ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.2.427.02, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА (ДОКТОРА) НАУК

аттестационное дело № _____

решение диссертационного совета от 01.07.2022 № 5

О присуждении Вульфину Алексею Михайловичу, гражданину РФ, ученой степени доктора технических наук.

Диссертация «Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных» по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите 28.03.2022 г. (протокол № 2) диссертационным советом 24.2.427.02, созданным на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский государственный авиационный технический университет» Министерства науки и высшего образования Российской Федерации, 450008, г. Уфа, ул. К. Маркса, 12, приказом Министерства науки и высшего образования № 43/нк от 30.01.2019 г.

Соискатель Вульфин Алексей Михайлович «21» апреля 1986 года рождения **диссертацию** на соискание ученой степени кандидата технических наук «Алгоритмы обработки информации для диагностирования инженерной сети нефтедобывающего предприятия с интеллектуальной поддержкой принятия решений» защитил в 2012 году, в диссертационном совете, созданном на базе государственного образовательного учреждения высшего профессионального образования «Уфимский государственный авиационный технический

университет» после окончания аспирантуры в 2011 году в государственном образовательном учреждении высшего профессионального образования «Уфимский государственный авиационный технический университет», работает доцентом на кафедре вычислительной техники и защиты информации Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский государственный авиационный технический университет» Министерства науки и высшего образования Российской Федерации.

Диссертация выполнена на кафедре вычислительной техники и защиты информации Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский государственный авиационный технический университет» Министерства науки и высшего образования Российской Федерации.

Научный консультант – доктор технических наук, профессор, Васильев Владимир Иванович, Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет», профессор кафедры вычислительной техники и защиты информации.

Официальные оппоненты:

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

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

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

дали положительные отзывы на диссертацию.

Ведущая организация Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург, в своем положительном заключении, подписанным заведующим кафедрой вычислительной техники и защиты информации, доктором технических наук, профессором Аралбаевым Ташбулатом Захаровичем, утвержденном проректором по научной работе, доктором физико-математических наук, профессором Летута Сергеем Николаевичем, указала, что диссертация Вульфина Алексея Михайловича на соискание ученой степени доктора технических наук является завершенной научно-квалификационной работой, в которой на основании выполненных автором исследований разработаны научно-обоснованные технические и технологические решения, направленные на решение актуальной проблемы разработки моделей и методов комплексной оценки рисков информационной безопасности объектов КИИ с использованием методов и технологий интеллектуального анализа данных, внедрение которых вносит значительный вклад в развитие страны. Диссертация соответствует требованиям п.9 «Положения о присуждении ученых степеней», а ее автор – Вульфин Алексей Михайлович – заслуживает присуждения ему ученой степени доктора технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Диссертация обладает внутренним единством, содержит новые научные результаты и положения. Автореферат диссертации соответствует содержанию диссертации по основным квалификационным признакам: цели, задачам, новизне, актуальности, достоверности, научной и практической значимости. Количество публикаций, в которых излагаются основные научные результаты диссертации на соискание ученой степени доктора наук достаточное. Тема и содержание диссертации соответствуют специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Соискатель имеет более 100 опубликованных работ, по проблеме диссертационного исследования опубликовано 74 работы, в том числе: 24 статьи в ведущих рецензируемых научных журналах, входящих в перечень изданий,

рекомендованных ВАК, 19 публикаций в отечественных и зарубежных изданиях, индексируемых международными системами Scopus и Web of Science (из них, 2 – Q2); 2 коллективные монографии, изданные в России и за рубежом, 1 патент на изобретение; 17 свидетельств о государственной регистрации программы для ЭВМ, 11 трудах конференций и других работах. 6 публикаций выполнены соискателем единолично, остальные – при непосредственном участии соискателя.

