетях

Предобработка и извлечение признаков. На этапе предобработки удаляются идентичные признаки, заполняются или удаляются признаки, содержащие нечисловые значения «NaN» и «Infinity». Значения категориальных признаков («Flow ID», «Source IP», «Destination IP» и «Timestamp») преобразуются в численные значения с помощью соответствующей схемы порядкового или унитарного кодирования (Label Encoder или One-Hot-Encoder).

Далее выполняется нормализация признаков с приведением к нулевому среднему и единичному стандартному отклонению.

Поскольку наборы данных не сбалансированы, применяются следующие схемы:

– удаление классов с очень малым количеством примеров (например, «Heartbleed», «Web Attack – Sql Injection», «Infiltration», «Web Attack – XSS» и «Bot» для набора CICIDS2017);

– аугментация имеющейся выборки на основе алгоритмов увеличение числа примеров миноритарного класса (алгоритмы SMOTE) или удаление примеров мажоритарного класса.

Оценка возможности понижения размерности пространства признаков. Оценка суммарной объяснимой дисперсии данных в зависимости от количества главных компонент для набора данных CICIDS2017 представлена на рисунке З.1.

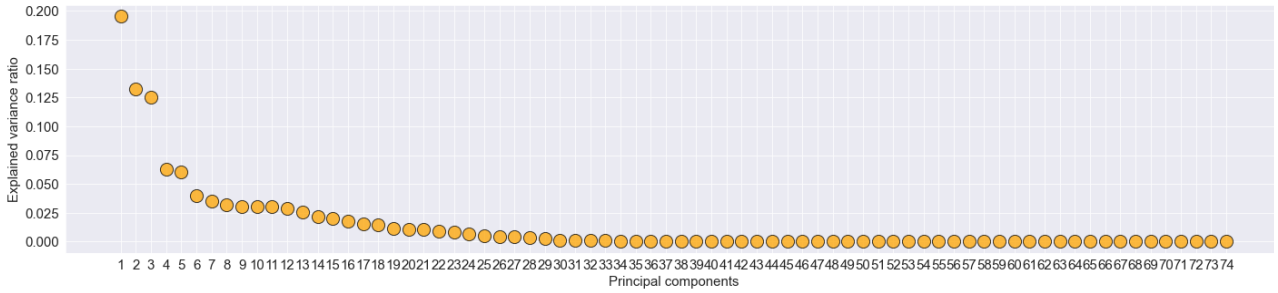


Рисунок З.1 – Зависимость суммарной объяснимой дисперсии (ось ординат) от количества главных компонент (ось абсцисс)

Ощутимое влияние на долю объясняемого коэффициента дисперсии оказывают первые 20 главных компонент. Дальнейшая процедура отбора признаков позволит существенно сократить их общее количество, поэтому применение процедуры понижения размерности пространства признаков не является необходимым. Для набора данных WSN-DS-2016 лучший результат удалось достичь,

применив нейросетевой автоенкодер с четырехслойной архитектурой, осуществляющий нелинейное сжатие пространства признаков. Для набора данных NSL-KDD количество выделенных главных компонент варьировалось в пределах от 4 до 24.

Отбор признаков. Ярко выраженные сигнатурные признаки, согласно [54], удаляются: «Flow ID», «Source IP», «Source Port», «Destination IP», «Destination Port», «Protocol» и «Timestamp». Это позволит строить модели ML, которые ориентированы на обнаружение статистических особенностей сетевых сессий, соотнесенных с сетевыми атаками, а не с сигнатурными параметрами, которые могут быть изменены или подделаны злоумышленником, и с которыми хорошо справляются традиционные системы обнаружения сетевых атак.

Далее применяются алгоритмы отбора и оценки значимости признаков. Набор данных разделяется на обучающую и тестовую выборку в соотношении 0,7 и 0,3. На обучающей выборке с помощью алгоритма перекрестной проверки с разбиением на 10 групп строится классификатор на основе дерева решений с последующей оценкой значимости признаков. Пример ранжирования признаков по степени значимости для принятия решения о принадлежности к заданному классу для набора данных CICIDS2017 приведен на рисунке 3.2.

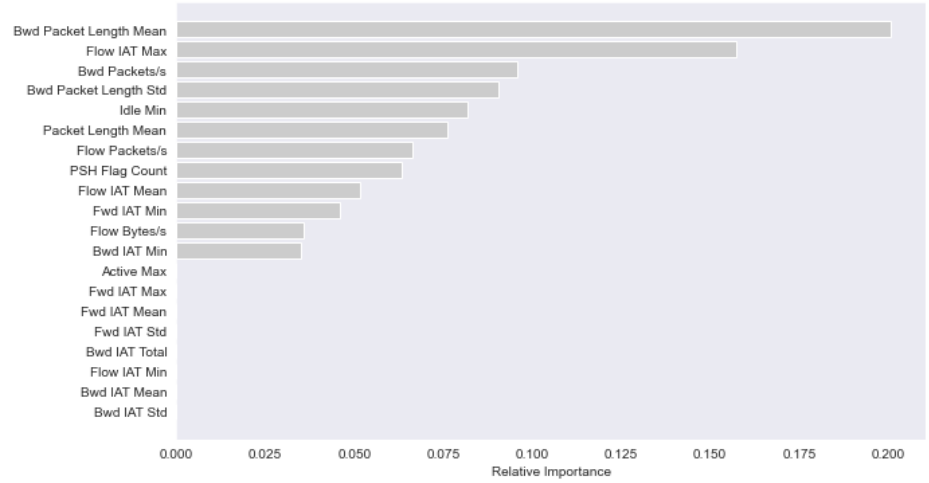


Рисунок 3.2 – Гистограмма оценки значимости признаков (ось ординат – признаки), полученная с помощью классификатора на основе дерева решений (ось абсцисс – относительные единицы)

Оценка значимости признаков выполняется также при помощи комитета (k = 250) случайных деревьев решений (RF) с использованием процедуры перекрестной проверки. Гистограмма оценки значимости выделенных с помощью RF признаков представлена на рисунке 3.3.

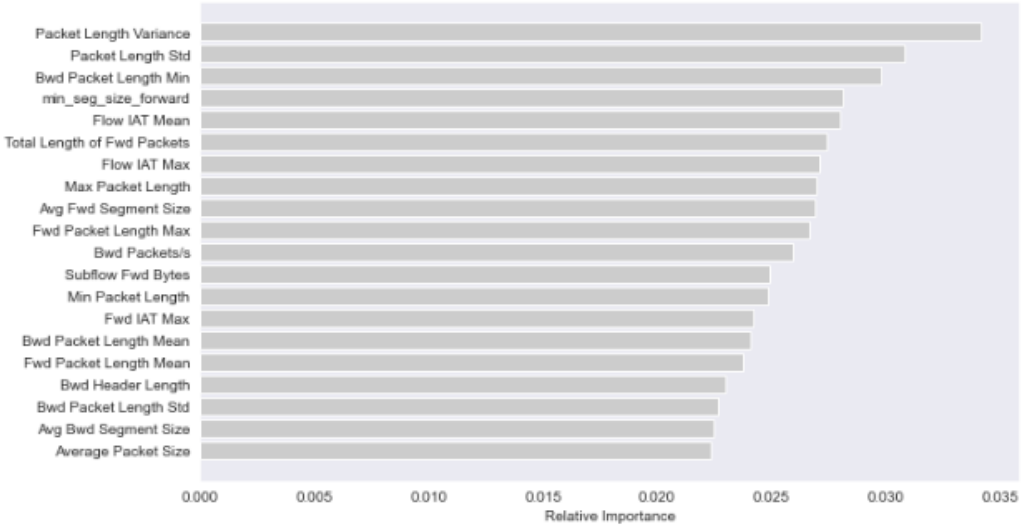


Рисунок 3.3 – Гистограмма оценки значимости признаков (ось ординат – признаки), полученная с помощью классификатора на основе комитета деревьев решений (ось абсцисс – относительные единицы)

Для набора данных WUSTL-IIOT-2018 оценка значимости признаков по аналогичному сценарию позволяет выдвинуть гипотезу о возможности оставить 1 или 2 наиболее значимых признака для построения классификатора (рисунок 3.4).

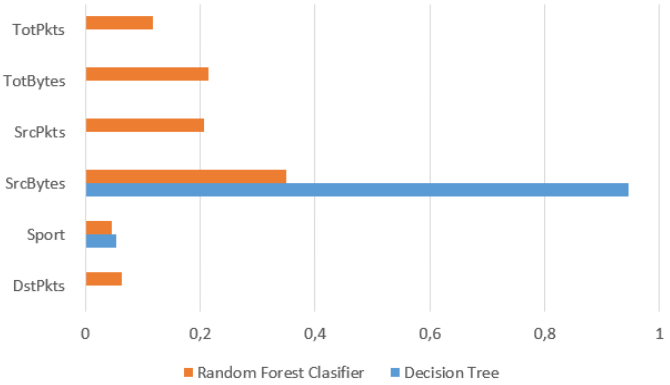


Рисунок 3.4 – Оценка значимости признаков с помощью классификатора на основе дерева решений и классификатора на основе комитета случайных деревьев (ось абсцисс – относительные единицы)

Используемые методы отбора признаков позволяют сократить их количество в 4-5 раз.

Выполняется поиск и удаление константных и квазиконстантных (с порогом вариабельности (дисперсия) за период анализа (обучающая выборка) 0,005). Далее производится оценка степени попарной корреляции признаков и удаление признаков с коэффициентом корреляции более установленного порога (например, для набора данных CICIDS2017 порог выбран равным 0,8). Итоговая

тепловая карта матрицы попарной корреляции приведена на рисунке 3.5. Полученные результаты согласуются с [54].

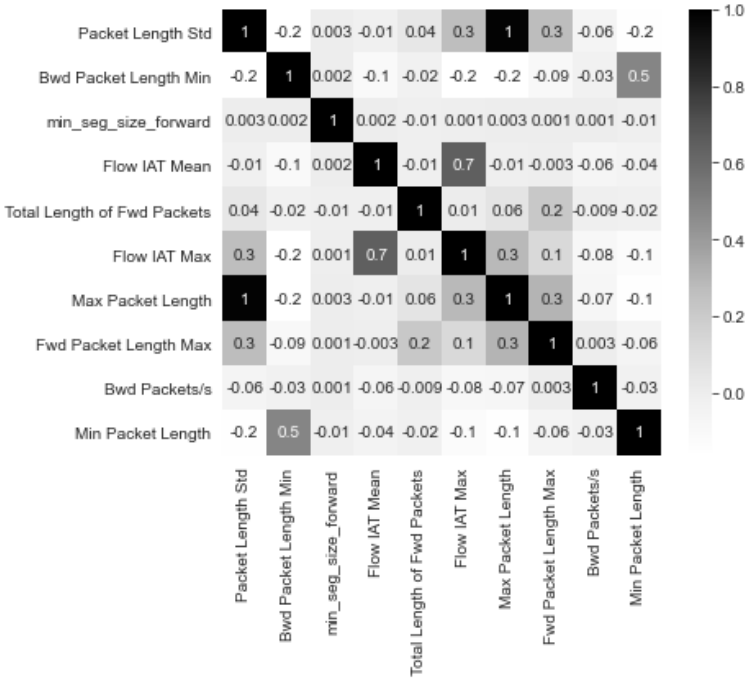


Рисунок 3.5 – Матрица попарной корреляции после исключения связанных признаков CICIDS2017 (коэффициент корреляции в диапазоне [-1, 1])

Для понижения размерности пространства признаков CICIDS2017 и визуализации распределения примеров по классам применен метод стохастического вложения соседей с *t*-распределением для понижения размерности пространства признаков и визуализации распределения примеров по классам (рисунок 3.6). Визуализация классов атак и нормальной работы набора данных WUSTL-IIOT-2018, напротив, позволяет сделать однозначный вывод о наличии структуры данных с сокращенным набором признаков и возможности дальнейшего построения классификатора (рисунок 3.7).