Наиболее значимые работы по теме диссертации:

1. 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. **2.** 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. **3.** 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. **4.** 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. **5.** 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. **6.** 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. **7.** 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. **8.** 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. **9.** 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. **10.** 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. **11.** 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. **12.** Вульфин А.М. Система управления данными кибербразведки [Электронный ресурс] // Моделирование, оптимизация и информационные технологии. – 2021. – № 9(1). – С. 1–18. – Режим доступа: https://moitvivt.ru/ru/journal/pdf?id=925 **13.** 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. **14.** 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.

На диссертацию и автореферат поступили **положительные** отзывы:

– **ведущей организации *ФГБОУ ВО «Оренбургский государственный университет»*** *Замечания*: **1.** Одной из особенностей концепции исследований работы является разработка комплексного подхода к исследованию рисков. Комплексность предполагает наличие некоторой совокупности объектов. Из текста диссертации не ясно, в какой мере является полным и достаточным множество предлагаемых моделей, методов и алгоритмов для обеспечения требуемой безопасности объектов информатизации. **2.** Объектом исследования является многоуровневая распределенная информационно-управляющая система. Структура

таких систем предполагает иерархический характер рисков. Из текста диссертации неясно, каким образом предполагается применить предложенный автором подход для построения систем защиты информации с учетом совмещенности рисков нижнего и верхнего уровня. **3.** Предложенный автором подход универсален, автором предложен целый ряд аспектов по его применению. В связи этим было бы целесообразным обобщить направления эффективного приложения результатов исследований, например, к задачам оценки, прогнозирования и принятия решений по минимизации временных и стоимостных затрат на построение систем защиты с учетом комплексного анализа рисков ИБ. **4.** В описании результатов исследования автор не всегда использует достаточно привычную для ИБ терминологию, в частности, «остаточные и приемлемые риски, модели угроз», по тексту автореферата имеются отдельные неточности в определении выводов, например (стр.7 автореферата), «Применение модели оценки степени опасности новых уязвимостей на основе прогнозирования набора метрик позволяет получить оценку степени их опасности (и набора ее метрик)», что в некоторых случаях затрудняет восприятие результатов. **5.** Из работы не вполне ясно, как оценивалась достоверность полученных оценок рисков ИБ объектов КИИ с учетом разброса исходных экспертных оценок.

– **официального оппонента** доктор технических наук, профессор Ажмухамедова Искандара Маратовича, декана факультета цифровых технологий и кибербезопасности ФГБОУ ВО «Астраханский государственный университет», г. Астрахань. *Замечания*: **1.** Первая глава диссертации недостаточно раскрывает проблемную ситуацию с точки зрения анализа сложных систем: для динамически изменяющейся среды функционирования объекта КИИ, открытых систем и постоянно возникающих угроз. С этой точки зрения, требуется создание не отдельных фрагментарных механизмов и инструментов, а создание комплексных систем обеспечения ИБ. **2.** В обзоре публикаций уделено недостаточное внимание существующим системам поддержки принятия решений в задачах оценки рисков ИБ. **3.** Отсутствует обоснование используемых для анализа данных в главе 1 методов Doc2Vec и Word2Vec. Хотя, например, в работе «Сравнение эффективности методов векторного представления слов для определения тональности текстов»

(http://msm.omsu.ru/jrns/jrn52/lychenko.pdf) указывалось, что «…классические методы, в частности метод латентно семантического анализа LSA, могут быть более полезными, чем Word2Vec. Это объясняется тем, что Word2Vec учится на низкоразмерных векторах с начала обучения и не использует всю информацию из учебного корпуса слов. Также доказано, что LSA более устойчив и не сильно зависит от размера корпуса.». **4.** В главе 2 приведено недостаточно подробное описание предложенного комплекса моделей анализа поведения пользователей конечной системы: при описании моделей использовано очень мало формул. Не очевидно, как происходит взаимодействие между блоками моделей. Для части формулировок моделей даны только определения. Это не позволяет в полной мере оценить его оригинальность и значимость для оценки рисков ИБ объекта КИИ. **5.** Не приведены оценки робастности (меры достоверности) предлагаемых интервальных оценок рисков ИБ, полученных с помощью иерархических нечетких когнитивных карт. **6.** Не рассмотрены особенности технической реализации разработанных алгоритмов в виде программно-аппаратных средств, нет рекомендаций по их применению и оценки требуемых экономических затрат при решении конкретных задач.