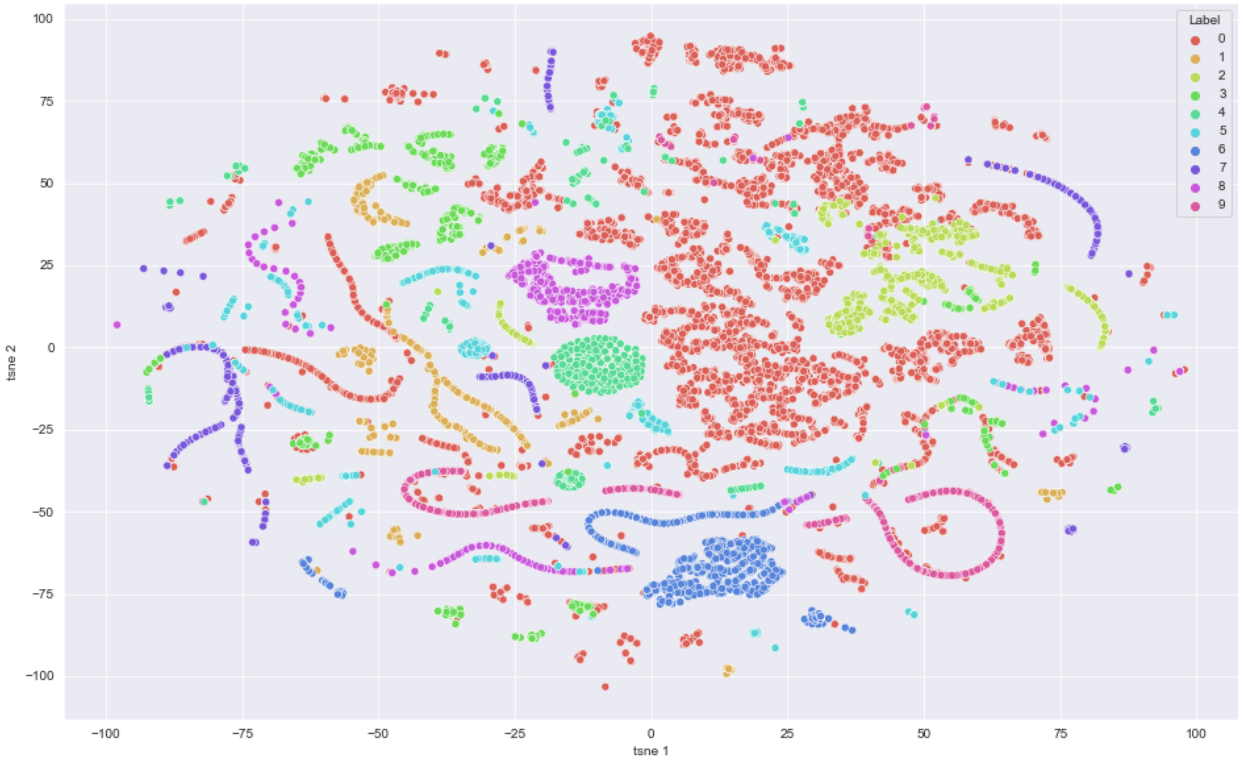


Рисунок 3.6 – Визуализация распределения примеров по классам *t*-распределением (по осям – компоненты t-SNE разложения в диапазоне [-100, 100], 0-9 – метки классов)

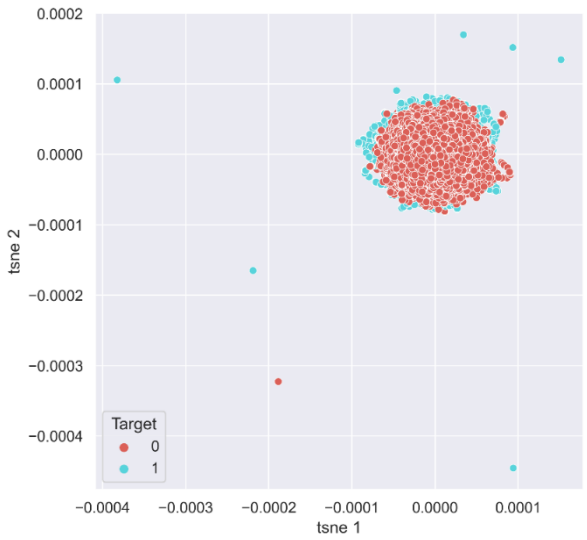


Рисунок 3.7 – Визуализация пространства признаков с помощью стохастического вложения соседей с t-распределением: 0 – «нормальная работа», 1 – «атака» (по осям – компоненты t-SNE разложения в диапазоне [-100, 100])

Построение классификаторов и ансамблей. Для решения задачи обнаружения сетевых атак на основе формализованного вектора признаков необходимо создание и подбор параметров моделей машинного обучения. Применена процедура оптимизации гиперпараметров каждой модели с применением поиска по

сетке, перекрестной проверкой с 10 проходами и оценкой качества модели на выделяемой тестовой выборке.

Применяемые классификаторы [226]:

– на основе алгоритма градиентного бустинга для ансамбля деревьев решений (XGBClassifier);

– на основе комитета деревьев решений (Random Forest, RF);

– на основе k-ближайших соседей (K-Nearest Neighbors, KNN);

– на основе машины опорных векторов (Support Vector Machines, SVM);

– на основе логистической регрессии (Logistic Regression, LR);

– на основе «мелкой» нейронной сети прямого распространения – многослойный персептрон (shallow MLP);

– на основе сверточных нейронных сетей с одномерным и двумерным входным слоем (CNN1D и CNN2D соответственно);

– на основе глубокой нейронной сети (DNN).

Для классификатора на основе сверточной нейронной сети с двумерным входным слоем признаков CNN2D вектора признаков образцов набора преобразованы в графические примитивы размерностью 5x2 (CICIDS2017) в градациях серого (рисунок 3.8).

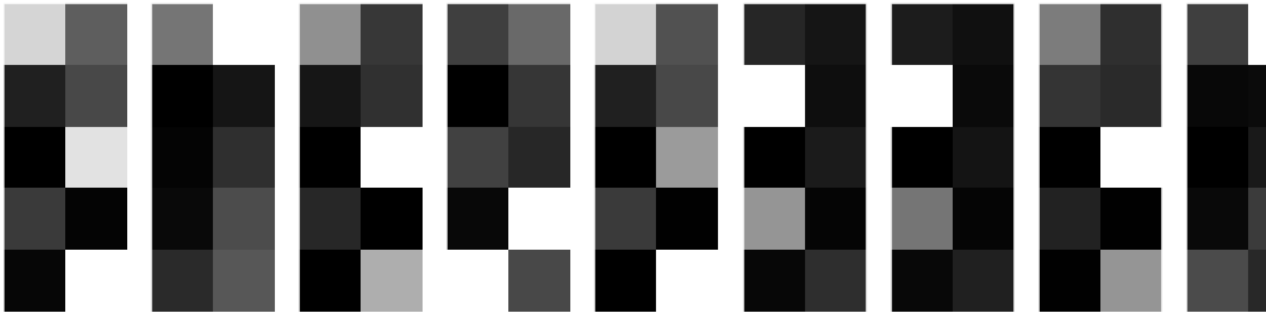


Рисунок 3.8 – Двумерное представление признаков примеров набора данных

На заключительном этапе строится ансамбль классификаторов, включающий в себя комитет деревьев решений (RF), классификатор на основе алгоритма градиентного бустинга на ансамбле деревьев решений (XGBClassifier) и ExtraTreesClassifier. Последний реализует метаоценку, соответствующую набору рандомизированных деревьев решений, или деревьев на различных подвыборках набора данных, использует усреднение для повышения точности прогнозирования и контроля избыточной подгонки отдельных моделей. Параметры комитета: тип голосования – «soft» (голосование и взвешивание предсказаний моделей для каждого класса); веса моделей распределены как {2, 1, 3}.

Использование беспроводных сенсорных сетей (WSN, Wireless sensor network) как среды беспроводного взаимодействия цифровых объектов в составе сети промышленного интернета вещей в различных автоматизированных системах [122, 144] обладает рядом преимущества.

Таблица 3.1 – Классификация атак в промышленных беспроводных сенсорных сетях по направлению воздействия [122]

Тип атаки	**Описание**
Измененная маршрутная информация.	Наибольшая угроза для децентрализованных сетей; Последствия: увеличение времени доставки пакета данных;
Выборочная рассылка	Поврежденный узел сенсорной сети способен избирательно стирать необходимые пакеты. Последствия: нарушение целостности и доступности данных;
Атака «бездонная воронка» (Sinkhole Attack)	Поврежденный узел сети меняет свое нормальное поведение в системе и начинает перенаправлять на себя весь трафик сенсорной сети, напоминая «воронку». Последствия: как только поврежденный узел смог стать посредником между сенсорным узлом и базовой станцией, он способен производить манипуляции с перехваченными пакетами данных.
Атака «червоточина» (Wormhole attack)	Организация транспортной среды между поврежденными узлами сенсорной сети для транспортировки перехваченных пакетов для атакующей системы. Не требует компрометации узла сенсорной сети.
«Колдовская» атака (Sybil attack)	Использование поврежденным узлом сенсорной сети нескольких лжеинидентификаторов, представляясь одновременно несколькими узлами сети. Последствия: нарушение правильной работы распределенного хранения, маршрутизации, агрегации данных, голосования в сенсорной сети.
Атака «переполнение» («HELLO» flood attack)	Вид широковещательной атаки. Злоумышленник, используя высокочастотный радиопередатчик с большой вычислительной мощностью, организует рассылку «Hello»-пакетов всем узлам беспроводной сенсорной сети, что интерпретируется узлами, получившими Hello-пакеты, как посылку данных от своего соседа, при этом пакеты будут исходить от пораженных узлов.
Атаки по расписанию	Изменение поведения широковещательной рассылки по расписанию временного мультиплексирования канала (TDMA). Последствия: коллизия пакетов, которая приводит к потере данных.

Результаты обнаружения сетевых атак в промышленной сети на основе алгоритмов интеллектуального анализа данных [142]

Таблица 3.2 – Оценка эффективности различных классификаторов.

Модель	Accuracy	Precision	Recall	F1	Время обучения, с
RandomForestClassifier (RF)	1.000	1.000	1.000	0.919	111.36
LogisticRegression (LR)	0.999	0.983	0.995	0.918	175.21
MLPClassifier (MLP)	0.999	0.986	0.995	0.919	2459.23

Результаты анализа сетевого трафика на основе методов машинного обучения [255]

Набор данных CICIDS2017 содержит трафик наиболее распространенных сетевых атак (в формате PCAP) и включает результаты анализа сетевого трафика с использованием CICFlowMeter с размеченными потоками на основе маркера времени, IP-адресов источника и назначения, портов источника и назначения, протоколов и атак. Промоделирована работа 25 пользователей с использованием протоколов HTTP, HTTPS, FTP, SSH и электронной почты. Суммарно общее количество примеров составляет 3119345, а количество выделенных признаков – 84.