– **официального оппонента** доктора технических наук, доцента Катасёва Алексея Сергеевича, профессора кафедры систем информационной безопасности ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ», г. Казань. *Замечания*: **1.** В явном виде не сформулирована решаемая в диссертации научно-техническая проблема. При этом на ее формулировку косвенно указывает первая задача диссертационного исследования, посвященная системному анализу проблемы комплексной оценки рисков информационной безопасности объектов КИИ. Кроме того, в заключении сказано, что в ходе диссертационного исследования разработаны научно обоснованные технические и технологические решения, направленные на решение проблемы разработки моделей и методов комплексной оценки рисков информационной безопасности объектов КИИ на основе методов и технологий интеллектуального анализа данных. В первом случае внимание акцентируется на проблеме комплексной оценки рисков информационной безопасности, а во втором – на проблеме разработки моделей и методов комплексной

оценки рисков информационной безопасности. В диссертации желательно было бы привести однозначную ее формулировку. **2.** Шестая задача диссертационного исследования сформулирована как «Разработка архитектуры исследовательского прототипа интеллектуальной системы поддержки принятия решений…». Хотя фактически в диссертации разработан и программно реализован полноценный прототип системы, а не только его архитектура. В этом смысле задача сформулирована более узко, чем ее фактическое решение. Поэтому слово «архитектура», скорее всего, является лишним. **3.** В первой главе диссертации приведен обзор существующих решений, основанных на применении методов интеллектуального анализа данных и когнитивного моделирования для оценки рисков ИБ информационных систем. При этом не в полной мере раскрыты вопросы критического анализа применимости указанных методов для объектов КИИ с учетом специфики, отраженной в существующих нормативно-правовых документах. **4.** В диссертации используется большое количество терминов и обозначений. При этом часть терминов, в частности, при обозначении алгоритмов классификации и обнаружения аномалий, в тексте представлены без соответствующего русскоязычного варианта, что затрудняет анализ промежуточных результатов. **5.** Не все используемые в диссертационной работе аббревиатуры вынесены в список сокращений и условных обозначений. В частности, это касается аббревиатуры ИТКС (информационно-телекоммуникационная система). При этом аббревиатура НКК (нечеткая когнитивная карта) присутствует в этом списке дважды. **6.** Многие рисунки в автореферате диссертации, например, 3, 4, 5, 7, 15, 20 - плохо читабельные, что затрудняет их понимание и интерпретацию. В частности, на рисунке 20 практически невозможно разобрать текст. При подготовке автореферата автору следовало бы обратить на это внимание.

– **официального оппонента** доктора технических наук, профессора **Шелупанова Александра Александровича**, президента ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники», г. Томск. *Замечания*: **1.** В диссертации не нашли отражения организационные аспекты процедуры комплексной оценки рисков ИБ объектов КИИ. **2.** Не уделено внимания

построению моделей внешнего и внутреннего злоумышленника, что, безусловно, должно учитываться при определении актуальных угроз и степени опасности уязвимостей объектов КИИ. Отсутствие таких моделей может поставить под сомнение сам подход к комплексной оценке рисков и по сути, снижает востребованность предложенной автором концепции комплексной оценки рисков ИБ объектов КИИ. **3.** Приведенное на стр.47 диссертации определение риска ИБ имеет отличия от соответствующего определения риска, приведенного в Глоссарии в конце диссертации (Приложение 1). **4.** Неясно, каковы ограничения области применения предложенных в работе методов и алгоритмов комплексной оценки рисков ИБ объектов КИИ (классы объектов, специфика информационной инфраструктуры, состав ее программного и аппаратного обеспечения, характер информационных потоков в организации и т.п.). Не определены они и в тексте диссертации. Это вызывает закономерный вопрос, связанный с глубиной проработки предложенных методов. **5.** Диссертация (так же, как и автореферат) в значительной степени перегружена рисунками, что, с одной стороны, несомненно, повышает наглядность изложения, но, с другой стороны, приведенные рисунки местами имеют мелкий масштаб и содержат большое число обозначений и сокращений (аббревиатур), что затрудняет рассмотрение. Некоторые рисунки представляются излишними. Например, вызывает сомнение оригинальность предложенного конвейера обработки текстовых описаний (рис.8 автореферата). Кроме того, рисунки и схемы выполнены с нарушениями требований ЕСПД и ГОСТ. **6.** В работе не указаны заявленные методы системного анализа, которые использовались автором при исследованиях.

Получено 9 положительных отзывов на автореферат:

1. ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», заведующий кафедрой информационной безопасности, д.т.н., профессор **Карташевский Вячеслав Григорьевич**. *Замечания*: недостаточные пояснения к рисункам и диаграммам, в частности при расшифровке обозначений и терминов, что, впрочем, можно объяснить ограниченным объемом автореферата.

2. ФГАОУ ВО «Пермский национальный исследовательский политехнический университет», заведующий кафедрой «Автоматика и телемеханика», д.т.н., профессор **Южаков Александр Анатольевич**. Замечания: *в формулировках научной новизны недостаточно четко отражен предлагаемый в работе подход к обеспечению динамического конфигурирования моделей комплексной оценки рисков ИБ, с учетом непрерывно изменяющегося состояния распределенных иерархически организованных информационно-телекоммуникационных систем.*

3. ФГАОУ ВО «Омский государственный технический университет», заведующий кафедрой «Комплексная защита информации», д.т.н., доцент **Ложников Павел Сергеевич**. *Замечания*: недостаточное внимание, уделенное анализу согласованности экспертных оценок при оценке достоверности результатов когнитивного моделирования, и отсутствие рекомендаций для учета степени их разброса.

4. ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ», Заместитель заведующего кафедрой 44, профессор отделения Интеллектуальных кибернетических систем офиса образовательных программ, д.т.н., доцент **Милославская Наталья Георгиевна**. *Замечания*: в автореферате не в полной мере раскрыто понятие «аномалия» при анализе многомерных временных рядов параметров мониторинга состояния АСУ ТП нефтедобычи.

5. ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С.П. Королева», профессор кафедры безопасности информационных систем, **д.ф.-м.н., профессор Новиков Сергей Яковлевич;** доцент кафедры безопасности информационных систем, **к.т.н., доцент Бурлаков Михаил Евгеньевич**. *Замечания*: не приведена классификация аномалий состояния объектов КИИ, пользователей конечных систем и пользовательского окружения; на рисунке 4 часть обозначений не раскрыты, что снижает его информативность.

6. ФГБОУ ВО «Башкирский государственный университет» (заведующий кафедрой Управления информационной безопасностью, **д.ф.-м.н., доцент**

Исмагилова Альбина Сабирьяновна. *Замечания*: в автореферате не приводятся оценки производительности и необходимых вычислительных ресурсов для развертывания разработанной системы поддержки принятия решений.