Набор данных был разделен на обучающую и тестовую выборки – 16800 и 7200 примеров соответственно.

С использованием перекрестной проверки с 5-ю разбиениями обучающего набора данных, была проведена процедура классификации обучающего и тестового набора данными классификаторами с указанными выше параметрами (Таблица 3.3).

Таблица 3.3 – Результаты первого этапа тестирования классификаторов

	Название классификатора	CV Fit Time, секунд	CV mean F1	Test F1
1	XGBClassifier	10.35923	0.96816	0.96653
4	RF	1.15881	0.96637	0.96597
0	KNN	0.04588	0.94542	0.94639
10	MLP	44.32636	0.92185	0.92000
2	SVM	2.96680	0.75893	0.75444
6	LR	1.86500	0.71601	0.73319
3	CART	0.03520	0.67369	0.66528
7	NB	0.00738	0.61369	0.60153
5	AdaBoost	0.83967	0.53167	0.56597
8	LDA	0.02663	0.56911	0.55667
9	QDA	0.01414	0.54542	0.52333

Во втором эксперименте были использованы сверточные нейронные сети с одномерным и двумерным входным слоем (CNN1D и CNN2D соответственно).

Набор данных был разделен на выборки аналогично предыдущей модели. Само обучение заняло 100 эпох, по итогу чего F1-мера модели на обучающей выборке составила 0,935, на тестовой выборке – 0,943.

На заключительном этапе был использован комитет классификаторов, включающий в себя Случайный лес, Алгоритм AdaBoost и ExtraTreesClassifier.

Последний реализует метаоценку, соответствующую ряду рандомизированных деревьев решений, или дополнительных деревьев на различных подвыборках набора данных, и использует усреднение для повышения точности прогнозирования и контроля избыточной подгонки.

Параметры комитета: тип голосования – «soft» (полноценное голосование и взвешивание предсказаний моделей для каждого класса); веса распределены как [2, 1, 3].

Набор данных был разделен на выборки аналогично предыдущей модели. После обучения f1-мера модели на обучающей выборке составила 0,981, на тестовой выборке – 0,967 (Таблица 3.4).

Таблица 3.4 – Результаты второго этапа тестирования классификаторов

Название классификатора	Точность на обучающей выборке	F1-мера на обучающей выборке	Точность на тестовой выборке	F1-мера на тестовой выборке
VotingClassifier	0.980	0.981	0.967	0.967
RF	0.976	0.977	0.967	0.967
KNN	0.982	0.982	0.954	0.955
CNN2D	0.936	0.935	0.944	0.943
CNN1D	0.917	0.916	0.924	0.922
DNN	0.873	0.872	0.879	0.878
SVM	0.529	0.408	0.520	0.399
LR	0.439	0.268	0.434	0.263

Классификаторы расположены в таблице 5 по убыванию значения их f1-меры на тестовой выборке.

Система защищенного обмена данными в программно определяемых сетях объектов энергетического комплексам

Технология программно-определяемых сетей (SDN) позволяет повысить эффективность управления и обеспечить требуемый уровень масштабируемости решений за счет отделения функций передачи трафика от функций управления, которые вынесены в контроллеры, что упрощает и удешевляет коммутационное оборудования.

Угрозы нарушения информационной безопасности и соответствующие им меры противодействия можно разделить уровни, согласующиеся с архитектурой SDN. Анализ угроз и уязвимостей SDN основан на применении банка данных угроз ФСТЭК России (таблица 3.5).

Таблица 3.5 – Описание видов угроз в SDN-сетях

Уровень атаки	Вид атаки	Краткое описание	Меры защиты	Особенности реализации защитных мер	Актуальность угрозы
Уровень инфраструктуры [14]	«Человек посередине» УБИ.034	Перехват и модификация злоумышленником данных, передаваемых между контроллером и коммутаторами или между коммутаторами	- создание защищенного канала между контроллером и коммутатором (TLS) - использование зашифрованных меток	пакеты, не зашифрованные определенным образом, будут отбрасываться; TLS – ресурсоемкая и сложно конфигурируемая схема; в спецификации не является обязательной мерой;	Высокая
	DoS-атака на коммутатор УБИ.012	Генерация злоумышленником большого количества трафика, приводящая к переполнению таблицы потоков/буфера коммутатора	- использование зашифрованных меток - использование систем обнаружения вторжений (СОВ) с модулем обнаружения аномалий	При получении пакета проверяется наличие метки и ее корректность, в противном случае пакет отбрасывается;	Высокая
Уровень контроля	DoS-атака на контроллер УБИ.014	Большое количество трафика, посылаемого на коммутаторы, вынуждает их посылать запросы контроллеру на получение новых правил, резко снижая его производительность [21]	- использование зашифрованных меток - резервирование контроллеров		Высока
	Угрозы для контроллера от приложений	Разнообразие приложений и их требований	- регулярное обновление	использовать только доверенные	Низкая

	УБИ.007	может приводить к различного рода конфликтам и непредвиденным ситуациям	ПО контроллера - актуальная политика безопасности на контроллере	приложения от официальных производителей	
Уровень приложений	Несанкционированный доступ приложений к ресурсам сети УБИ.006	Приложение с вредоносным кодом, внедренным в него злоумышленниками, может получить несанкционированный доступ к ресурсам сети и изменять ее конфигурацию	- использование приложений только от доверенных производителей - регулярное обновление приложений		Низкая

Для обеспечения защиты OpenFlow управляющего трафика сети ключевыми являются обеспечение доступности и целостности данных. Возможные контрмеры и особенности их реализации представлены в табл. 3.6.

Таблица 3.6 – Основные контрмеры и особенности их применения

Последствия атаки	Достоинства	Недостатки
Использование СОВ с модулем обнаружения аномалий	СОВ с модулем обнаружения аномалий позволяет обнаруживать аномальное отклонение в параметрах трафика и сети, предупреждая в том числе и о DoS-атаках;	СОВ не противодействует самой атаке, к тому же эффективность зависит от ее правильной настройки, и влечет за собой дополнительные расходы. В случае атаки «человек посередине» практически бесполезна;
Резервирование контроллеров	благодаря резервному контроллеру в SDN появляется возможность взятия им на себя полномочий по управлению сетью в случае, когда был атакован основной контроллер;	резервный контроллер требует сложной настройки конфигурации и дополнительные расходы; не решает проблему DoS-атаки; может быть использована в качестве придания дополнительной надежности сети, но не как основной мерой защиты;
Использование зашифрованных меток	внедрение в заголовок пакета зашифрованной метки, позволяющей определить, является ли трафик корректным и исходящим от доверенного устройства в сети;	накладные расходы на модификацию передаваемых пакетов управляющего трафика; дополнительные вычислительные ресурсы, необходимые на операции шифрования и дешифрования;

Предлагается использовать метод внедрения в заголовок IP-пакета зашифрованной метки, являющейся зашифрованной хэш-суммой содержимого пакета. При принятии пакета, первым делом проверяется корректность данной

метки. В случае успешной проверки пакет идет на дальнейшую обработку, либо просто отбрасывается. Так как время данной проверки относительно мало, это позволяет избежать негативных последствий DoS-атак. В случае атаки «человек посередине» данная мера защиты так же будет эффективна.

Протокол OpenFlow располагается над транспортным уровнем модели OSI и использует TCP в своей работе. При этом извлечение OpenFlow данных из пакета занимает относительно много процессорного времени сетевого оборудования. Во многом из-за этого становится возможным отказ контроллера в результате DoS-атаки.

Хеш-сумма содержимого пакета, которая отправляется вместе с пакетом, позволит принимающей стороне убедиться в целостности содержащейся информации. Во избежание подделки тела пакета и хэш-суммы злоумышленником необходимо шифровать внедряемую метку. Следовательно, без соответствующего ключа злоумышленник не сможет расшифровать ее, изменить и зашифровать вновь. При попытке изменения только тела пакета, принимающая сторона обнаружит подмену, так как шифрованный и вычисленный хэши не совпадут, и отбросит пакет.

Итоговый алгоритм защиты управляющего трафика SDN включает следующие шаги:

- обнуление поля идентификатора и контрольной суммы в заголовке пакета;
- расчет хэш-суммы тела пакета при помощи алгоритма ГОСТ 34.11-2018;
- шифрование хэш-суммы при помощи ГОСТ 34.12-2018;
- получившаяся метка помещается в поле «Идентификатор» IP-пакета.

Приложение И – Методика тестирования и оценка эффективности предложенных способов мониторинга целостности ТМИ

5А1. В данном случае не происходит атака злоумышленника, а происходит отказ оборудования или обрыв передачи сигнала с борта ЛА. Начиная с 85 итерации значения данных, полученных с ЛА, резко изменились, и значение их средней величины снизилось относительно средней величины предыдущих значений, получаемых с модели. Падение величины принимаемого сигнала произошло практически на последних итерациях в текущем временном окне анализа, однако, значения параметров согласованности говорят о недостоверности принимаемых данных, но сигнал системы контроля свидетельствует о неполадках на борту. Симулирована ситуация «Отказ оборудования».

5А2. В данном примере симулирована атака злоумышленника «2В. Подмена данных на данные, непохожие на подлинные, в конце временного окна». На 57 итерации среднее значение передаваемого сигнала резко изменилось по сравнению с предыдущими данными. Искажение сигнала происходит на поздних итерациях, что снижает чувствительность коэффициента детерминации. Однако, значения коэффициента и детерминации, значение MAPE и евклидово расстояние низкие. система контроля показывает, что на ЛА все в порядке, а параметры согласованности ТВР низкие для установившегося режима работы САУ ГТД. Целостность данных нарушена.

5Б1. В данном примере симулирована атака злоумышленника «2Б. Подмена данных на данные, похожие на подлинные, в середине временного окна». Этот пример иллюстрирует ситуацию, когда параметры согласованности ТВР принимают низкие значения, САУ ГТД находится в переходном режиме работы, система контроля говорит о нормальной работе САУ ГТД на ЛА. Такие низкие параметры согласованности свидетельствуют о нарушении целостности данных.

5Б2. Атака злоумышленника отсутствует. Здесь САУ ГТД работает в установившемся режиме, а, значит, параметры согласованности ТВР должны иметь высокие значения, что и отражают значения коэффициента детерминации, MAPE и евклидово расстояние. Целостность данных не нарушена. Атака отсутствует.

5В1. САУ ГТД находится в переходном режиме работы, а, значит, окно для рассогласованности параметров шире и некоторые из параметров согласованности могут принимать средний уровень значений, а именно коэффициент

детерминации, а также евклидово расстояние, однако, MAPE имеет высокое значение. Целостность данных не нарушена. Атака отсутствует.

5В2. САУ ГТД находится в переходном режиме работы, и, несмотря на низкое значение MAPE, коэффициент детерминации высокие, евклидово расстояние мало. Целостность данных не нарушена. Атака отсутствует

5В3. В данном случае, во временном окне параметр САУ ГТД принимал постоянное значение, поэтому невозможно вычислить коэффициент детерминации, им присваивается значение NaN (Not-a-Number), однако, MAPE и евклидово расстояние принимают низкие значение, режим работы САУ ГТД статический, система контроля говорит о нормальном режиме работы. Целостность данных не нарушена. Атака отсутствует.

5Г1. Симулирована атака злоумышленника «3А. Увеличение (уменьшение) параметров САУ ГТД при сохранении характера поведения параметров в течение всего временного окна». Установившийся режим САУ ГТД. Сигнал системы контроля – нормальная работа. Из-за того, что характер поведения параметров сохраняется, коэффициенты и детерминации принимают высокое значение, однако, MAPE и евклидово расстояние низкие, следовательно, целостность данных нарушена.

5Г2. Симулирована атака злоумышленника «1А. Наложение шума на передаваемые данные в течение всего временного окна». Установившийся режим САУ ГТД. Сигнал системы контроля –нормальная работа. Все параметры согласования принимают низкие значения. Целостность данных нарушена.

5Д. Симулирована атака злоумышленника «4А. Подделка управляющих и внешних воздействий в течение всего временного окна». Установившийся режим САУ ГТД. Сигнал системы контроля –нормальная работа. Все параметры согласования принимают низкие значения. Данные, сгенерированные моделью, не соответствуют данным, полученным с САУ ГТД. Целостность данных нарушена.

При решении задачи кластеризации на типы согласованности выделены 7 типов согласованности, представленные в таблице И.1

Таблица И.1

Коэф. Детерминации	Евклидово расстояние	MAPE	Тип согласования ТВР
высокий	высокий	высокий	1 тип
высокий	высокий	средний	

высокий	средний	высокий	
средний	высокий	высокий	
высокий	средний	средний	2 тип
средний	высокий	средний	
средний	средний	высокий	
высокий	низкий	средний	3 тип
высокий	средний	низкий	
низкий	высокий	средний	
низкий	средний	высокий	
средний	средний	средний	
средний	низкий	средний	4 тип
средний	средний	низкий	
Низкий/NaN	средний	средний	
низкий	низкий	низкий	
высокий	высокий	высокий	
высокий	высокий	высокий	
высокий	низкий	низкий	5 тип
низкий	низкий	высокий	
низкий	высокий	низкий	
средний	низкий	низкий	6 тип
Низкий/NaN	средний	низкий	
Низкий/NaN	низкий	низкий	
Низкий/NaN	низкий	средний	
NaN	высокий	высокий	7 тип

Таблица И.2

К	РРС	Тип согласования	Результат
0	любой	любой	Отказ САУ ГТД.
1	установившийся	1	нормальная работа
1	установившийся	2	нормальная работа
1	установившийся	7	нормальная работа
1	установившийся	3	нарушение целостности
1	установившийся	4	нарушение целостности
1	установившийся	5	нарушение целостности
1	установившийся	6	нарушение целостности
1	неустановившийся	1	нормальная работа
1	неустановившийся	2	нормальная работа
1	неустановившийся	3	нормальная работа
1	неустановившийся	4	нарушение целостности
1	неустановившийся	5	нарушение целостности

1	неустановившийся	6	нарушение целостности

Таблица И.3

Фиг	К	Режим работы модели САУ ГТД	Коэф. Детерми-нации	Евклидово расстояние	MAPE	Принятое решение
5А1	0	переходный	низкий	средний	средний	Отказ САУ ГТД
5А2	1	установившийся	низкий	низкий	низкий	нарушение целостности
5Б1	1	переходный	низкий	низкий	низкий	нарушение целостности
5Б2	1	установившийся	средний	высокий	высокий	нормальная работа
5В1	1	переходный	средний	высокий	средний	нормальная работа
5В2	1	переходный	высокий	высокий	низкий	нормальная работа
5В3	1	установившийся	Низкий/ NaN	высокий	высокий	нормальная работа
5Г1	1	переходный	высокий	низкий	низкий	нарушение целостности
5Г2	1	переходный	низкий	низкий	низкий	нарушение целостности
5Д	1	переходный	средний	низкий	низкий	нарушение целостности

Таблица И.4

Коэффициент детерминации	Евклидово расстояние	MAPE	Тип рассогласования
0,808	0,000	0,135	1
0,513	0,005	0,394	7
1,000	0,010	0,643	1
1,000	0,005	0,364	1
1,000	0,000	0,076	1
0,549	0,813	4,242	7
0,417	0,173	3,586	7
0,731	0,117	2,976	1
0,417	18,442	27,822	6
0,646	18,394	27,784	6
1,000	13,964	23,002	6
0,999	13,847	24,276	6
0,990	10,855	25,690	6
1,000	2,289	13,419	2
1,000	2,288	13,419	2
1,000	2,288	13,420	2
1,000	2,289	13,421	2
1,000	2,288	13,411	2
1,000	2,289	13,417	2
0,403	8,783	8,353	6
0,340	9,533	9,286	6
0,446	1,312	6,244	3
0,668	1,312	6,244	3

Итоговой протокол экспериментов по классификации типа согласованности представлен в таблице И.5.

Таблица И.5

Тип рассогласования	Количество тестовых выборок	Количество случаев успешной классификации типа согласованности	Оценка вероятности успешной классификации типа согласованности
1	406	372	0,916
2	440	405	0,920
3	93	86	0,925
4	307	283	0,922
5	300	276	0,920
6	616	566	0,919
7	338	311	0,920
Итого	**2500**	**2299**	**0,92**

Таблица И.6

Тип атаки	Количество тестовых выборок	Количество случаев успешного распознавания атаки	Оценка вероятности успешного распознавания атаки
1а	341	330	0,97
1б	403	386	0,96
1в	402	331	0,82
2а	310	300	0.97
2б	310	278	0,89
2в	310	269	0,87
3а	309	281	0.90
3б	310	265	0,85
3в	310	259	0.83
4а	309	279	0,90
4б	311	263	0,85
4в	320	257	0,80
Итого	**3945**	**3498**	**0,89**

Таблица И.7

Тип атаки	Количество тестовых выборок	Количество случаев успешного распознавания атаки	Оценка вероятности успешного распознавания атаки
1а	281	239	0,85
1б	293	223	0,76
1в	272	196	0,72
2а	279	226	0.81
2б	298	228	0,76
2в	280	236	0,79
3а	300	222	0.74
3б	289	205	0,71
3в	279	196	0.7
4а	280	265	0,95
4б	274	260	0,95
4в	290	259	0,89
Итого	**3415**	**2755**	**0,81**

Приложение К Сравнительный анализ алгоритмов когнитивного моделирования при оценке рисков ИБ

Рассматриваются [126] следующие подходы к формированию оценки рисков ИБ на основе экспертных оценок и данных проведенного аудита:

1. сети Байеса на основе графа атак;
2. нечеткие когнитивные карты;
3. нечеткие серые когнитивные карты.

Эти подходы объединяет возможность получения интегральной оценки рисков ИБ на основе вероятностного подхода и когнитивного моделирования.

Целью является сравнительный анализ методов когнитивного моделирования при оценке рисков ИБ на основе построения модели атакующих действий злоумышленника с применением технологий интеллектуального анализа. Для достижения поставленной цели необходимо выполнить оценку особенностей применения методов когнитивного моделирования (сеть Байеса на основе графа атак, нечеткие когнитивные карты и нечеткие серые когнитивные карты) для оценки рисков ИБ компьютерной сети на примере.

К.1 Анализ возможностей когнитивного моделирования с помощью сети Байеса на основе графа атак для оценки рисков информационной безопасности

Графы атак являются инструментом топологического анализа защищенности информационной системы и позволяют учитывать взаимосвязь и свойства объектов информационной системы на основе результатов сканирования сети, модели нарушителя и данных о конфигурации сети (правила фильтрации межсетевого экрана, маршрутизации, обнаружения атак, достижимости хостов и т.д.). Классификация представления графов атак приведена в таблице К.1 [126].

Для формирования рассуждений в условиях неопределенности в соответствии с оценками вероятностей событий и связи между событиями удобным является построение на основе condition-oriented dependency графа сетевой модели в виде сети Байеса.

Таблица К.1 – Классификация графов атак

Название	Описание
state enumeration graph	вершинам соответствуют тройки (s, d, a), где s – источник атаки, d – цель атаки, a – элементарная атака; дуги обозначают переходы из одного состояния в другое
condition-oriented dependency graph	вершинам соответствуют результаты атак, а дугам – элементарные атаки, приводящие к таким результатам
exploit dependency graph	вершины соответствуют результатам атак или элементарным атакам, дуги отображают зависимости между вершинами – условия, необходимые для выполнения атаки и следствие атаки

Совместное распределение вероятностей для текущего узла и родительских узлов можно записать в виде (К.1):

$$P(X) = \prod_{i=1}^{n} P(X_i | parents(X_i)) \quad (К.1)$$

где $X = \{X_1, \ldots, X_n\}$ множество случайных величин (непрерывных или дискретных) и для каждого узла X_i имеется направленное ребро от каждого узла в паре родительских узлов X_i, указывающее на X_i.

Такая графическая модель может использоваться для оценки рисков ИБ информационной системы с помощью когнитивного моделирования. Каждой вершине графа атак соответствует узел компьютерной сети, которому соответствует значение вероятности достижения этой вершины злоумышленником. Эти оценки выставляются в соответствии с базой системы оценки общей уязвимости CVSS 2.0, в которой численно характеризуется уязвимость по различным параметрам.

В качестве иллюстрации использования сети Байеса для оценки риска ИБ с применением когнитивного моделирования рассмотрим пример из [126].

Рассмотрим компьютерную сеть (рисунок К.1, а), в которой сервер $Host_1$ имеет доступ к передаче и приему файлов по протоколам File Transfer Protocol (FTP), Secure Shell (SSH) и Remote Shell (RSH), а сервер $Host_2$ имеет доступ к передаче и приему данных по протоколам FTP и RSH. Межсетевой экран пропускает трафик по протоколам FTP, SSH и RSH с рабочей станции пользователя $Host_0$ на оба сервера и блокирует весь остальной трафик. Цель злоумышленника – получить права администратора (root) на $Host_2$.

На графе атак (рисунок К.1, б) условия *c* представлены в виде эллипсов, в которых в круглых скобках указан задействованный узел сети. Уязвимости *e* отображаются в прямоугольниках, указывая в нижнем индексе на исходный и конечный узел, где первое число отображает источник, второе – назначение.

Их рисунка К.1, б, видно, что для атакующего существует три возможных пути проведения атаки. Один из путей атаки начинается с использования переполнения буфера SSH с $Host_0$ на $Host_1$ ($ssh\_bof_{0,1}$), что дает злоумышленнику возможность выполнять произвольный код на $Host_1$ в роли обычного пользователя. Затем злоумышленник использует уязвимость FTP на $Host_2$ ($ftp\_rhosts_{1,2}$) для анонимной загрузки списка доверенных хостов. Это позволяет злоумышленнику удаленно выполнять команды оболочки на $Host_2$ без предоставления пароля. Использование локального переполнения буфера на $Host_2$ ($local\_bof_{2,2}$) повышает привилегии злоумышленника до уровня администратора на этом сервере.

Вероятности того, что злоумышленник может успешно использовать уязвимости в сети получены на основе «Base Score» из базы уязвимостей CVSS 2.0, и составляют: $p(ftp\_rhosts) = 0.8$, $p(sshd\_bof) = 0.1$, $p(rsh) = 0.9$ и $p(local\_bof) = 0.1$. Вероятности выполнения условий в этом подходе принимаются равными 1.

Финальная вероятность достижения злоумышленником вершины $P(root_2)$ равна $P(root_2) = P(local\_bof_{2,2}) = 0.087$.