7. ФГАОУ ВО «Южно-Уральский государственный университет, национальный исследовательский университет)», заведующий кафедрой защиты информации Высшей школы электроники и компьютерных наук, **к.т.н., доцент Соколов Александр Николаевич**. *Замечания*: из текста автореферата не ясно, какова связь оценки риска, обозначенной как R_i на стр. 11, и моделями-регрессорами оценки степени опасности с теми же обозначениями R_i на рис. 2 (стр. 13)? Из описаний ориентированных графов G на стр. 13 и НКК на стр. 15 не ясно, какие вершины графов соединяются ребрами и каким образом определяются направления ребер? На стр. 15 сказано, что комплекс моделей анализа аномалий в поведении пользователей конечной системы разработан с целью оценки угрозы нарушения конфиденциальности и целостности информации. Как в этом случае оцениваются угрозы нарушения доступности? При описании графа НКК на стр. 15 используется кортеж множеств <C, F, W>, но далее речь ведется об элементах $X_i(t)$. Множество этих элементов, видимо, тоже нужно включить в этот кортеж. В формуле (2) на стр. 16 для $X_i(t)$ – значения переменной состояния i-го концепта C_i используется обозначение $X_i(t)$ (с волной). Это же происходит и с переменными W_{ij} – в определении они без волны, а в формуле с волной. Чем обусловлена разность в обозначениях? При пояснении формулы (2) на стр. 16 автор говорит о весах связей W_i. Видимо, речь идет о W_{ji}.

8. ФГБОУ ВО «Ульяновский государственный технический университет», ректор, **д.т.н., профессор Ярушкина Надежда Глебовна**. *Замечания*: не вполне ясен механизм построения и работы ансамбля нечетких когнитивных моделей при оценке рисков ИБ. При описании предложенной методики количественной оценки рисков ИБ в задаче обеспечения целостности телеметрической информации не приведено описание выделенных зон и трактов безопасности (рисунок 14).

9. ФГБОУ ВО «Воронежский государственный технический университет», заведующий кафедрой систем информационной безопасности, д.т.н., профессор **Остапенко Александр Григорьевич**. *Замечания*: недостаточно ясно, учитывалась ли хаотичность временного ряда в модели обнаружения аномалий состояния объектов и сущностей в зоне анализируемого объекта КИИ. На рис.4 стр. 15 автореферата приведена модель обнаружения аномалий состояния подсистем в зоне объекта КИИ. В схеме присутствует модуль кластерного анализа вектора признаков состояния объекта. Однако, из текста автореферата недостаточно ясно, какие именно методы кластеризации использует автор.

Выбор официальных оппонентов и ведущей организации обосновывается их достижениями в данной отрасли наук, наличием публикаций в соответствующей сфере исследования и способностью определить научную и практическую ценность диссертации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

– **разработана** концепция комплексной оценки рисков информационной безопасности (ИБ) объектов критической информационной инфраструктуры (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 влияние факторов неопределенности;

– **предложен** оригинальный подход к количественной оценке рисков ИБ объектов КИИ, основанный на построении иерархии вложенных когнитивных карт, с учетом структурно-функциональной организации объекта КИИ, отличающийся применением технологий интеллектуального анализа слабоструктурированных данных мониторинга состояния объекта и данных из внешних источников, что позволяет повысить достоверность итоговых количественных оценок рисков нарушения ИБ;

– **доказана** перспективность применения методов интеллектуального анализа данных в задачах комплексной оценки рисков ИБ объектов КИИ с целью повышения оперативности и достоверности результатов с учетом 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;

– **введен** комплекс проблемно-ориентированных моделей параметризации угроз и уязвимостей объектов КИИ, основанных на использовании технологий интеллектуального анализа текстовых данных и обнаружения аномалий в накапливаемых данных мониторинга их состояния, отличающийся применением и организацией ансамбля гетерогенных моделей машинного обучения при оценке опасности уязвимостей и построении детекторов аномалий, что позволяет снизить трудоемкость и автоматизировать низкоуровневое моделирование сценариев эксплуатации уязвимостей и реализации угроз.

Теоретическая значимость исследования обоснована тем, что:

– **доказана** целесообразность оценки рисков ИБ объектов КИИ на основе применения предложенных моделей, методов и алгоритмов интеллектуального анализа многомерных временных рядов накапливаемых параметров, характеризующих состояние этих объектов, сетевого трафика промышленных сетей и поведения пользователей конечных систем, что позволяет повысить достоверность и оперативность поиска скрытых зависимостей в накапливаемых данных, и в целом результатов оценивания рисков ИБ с помощью инструментов когнитивного моделирования за счет уточнения априорных оценок вероятностей реализации угроз и эксплуатации уязвимостей;

– применительно к проблематике диссертации результативно **использован** комплекс существующих базовых методов, в том числе методов системного анализа, когнитивного моделирования; семантического анализа, нейросетевого моделирования и машинного обучения; методы оценки рисков ИБ и обнаружения аномалий временных рядов;

– **изложены** аргументы и факты, доказывающие, что разработка и совершенствование моделей, методов и средств комплексной оценки рисков ИБ на основе интеллектуального анализа слабоструктурированных данных для обеспечения устойчивости работы объектов КИИ на всех уровнях информационного пространства является актуальной научно-технической проблемой;

– **раскрыты** противоречия, возникающие при использовании традиционных моделей, методов и инструментальных средств поддержки принятия решений при анализе и управлении рисками ИБ, направленных, как правило, на решение частных слабо связанных между собой задач защиты информации, что затрудняет их применение для обеспечения ИБ современных высокотехнологичных объектов КИИ;

– **изучены** основные факторы, влияющие на безопасность киберфизических объектов и систем в пределах единой информационной среды (киберпространства) и оценку потенциального ущерба (последствий) для этих объектов и систем;

– **проведена** модернизация существующих подходов к комплексной оценке рисков ИБ объектов КИИ, заключающаяся в интеграции технологий нечеткого когнитивного моделирования и методов машинного обучения, а также разработке комплекса проблемно-ориентированных моделей, методов и алгоритмов комплексной оценки рисков ИБ объектов КИИ, обеспечивающих на основе информации, получаемой в процессе мониторинга состояния объекта поддержку принятия управленческих решений по обеспечению ИБ.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

– **разработаны и внедрены** в ООО «Фродекс», ООО «Инженерный центр систем безопасности», ОАО НПП «Полигон», ЗАО «Республиканский центр защиты информации», ООО «Уфимский научно-технический центр», ФГБОУ ВО «УГАТУ» результаты диссертационной работы, в том числе:

– в проектной работе на этапе оценки рисков, связанных с нарушением конфиденциальности, целостности и доступности информации вследствие возможного воздействия внешних и внутренних угроз на информационные активы объектов КИИ – методика комплексного анализа и оценки рисков информационной безопасности (ИБ) объектов КИИ с использованием методов нечеткого когнитивного моделирования и машинного обучения и методика оценки актуальных угроз и уязвимостей программного обеспечения (ПО) значимых объектов КИИ с использованием технологий семантического анализа и машинного обучения;

– при решении задач обеспечения информационной безопасности информационно-телекоммуникационных систем – метод, модели, алгоритмы и программная реализация обнаружения с их помощью аномалий в накапливаемых данных мониторинга состояния сетевого окружения конечных систем информационно-телекоммуникационной инфраструктуры; алгоритмическое и программное обеспечение защиты управляющего трафика программно-определяемых сетей;

– в задачах мониторинга состояния оборудования АСУ ТП – метод, алгоритмы и программное обеспечение для обнаружения аномалий технологических временных рядов накапливаемых параметров, характеризующих состояние сложных технических объектов нефтедобычи, на основе технологий интеллектуального анализа;

– при решении задач, связанных с обеспечением кибербезопасности информационных систем – 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);

– в ФГБОУ ВО «Уфимский государственный авиационный технический университет» при реализации перспективных проектов, связанных с обеспечением информационной безопасности корпоративной информационной сети вуза, проведением научно-исследовательских работ и учебного процесса –

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); проблемно-ориентированный программный комплекс «Полигон»;

– **определены** перспективы практического использования полученных теоретических и практических результатов в задачах комплексной оценки рисков ИБ многоуровневых распределенных информационно-управляющих систем (объектов КИИ);