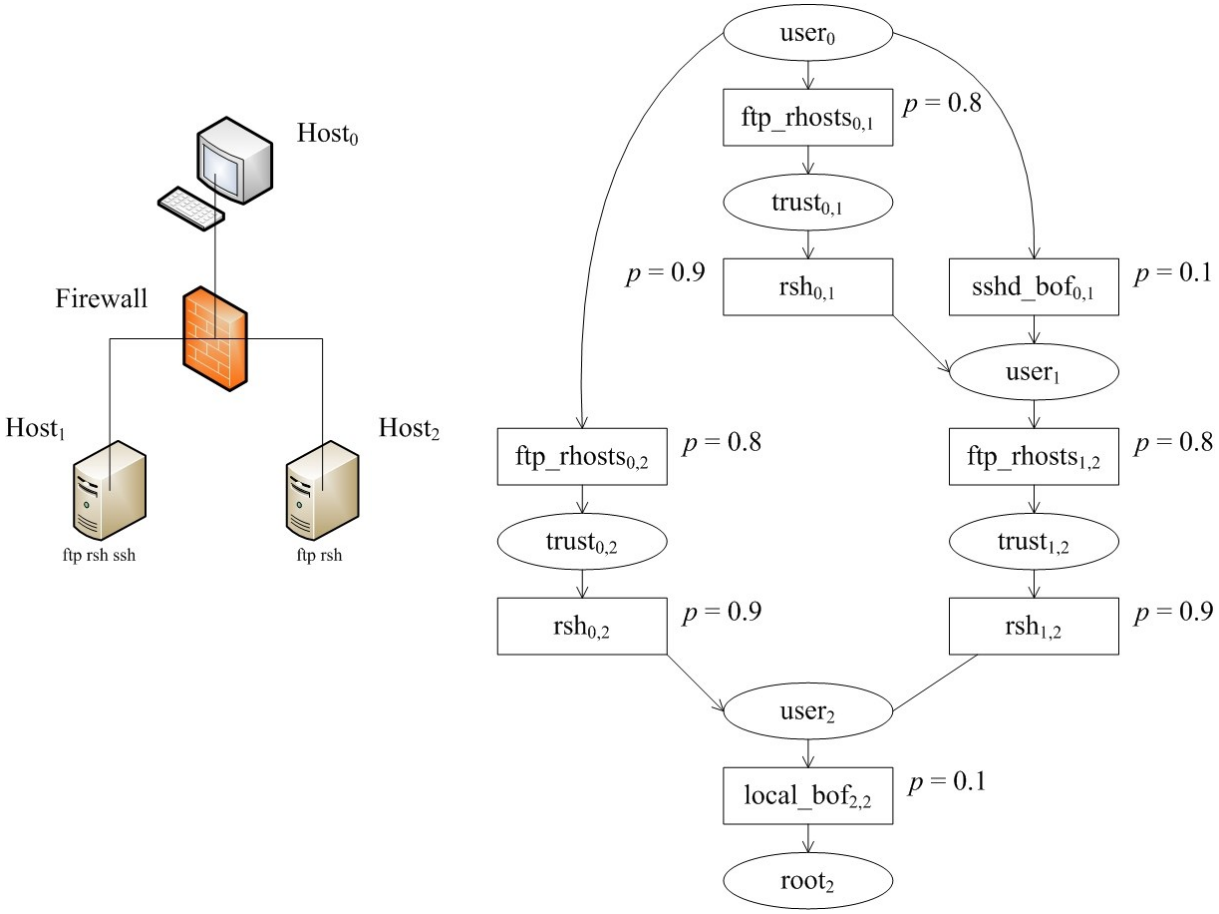


Рисунок ВиБер.1 – Конфигурация сети и граф атак

Расчет данным методом позволяет получить вероятностную оценку, непосредственно пригодную определения рисков ИБ для целевого актива. Недостатком такого подхода является сложность масштабирования, так как для больших корпоративных информационных систем необходим переход к приближенным вероятностным выводам.

К.2 Анализ возможностей когнитивного моделирования оценки рисков ИБ с помощью нечетких когнитивных карт

Рассмотрим нечеткую когнитивную карту (рисунок К.2), построенную на топологии сети, представленной в примере, рассмотренном выше. Здесь внешний пользователь – атакующий, он представлен концептом 1, а целевой узел – концептом 7.

Веса связей между узлами взяты из предыдущего примера, однако в некоторых вариантах расчетов [56, 128] весовые коэффициенты получают с помощью экспертной оценки.

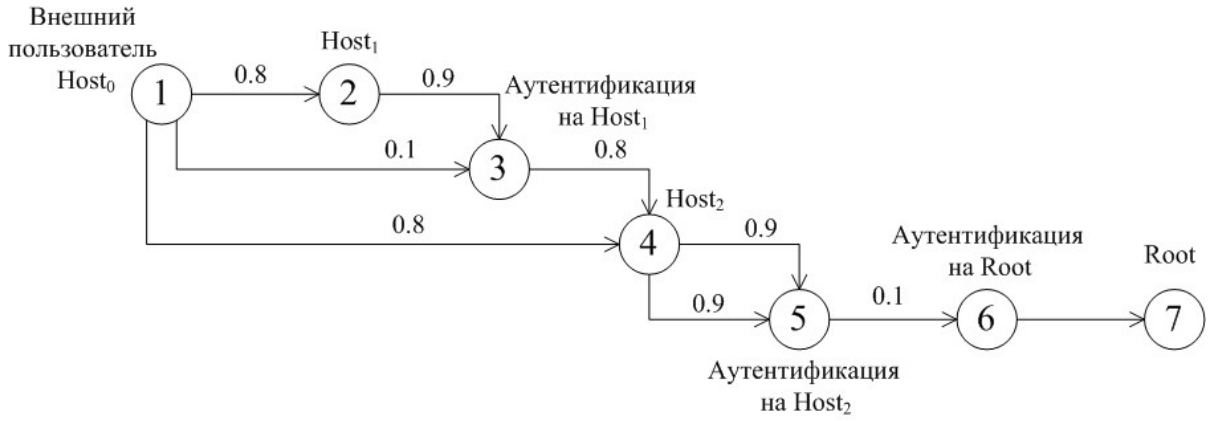
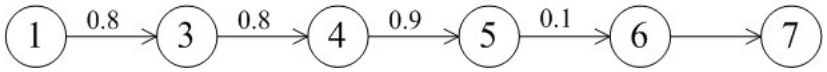


Рисунок К.2 – Нечеткая когнитивная карта

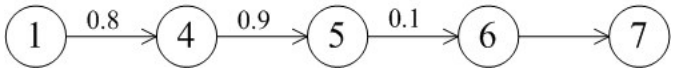
Значение $P_{act} = 0.7$, т.к. действие осуществляется внешним пользователем.

Рассмотрено три сценария действий атакующего (рисунок 3а-в).

а)



б)



в)

Рисунок К.3 – Сценарии атакующих действий

Вероятности реализации этих сценариев принимает следующие значения: $P_1 = 0.0363$, $P_2 = 0.0403$, $P_3 = 0.0504$.

Вероятность атаки на целевой объект равна:

$P = max\{P_j\}.$	

Недостаток НКК – необходимость ввода оценки «Вероятность активации входного концепта». Данная экспертная оценка существенно влияет на финальную оценку рисков ИБ, а также отсутствует в двух других рассматриваемых методиках расчётах рисков ИБ. Вторым недостатком является невозможность комплексно оценить влияние нескольких факторов на один узел. Для такого случая используется операция поиска максимума среди весов влияния, что не всегда отражает вероятность реализации атаки на данный узел.

К.3 Анализ возможностей когнитивного моделирования оценки рисков ИБ с помощью нечетких серых когнитивных карт

Нечеткая серая когнитивная карта для рассматриваемой топологии сети представлена на рисунке 4:

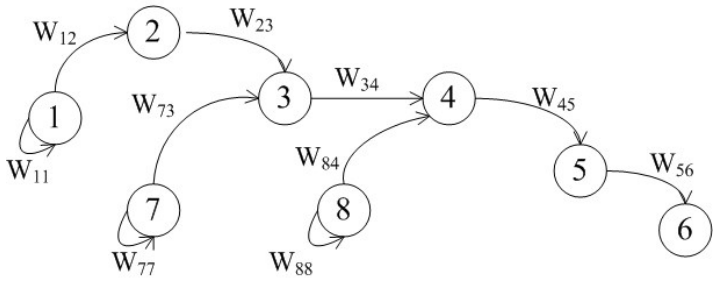


Рисунок К.4 – Нечеткая серая когнитивная карта

Концепт C_1 – угроза доступа внешнего пользователя к $Host_1$, C_2 – $Host_1$, концепт C_3 представляет собой процедуру аутентификации на $Host_1$, концепт C_4 – $Host_2$, C_5 – аутентификация на $Host_2$, C_6 – получение прав администратора на $Host_2$. C_7 – угроза аутентификации на $Host_1$, концепт C_8 – угроза доступа к $Host_2$. Концепты C_1, C_7 и C_8 – драйверы.

Веса связей взяты из примера, но представлены в таблице К.2 в виде «серых» чисел.

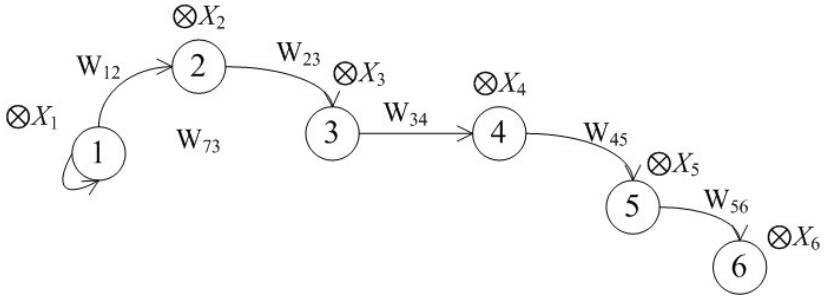
Таблица К.2 – Значения весов НСКК

Вес	Значение веса связи	«Серость»
W_{12}	[0.7; 0.9]	0.1
W_{23}	[0.85;0.95]	0.05
W_{73}	[0.05;0.2]	0.075
W_{84}	[0.7;0.9]	0.1
W_{34}	[0.7; 0.9]	0.1
W_{45}	[0.85;0.95]	0.05
W_{56}	[0.05;0.2]	0.075

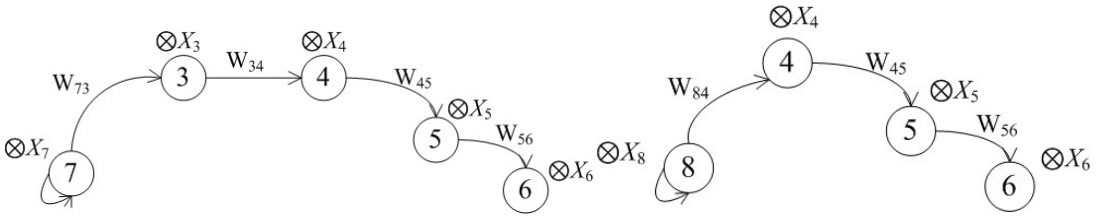
Значения «серости» оценки вычисляются по формуле (К.2):

$$\Phi(\otimes W_{ij}) = \frac{\left|\overline{W_{ij}} - \underline{W_{ij}}\right|}{2} \quad \text{(К.2)}$$

Рассмотрим три сценария атаки на рисунке К.5.



а)



б) в)

Рисунок К.5 – Сценарии атаки: первый (а), второй (б), третий (в)

Произведем оценку верхней и нижней границы X_6. Начальные условия для $X_2 - X_6 = \{0,0\}$, а X_1 как оценка генератора, имеет оценку $\{0.8,\ 1\}$. Тогда рассчитаем значения оценок состояния. Расчётные установившиеся значения для верхних и нижних границ достигаются за 10 тактов.

Серый вектор для сценария 1 получился следующим:

$$\otimes X_A = \{[0.8;\ 1], [0.37;\ 0.51], [0.24;\ 0.41], [0.2;\ 0.33], [0.073;\ 0.062]\}$$

Искомые значения для концепта C_6 будут определяться серым числом $\otimes X_6 \in [0.0073;\ 0.062]$.

После выполнения аналогичных расчетов для сценариев 2 и 3 получаем:

Сценарий 2: $\otimes X_6 \in [0.015;\ 0.083]$.

Сценарий 3: $\otimes X_6 \in [0.017;\ 0.086]$.

Интегральное значение оценки рисков ИБ вследствие получения прав администратора на $Host_2$ примем как среднее арифметическое сценариев 1-3:

$$\otimes X_6 \in [0.011;\ 0.077]$$

Данный метод позволяет учесть фактор неопределенности, возникающий в процессе оценки вероятности уязвимости каждого из узлов ИБ и, в отличии от НКК, позволяет оценивать комплексное влияние нескольких факторов на один узел информационной сети в каждом из сценариев атак.

К.4 Сравнительная характеристика возможностей когнитивного моделирования при оценке рисков ИБ

Сравнительный анализ когнитивного моделирования оценки рисков ИБ с использованием Байесовской сети, НКК и НСКК приведены в таблице К.3.

Таблица К.3 – Сравнительная характеристика методов оценки рисков ИБ

Критерий	Байесовская сеть	НКК	НСКК
Простота использования	Низкая	Средняя	Средняя
Интерпретируемость результатов	Выше средней	Средняя	Средняя

Сложность вычислительной реализации	Высокая	Средняя	Выше средней
Согласованность оценок с другими подходами	Выше средней	Высокая	Высокая
Применимость к организации (объекту защиты) разного размера и области деятельности	Средняя	Выше средней	Выше средней
Удобство применения методики и наличие ПО	Выше средней	Средняя	Средняя
Удобство восприятия результатов оценки	Среднее	Выше средней	Выше средней

Основной проблемой при использовании рассмотренных методов когнитивного моделирования является недостаточный объем статистической информации об угрозах и уязвимостях и/или его противоречивость и неполнота, что затрудняет формирование достоверных оценок рисков ИБ и приводит к существенному влиянию качества экспертных оценок, полученных в процессе аудита ИБ, на итоговые результаты.

К.5 Оценка рисков ИБ АСУ ТП нефтедобывающего предприятия с помощью ансамбля когнитивных карт

В качестве исследуемого объекта защиты рассматривается АСУ ТП нефтедобывающего предприятия, интегрированная в комплексную систему оперативного контроля и управления в реальном масштабе времени, и позволяющая передавать накапливаемые технологические данные в системы управления производственными процессами вышележащих уровней. Технологическая цепочка включает основные элементы: добыча нефти, сбор нефти, подготовка нефти, транспортировка товарной нефти.

Обобщенная структурная схема территориально распределенной системы обустройства месторождения [136, 138] и транспорта товарной нефти (ТТН), представлена на рисунке К.6, где: УПН – установка подготовки нефти; ЦПС – центральный пункт сбора; НПС – нефтеперекачивающая станция; ПСП – приемо-сдаточный пункт; ГСС – газосборная сеть; 1 – ВПТ – внутри промысловой трубопровод; ДС – добывающие скважины; НС – нагнетающая скважина; ВС – водозаборная скважина; КС – куст скважин; 2 – водовод; 3 – нефтесборный трубопровод; МН – магистральный нефтепровод; АГЗУ – автоматическая групповая

замерная установка; ДНС – дожимная насосная станция; УПСВ – установка предварительного сбора воды; КНС – кустовая насосная станция.

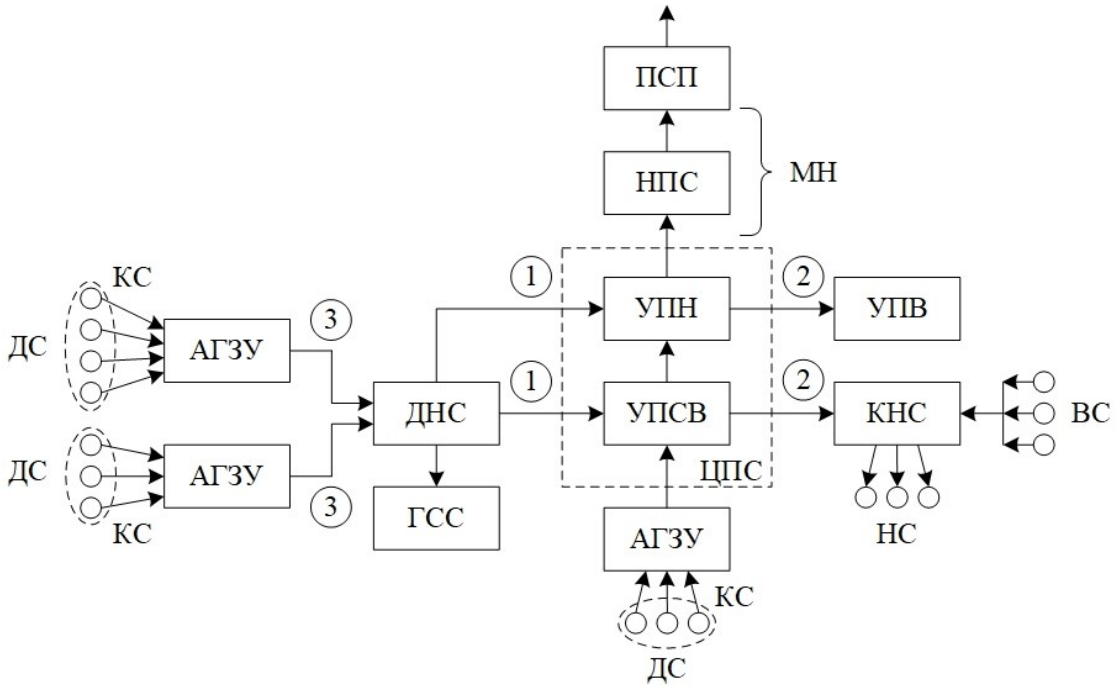


Рисунок К.6 – Обобщенная структурная схема территориально-распределенной системы обустройства месторождения и транспорта товарной нефти

Согласно терминологии ГОСТ 62443, необходимо реализовать несколько стадий анализа и моделирования объекта защиты. Первой стадией является создание референсной модели объекта защиты, позволяющей выделить основные виды деятельности, технологические цепочки и процессы, АСУ и прочие активы, распределенные по 5 логическим уровням.

Подсистемы АСУ ТП месторождения можно рассматривать как отдельные зоны безопасности, объединяемые по принципу единства выполняемых функций и требований к безопасности их реализации. Ввиду сложности анализируемого объекта, рассмотрим фрагмент референсной модели архитектуры АСУ ТП месторождения, включающий основные элементы АСУ кустовых площадок, телекоммуникационное оборудование, линии связи и т.п. (рисунок К.7).

Основные последствия реализации атак на АСУ кустовых площадок:

– останов кустовой площадки;

– блокировка систем противоаварийной защиты;

– блокировка автоматизированных систем пожаротушения;

– потеря возможности мониторинга параметров оборудования и ТП;

– перевод объекта в аварийный режим.

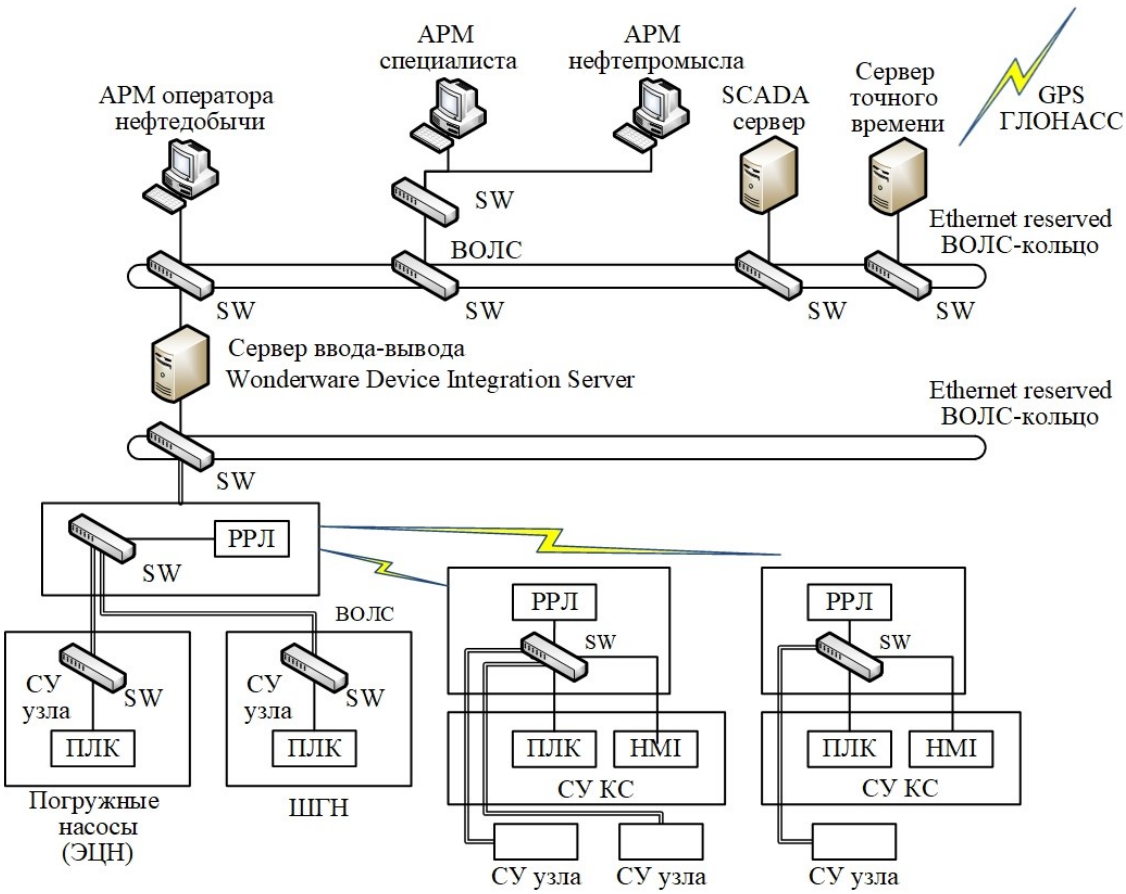


Рисунок К.7 – Фрагмент референсной модели архитектуры АСУ ТП кустовых площадок

Согласно отчетам «Лаборатории Касперского» и Positive Technologies[1] [55, 120], наиболее часто подвергаются атакам следующие элементы промышленных систем: SCADA-системы, ПЛК, инфраструктура и ОС, сетевые протоколы.

Для рассматриваемого фрагмента референсной модели архитектуры АСУ ТП кустовых площадок на основе данных BSI[2], предлагается проанализировать возможные векторы атак, реализуемые внутренним злоумышленником (в последнем случае, это такие атаки, как: подмена исполняемые файлов ПО серверов и АРМ, перезапись проектов ПЛК в ходе работы системы, отказ в обслуживании оборудования).