– **создан исследовательский прототип** интеллектуальной системы поддержки принятия решений (ИСППР) по оценке рисков ИБ объектов КИИ, реализующий разработанный комплекс проблемно-ориентированных моделей, методов и алгоритмов комплексной оценки рисков ИБ объектов КИИ, применение которого позволяет повысить оперативность и достоверность результатов оценивания рисков ИБ и снизить эффект неопределенности от влияния субъективных факторов (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 %;

– **представлены** предложения по дальнейшему развитию полученных результатов, направленные на совершенствование технологий интеллектуального анализа текстовых описаний угроз и уязвимостей на основе нейросетевых моделей трансформеров, что позволит использовать мультиязычные базы знаний для сопоставления угроз, уязвимостей и сценариев их эксплуатации и дополнительно повысить достоверность оценок рисков ИБ объектов КИИ.

Оценка достоверности результатов исследования выявила:

– **теоретическая часть работы** базируется на известных, проверяемых и апробированных данных, фактах и согласуется с опубликованными ранее работами других авторов, а также экспериментальными данными как по теме диссертации, так и по смежным отраслям знаний;

– **идея базируется** на анализе и обобщении передового опыта, накопленного в процессе комплексирования и адаптации методов интеллектуального анализа данных и технологий когнитивного моделирования в задачах оценки рисков ИБ многоуровневых распределенных информационно-управляющих систем;

– **использовалось** сравнение авторских данных и данных, полученных ранее по рассматриваемой и смежным с ней тематикам, а также сравнение полученных результатов с решениями, предлагаемыми экспертными группами в рассматриваемой предметной области;

– **установлено** качественное и количественное совпадение авторских результатов с результатами, представленными в независимых источниках, в задачах цифрового профилирования и аномалий сетевого трафика в гетерогенных промышленных сетях, обнаружения аномалий в данных мониторинга состояния АСУ ТП объекта нефтедобычи.

Личный вклад соискателя состоит в планировании, постановке и анализе результатов эксперимента, получении и интерпретации результатов на различных этапах и уровнях обработки эмпирических и теоретических данных, а также в

выдвижении, формулировании и представлении основополагающих идей диссертационной работы, подготовке основных публикаций по выполненной работе.

Диссертационный совет пришел к выводу о том, что в диссертации:

– соблюдены установленные Положением о присуждении ученых степеней критерии, которым должна отвечать диссертация на соискание ученой степени доктора технических наук;

– отсутствуют недостоверные сведения об опубликованных соискателем ученой степени работах, в которых изложены основные научные результаты диссертации;

– соискатель ссылается на авторов и источники заимствования;

– оригинальность диссертационной работы составляет 92,47 %.

В ходе защиты диссертации критических замечаний высказано не было.

Соискатель Вульфин А.М. ответил на задаваемые ему в ходе заседания вопросы и привел собственную аргументацию при ответе на все вопросы.

Диссертационная работа Вульфина Алексея Михайловича «Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных» соответствует п. 9-11, 13, 14 Положения о присуждении ученых степеней (утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 года №842, в редакции с изменениями, утв. Постановлением Правительства РФ от 07.06.2021), предъявляемых к докторским диссертациям. Тема работы и содержание исследований соответствуют научной специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

На заседании 01.07.2022 г. диссертационный совет принял решение

– за решение научной проблемы комплексной оценки рисков информационной безопасности объектов критической информационной инфраструктуры на основе методов и технологий интеллектуального анализа данных, имеющей важное хозяйственное значение

присудить Вульфину А.М. ученую степень доктора технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

При проведении тайного голосования диссертационный совет в количестве 19 человек, из них 8 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 20 человек, входящих в состав совета, проголосовали: за – 19, против – 0, недействительных – 0.

Председатель
диссертационного совета
д-р техн. наук, профессор Султанов Альберт Ханович

Ученый секретарь
диссертационного совета
д-р техн. наук, доцент Виноградова Ирина Леонидовна

01 июля 2022 года