Исходя из сформированного списка векторов атак и последствий их реализации, рассмотрим задачу анализа рисков кибербезопасности промышленных объектов с учетом воздействия на систему возможных внутренних угроз, используя в качестве инструмента моделирования аппарат когнитивного

[1] Уязвимости в АСУ ТП: итоги 2018 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ics-vulnerabilities-2019/ (дата обращения: 13.03.2020).
[2] Обеспечение кибербезопасности промышленного IT- контура. URL: https://www.pta-expo.ru/spb/ethernet/2014/prosoft_ProSoft_2.pdf (дата обращения: 13.03.2020).

моделирования. Когнитивная карта для оценки рисков кибербезопасности АСУ ТП кустовых площадок представлена на рисунке К.8.

Основные концепты когнитивной карты приведены в таблице К.4.

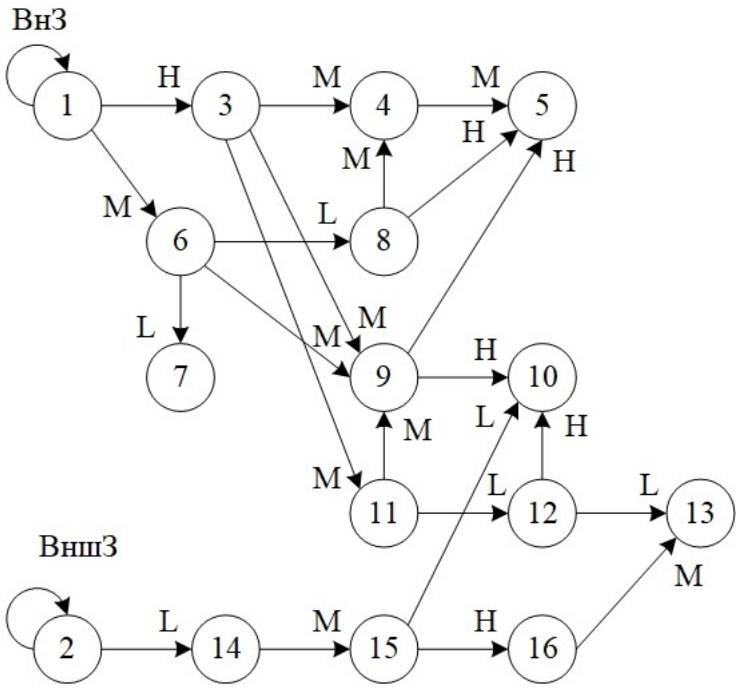


Рисунок К.8 – Когнитивная карта для оценки рисков кибербезопасности АСУ ТП

Таблица К.4 – Список концептов когнитивной карты анализа рисков кибербезопасности промышленного объекта

Концепт	Название концепта
C_1	Воздействие внутреннего злоумышленника
C_2	Воздействие внешнего злоумышленника
C_3	Физический доступ к АРМ оператора
C_4	Авторизация с правами легитимного пользователя системы
C_5	Несанкционированное управление кустовой площадкой. Целевой концепт (X_5).
C_6	Эксплуатация уязвимостей сетевого оборудования и/или ошибок конфигурации
C_7	Отказ в обслуживании сети нижнего уровня промышленного объекта. Целевой концепт (X_7).
C_8	Прослушивание сетевого трафика и перехват данных учетных записей пользователей
C_9	Изменение алгоритма управления объектами промышленной системы за счет модификации конфигурационных файлов PLC (использование протоколов HTTP + FTP)
C_{10}	Нарушение логики работы промышленного объекта. Целевой концепт (X_{10}).
C_{11}	Доступ к ОС через протоколы SSH/Telnet (эксплуатация уязвимостей удаленного доступа)

C_{12}	Эксплуатация уязвимостей датчиков сбора параметров технического объекта (-ов) и подмена конфигурационных файлов
C_{13}	Модификация актуальных параметров телеметрии (нарушение целостности). Целевой концепт (X_{13}).
C_{14}	Подмена сигнала точного времени в зоне приема антенны (GPS/ГЛОНАСС)
C_{15}	Установка некорректного времени на сервере точного времени (NTP)
C_{16}	Нарушение последовательности технологических событий, отображаемых в SCADA системе

Рассмотрим три варианта реализации НКК (обычная НКК, серая НКК и интуиционистская НКК). В таблице К.5 приведены значения весов связей между концептами, определенные экспертами.

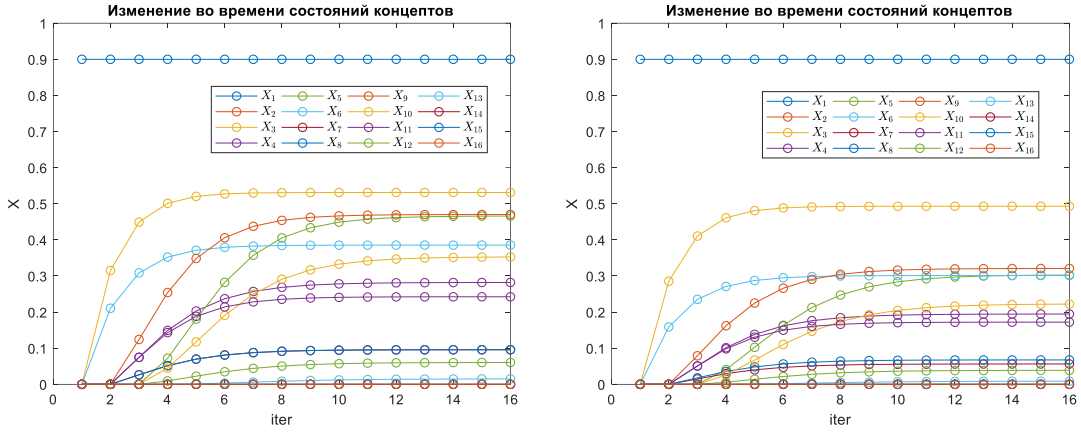
Таблица К.5 – Веса связей между концептами НКК

Вес связи $C_i \to C_j$	**Обычная НКК**	**Серая НКК**	**Интуиционистская НКК (iFCM-I)**	
W_{ij}	W_{ij}	$\left[\underline{W}_{ij}, \overline{W}_{ij}\right]$	W_{ji}^{μ}	W_{ji}^{π}
W_{11}	1	[1; 1]	1	0
W_{13}	0,725	[0,6; 0,85]	0,725	0,1
W_{16}	0,475	[0,35; 0,6]	0,475	0,25
W_{22}	1	[1; 1]	1	0
$W_{2\ 14}$	0,25	[0,15; 0,35]	0,25	0,1
W_{34}	0,475	[0,35; 0,6]	0,475	0,25
W_{39}	0,475	[0,35; 0,6]	0,475	0,25
$W_{3\ 11}$	0,475	[0,35; 0,6]	0,475	0,25
W_{45}	0,475	[0,35; 0,6]	0,475	0,25
W_{67}	0,25	[0,15; 0,35]	0,25	0,25
W_{68}	0,25	[0,15; 0,35]	0,25	0,1
W_{69}	0,475	[0,35; 0,6]	0,475	0,25
W_{84}	0,475	[0,35; 0,6]	0,475	0,25
W_{85}	0,725	[0,6; 0,85]	0,725	0,1
W_{95}	0,725	[0,6; 0,85]	0,725	0,1
$W_{9\ 10}$	0,725	[0,6; 0,85]	0,725	0,1
$W_{11\ 9}$	0,475	[0,35; 0,6]	0,475	0,25
$W_{11\ 12}$	0,25	[0,15; 0,35]	0,25	0,1
$W_{12\ 10}$	0,725	[0,6; 0,85]	0,725	0,25
$W_{12\ 13}$	0,25	[0,15; 0,35]	0,25	0,1
$W_{14\ 15}$	0,475	[0,35; 0,6]	0,475	0,25
$W_{15\ 10}$	0,25	[0,15; 0,35]	0,25	0,1
$W_{15\ 16}$	0,725	[0,6; 0,85]	0,725	0,1
$W_{16\ 13}$	0,475	[0,35; 0,6]	0,475	0,25

Рассмотрим сценарий когнитивного моделирования воздействия внутреннего злоумышленника (активация концепта-драйвера C_1), эксплуатирующего

уязвимости программных и аппаратных компонент системы, с применением указанных вариантов построения НКК.

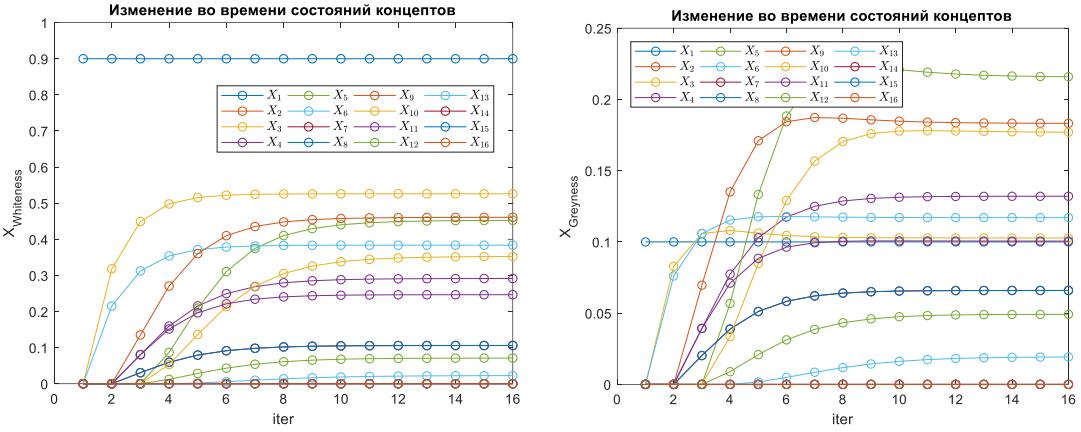
Для НКК и интуиционистской когнитивной карты изменение во времени состояний концептов приведено на рисунке К.9.



а) б)

Рисунок К.9 – Изменение во времени состояний концептов НКК (а) и ИНКК (б)

Изменение параметров состояний концептов НСКК («серость» и «белизна» оценки состояния) показаны на рис. К.10.



а) б)

Рисунок К.10 – Изменение во времени состояний концептов НСКК: (а) стабилизация «белого» значения концепта (б) стабилизация «серости» концепта

Приложение Л Акты внедрения

УТВЕРЖДАЮ
Генеральный директор
ООО «Фродекс»
_____ А.И. Луцкович
«01» 03 2022 г.

АКТ
о внедрении в ООО «Фродекс» результатов
диссертационной работы
Вульфина Алексея Михайловича
«Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных»

Комиссия в составе: Хафизова Артема Фоелевича, технический директор, Михайлова Владимира Анатольевича, руководитель проектов, Фахретдинов Руслан Маратович, Ведущий аналитик по информационной безопасности составила настоящий акт о том, что научно-технические результаты диссертационной работы А.М. Вульфина «Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных», представленной на соискание ученой степени доктора технических наук, полученные при выполнении работ с ООО «Фродекс» по договорам № 461-17 от 01.10.2017 г. и №457-18 от 01.11.2019 г., а именно:

- модели, алгоритмы и программная реализация цифрового профилирования и анализа совокупности отпечатков (fingerprints) пользовательских окружений и динамических пользовательских профилей в задаче противодействия кибермошенничеству (компонент антифрод-системы) обеспечивают точность определения удаленного управления на уровне 93 % (предложено впервые) и точность классификации мошеннических платежей на уровне 81 % (повышение эффективности на 16 % по сравнению с существующей системой) – внедрены и используются

нашей организацией при решении ряда задач, связанных с обеспечением кибербезопасности информационных систем.

Практическая ценность разработанных моделей, алгоритмов и программных средств применительно к сфере обеспечения кибербезопасности объектов финансового сектора заключается в повышении оперативности анализа динамических профилей пользователей и выявления инцидентов нарушений кибербезопасности, повышении обоснованности оценок угрозы нарушения конфиденциальности и целостности информации, а также оценок соблюдения требований политики информационной безопасности объектов КИИ.

Результаты диссертационной работы в настоящее время используются нами при выполнении ряда перспективных проектов.

Технический директор _____ / Хафизов А.Ф.

Руководитель проектов _____ / Михайлов В.А.

Ведущий аналитик по информационной безопасности _____ / Фахретдинов Р.М.

УТВЕРЖДАЮ
Директор
ООО «Инженерный центр
систем безопасности»
_____ А.И. Луцкович
«14» февраля 2022 г.

АКТ
о внедрении в ООО «Инженерный центр систем безопасности» результатов диссертационной работы
Вульфина Алексея Михайловича
«Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных»

Комиссия в составе: Луцкович Альберт Иванович, директор, Андреева Екатерина Юрьевна, Заместитель директора по ИБ, Константинов Евгений Вячеславович, Ведущий специалист отдела ИБ, составила настоящий акт о том, что следующие результаты диссертационной работы А.М. Вульфина «Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных», представленной на соискание ученой степени доктора технических наук: метод, модели, алгоритмы и программная реализация обнаружения с их помощью аномалий в накапливаемых данных мониторинга состояния сетевого окружения конечных систем информационно-телекоммуникационной инфраструктуры – используются при решении задач обеспечения информационной безопасности информационно-телекоммуникационных систем.

Практическая ценность указанных технических решений применительно к обеспечению информационной безопасности объектов информационно-телекоммуникационной инфраструктуры заключается в:

– повышении эффективности (выявление до 96 % сетевых атак в развернутом тестовом окружении) и оперативности выявления инцидентов нарушений безопасности в процессе анализа сетевого трафика в задаче обнаружения вредоносной сетевой активности;

– повышении эффективности системы корреляции событий информационной безопасности в составе Центра мониторинга и реагирования на инциденты информационной безопасности.

Директор _____ / Луцкович А.И.

Заместитель директора по ИБ _____ / Андреева Е.Ю.

Ведущий специалист _____ / Константинов Е.В.

Закрытое акционерное общество "РЕСПУБЛИКАНСКИЙ ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ"

ИНН 0274079299 КПП 027401001
р/сч 40702810510620000125
Филиал «Центральный» Банка ВТБ (ПАО) в г. Москве
к/сч 30101810145250000411 БИК 044525411

450008 г.Уфа ул. К.Маркса, 12,
корпус 5 УГАТУ, к.302
тел.:(347) 272-22-25
тел./факс:(347) 272-80-53

УТВЕРЖДАЮ
Директор
ЗАО «Республиканский центр
защиты информации»
_____ С.Н. Зарипов
«__» _____ 2022 г.

АКТ

о внедрении в ЗАО «Республиканский центр защиты информации» результатов диссертационной работы Вульфина Алексея Михайловича
«Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных»

Комиссия в составе:

1) главный инженер ЗАО «Республиканский центр защиты информации», к.т.н. Бакиров А.А.;

2) ведущий специалист ЗАО «Республиканский центр защиты информации» Федотов Д.Б.;

3) ведущий специалист ЗАО «Республиканский центр защиты информации» Кухарев С.Н.

составили настоящий акт о том, что научно-технические результаты диссертационной работы А.М. Вульфина «Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных», представленной на соискание ученой степени доктора технических наук:

- методика комплексного анализа и оценки рисков информационной безопасности (ИБ) объектов КИИ с использованием методов нечеткого когнитивного моделирования и машинного обучения;
- методика оценки актуальных угроз и уязвимостей программного обеспечения (ПО) значимых объектов КИИ с использованием технологий семантического анализа и машинного обучения

используются в проектной работе ЗАО «Республиканский центр защиты информации» (ЗАО «РЦЗИ») на этапе оценки рисков, связанных с нарушением конфиденциальности, целостности и доступности информации вследствие возможного воздействия внешних и внутренних угроз на информационные активы объектов КИИ.

Применение разработанной в диссертации методики оценки актуальных угроз и уязвимостей ПО позволяет сократить в 7-10 раз объемы просматриваемых экспертом данных и уменьшить время анализа в 10-12 раз с помощью префильтрации собираемых данных.

Результаты диссертационной работы используются нами совместно со специалистами Учебно-научного центра информационной безопасности (УНЦ ИБ) УГАТУ при проведении плановых работ по аудиту информационной безопасности объектов КИИ Республики Башкортостан.

Главный инженер ЗАО «РЦЗИ»,
к.т.н. _____ / А.А. Бакиров /

Ведущий специалист ЗАО «РЦЗИ» _____ / Д.Б. Федотов /

Ведущий специалист ЗАО «РЦЗИ» _____ / С.Н. Кухарев /

УТВЕРЖДАЮ
Генеральный директор
АО Научно-производственное
предприятие «Полигон»
_____ И.В. Селиванец
«31» 01 2022 г.

АКТ
о внедрении в АО НПП «Полигон» результатов
диссертационной работы
Вульфина Алексея Михайловича
«Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных»

Комиссия в составе: Хомского В.Н. - технического директора АО НПП «Полигон», Лелейтнера В.О. – заместителя технического директора АО НПП «Полигон» и Хомского А.Н. – технического директора ООО НИИСТИС в составе группы компаний НПП «Полигон» составила настоящий акт о том, что научно-технические результаты диссертационной работы А.М. Вульфина «Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных», представленной на соискание ученой степени доктора технических наук, а именно: алгоритмическое и программное обеспечение защиты управляющего трафика программно-определяемых сетей, используются в проводимых предприятием работах по обеспечению информационной безопасности информационно-телекоммуникационных систем, создаваемых на оборудовании, разрабатываемом и серийно выпускаемом предприятием.

Практическая ценность разработанных моделей, алгоритмического и программного обеспечения применительно к обеспечению информационной безопасности информационно-телекоммуникационной инфраструктуры

промышленных предприятий заключается в выявление до 95 % сетевых атак в развернутом тестовом окружении, что позволяет обеспечить повышение информационной безопасности в гетерогенных сетях объектов критической инфраструктуры.

Результаты диссертационной работы в настоящее время используются и запланированы к применению в рамках реализации перспективных проектов по обеспечению информационной безопасности телекоммуникационных систем общепромышленного и специального назначения.

Технический директор АО НПП «Полигон» _____ Хомский В.Н.
Зам. технического директора АО НПП «Полигон» _____ Лелейтнер В.О.
Технического директора ООО НИИСТИС _____ Хомский А.Н.

У Т В Е Р Ж Д А Ю
Директор
ООО «Уфимский НТЦ»
_____ И.З. Муллагалин
«14» февраля 2022 г.

АКТ
о внедрении в ООО «Уфимский НТЦ»
результатов диссертационной работы Вульфина Алексея Михайловича
«Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных»

Комиссия в составе: Мирянова Сергея Николаевича, руководителя департамента информационных технологий, Старцева Сергея Анатольевича, заместителя руководителя департамента информационных технологий по архитектуре составила настоящий акт о том, что научно-технические результаты диссертационной работы А.М. Вульфина «Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных», представленной на соискание ученой степени доктора технических наук, полученные в ходе реализации научно-исследовательских работ по договорам № ИФ-ТК-10-13-ХГ от 5.09.2013 г. и 01.03.2016 г., а именно:

– метод, алгоритмы и программное обеспечение для обнаружения аномалий технологических временных рядов накапливаемых параметров, характеризующих состояние сложных технических объектов нефтедобычи, на основе технологий интеллектуального анализа,

используются в ООО «Уфимский НТЦ» для мониторинга состояния оборудования АСУ ТП нефтедобычи на основе распознавания предобработанных динамограмм, характеризующих текущее состояние объектов.

Практическая ценность предложенных решений заключается в возможности обнаружения аномалий в данных мониторинга состояния АСУ ТП нефтедобычи, и возможности корректно классифицировать до 78-95 % состояний, в том числе, вызванных воздействием злоумышленника.

Результаты диссертационной работы использованы при выполнении ряда конкретных проектов для нефтедобывающих предприятий Республики Башкортостан.

Руководитель департамента информационных технологий

_____ / Мирянов С.Н.

Заместитель руководителя департамента ИТ по архитектуре

_____ / Старцев С.А.

УТВЕРЖДАЮ
Проректор по учебной работе
ФГБОУ ВО «УГАТУ»
_____ А.Н. Елизарьев
«__» _____ 2022 г.

АКТ

о внедрении результатов диссертационной работы
Вульфина Алексея Михайловича «Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных», представленной на соискание ученой степени доктора технических наук

Комиссия в составе: заведующего кафедрой вычислительной техники и защиты информации, д-р физ.-мат. наук, доцента Картака В.М., профессора кафедры вычислительной техники и защиты информации, д-р техн. наук, профессора Фрида А.И., начальника учебного управления, канд. техн. наук, доцента Рахмановой Ю.В., составила настоящий акт о том, что научно-технические результаты диссертационной работы А.М. Вульфина «Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных», представленной на соискание ученой степени доктора технических наук, а именно:

– методы, модели и алгоритмы комплексной оценки рисков ИБ объектов КИИ с использованием технологий нечеткого когнитивного моделирования и семантического анализа текстовых описаний угроз и уязвимостей программного обеспечения (ПО), используются в учебном процессе кафедры вычислительной техники и защиты информации при преподавании следующих учебных дисциплин: «Методы многомерного анализа данных в защите информации» и «Экспертные системы комплексной оценки безопасности информационно-телекоммуникационных систем» для обучающихся по направлению подготовки магистров 10.04.01 «Информационная безопасность», дисциплин «Искусственный интеллект в системах защиты информации», «Технологии обеспечения информационной безопасности» для обучающихся по направлению подготовки бакалавров, специалитета и магистров по направлению

09.04.01 «Информатика и вычислительная техника», профиль «Безопасность и защита информации»;

– проблемно-ориентированный программный комплекс «Полигон», предназначенный для имитации основных элементов информационной инфраструктуры промышленного объекта и реализующий функционал мониторинга состояния информационной и сетевой инфраструктуры на базе открытого ПО и распределенной вычислительной инфраструктуры, используется для тестирования и отладки методов, моделей и алгоритмов когнитивного моделирования и интеллектуального анализа слабоструктурированных данных, используется на кафедре вычислительной техники и защиты информации при выполнении курсовых работ и проектов, подготовке выпускных квалификационных работ по программам бакалавриата, специалитета, магистратуры, а также в исследованиях аспирантов.

Результаты диссертационной работы используются при реализации перспективных проектов, связанных с обеспечением информационной безопасности корпоративной информационной сети ФГБОУ ВО «УГАТУ» и проведением научно-исследовательских работ.

Заведующий кафедрой ВТиЗИ
д-р физ-мат. наук, профессор — В.М. Картак

Профессор кафедры ВТиЗИ
д-р техн. наук, профессор — А.И. Фрид

Начальник учебного управления
к.т.н., доцент — Ю.В. Рахманова