ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.2.479.07 НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 22.09.2023 № 11

О присуждении Кучкаровой Наиле Вакилевне, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов» по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите 03.07.2023 г., протокол № 8 диссертационным советом 24.2.479.07 на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий» Министерства науки и высшего образования Российской Федерации, 450008, г. Уфа, ул. К. Маркса, 12, созданным приказом Министерства науки и высшего образования Российской Федерации № 542/нк от 24.03.2023 г.

Соискатель Кучкарова Наиля Вакилевна, 29.01.1978 года рождения, работает старшим преподавателем кафедры вычислительной техники и защиты информации ФГБОУ ВО «Уфимский университет науки и технологий» Министерства науки и высшего образования Российской Федерации.

В 2020 г. окончила магистратуру ФГБОУ ВО «Уфимский государственный авиационный технический университет» по направлению подготовки 09.04.01

«Информатика и вычислительная техника», профиль «Безопасность, защита информации».

Приказом № 0034-А от 14.06.2022 г. зачислена в качестве экстерна для прохождения промежуточной аттестации; справка со сведениями о сданных кандидатских экзаменах выдана в 2023 г. ФГБОУ ВО «Уфимский университет науки и технологий».

Диссертация выполнена на кафедре вычислительной техники и защиты информации ФГБОУ ВО «Уфимский университет науки и технологий».

Научный руководитель – доктор технических наук, профессор Васильев Владимир Иванович, ФГБОУ ВО «Уфимский университет науки и технологий», профессор кафедры вычислительной техники и защиты информации.

Официальные оппоненты:

1. Доктор технических наук, профессор Болодурина Ирина Павловна, заведующий кафедрой прикладной математики ФГБОУ ВО «Оренбургский государственный университет»;

2. Кандидат технических наук, доцент Макарян Александр Самвелович, заведующий кафедрой кибербезопасности и защиты информации ФГБОУ ВО «Кубанский государственный технологический университет»

дали положительные отзывы на диссертацию.

Ведущая организация – Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет», г. Ставрополь, в своем положительном заключении, подписанном заведующим кафедрой организации и технологии защиты информации, и.о. директора Института цифрового развития, кандидатом технических наук, доцентом Петренко Вячеславом Ивановичем, заведующим кафедрой компьютерной безопасности, доктором физико-математических наук, доцентом Тебуевой Фаризой Биляловной и утвержденном проректором по научной и исследовательской работе, кандидатом физико-математических наук, доцентом Алихановым Анатолием Алиевичем, указала, что диссертация Кучкаровой Наили Вакилевны на соискание ученой степени кандидата

технических наук является законченной научно-квалификационной работой, в которой на основании выполненных исследований решена задача разработки метода, алгоритмов и инструментальных средств автоматизации оценки актуальных угроз безопасности информации (БИ) и уязвимостей программного обеспечения (ПО) объектов критической информационной инфраструктуры (КИИ) с использованием технологий интеллектуального анализа текстов, результаты которой обладают научной новизной и практической ценностью.

Диссертация соответствует требованиям пунктов 9, 10, 11, 13, 14 Положения ВАК о порядке присуждения ученых степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г. (с последующими изменениями), а её автор – Кучкарова Наиля Вакилевна – заслуживает присуждения ей ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 14 опубликованных работ по теме диссертации, в том числе 4 статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, либо в научных изданиях, индексируемых базой данных RSCI, 8 статей в других изданиях, получено 2 свидетельства о государственной регистрации программ для ЭВМ. 2 публикации выполнены соискателем единолично, остальные – при непосредственном участии соискателя.

Общий объем публикаций – 5,032 п.л., авторский вклад – 2,147 п.л.

Наиболее значимые работы по теме диссертации:

1. 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.

2. Васильев В.И., Вульфин А.М., Кучкарова Н.В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining //Системы управления, связи и безопасности. – 2021. – № 3. – С. 110-134.

3. Васильев В.И., Вульфин А. М., Кучкарова Н. В. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров //Вопросы кибербезопасности. – 2022. – № 2 (48). – С. 27-38.

4. Васильев В.И., Вульфин А.М., Кучкарова Н.В. Тематическое моделирование и суммаризация текстов в области кибербезопасности // Вопросы кибербезопасности. – 2023. – № 2(54). – С. 2-22.

5. Кучкарова Н. В. Исследование возможности использования кластерного анализа данных при оценке сценариев реализации угроз безопасности // Мавлютовские чтения. Уфа.– 2021. – С. 436-440.

6. Кучкарова Н.В. Применение моделей интеллектуального анализа текстов при оценке угроз информационной безопасности // Сборник статей по материалам VI Международной научно-практической конференции «Современные проблемы цивилизации и устойчивого развития в информационном обществе». – М: ИРОК, 2021. – С.178-184.

В диссертации отсутствуют недостоверные сведения об опубликованных соискателем ученой степени работах.

На диссертацию и автореферат поступили положительные отзывы, в которых содержится ряд замечаний:

– **ведущей организации** ФГАОУ ВО «Северо-Кавказский федеральный университет». *Замечания*: **1.** Во второй главе рассмотрены различные методы и алгоритмы кластеризации текстов применительно к задачам классификации (тематического моделирования) профильных научных статей в области ИБ. Несомненно, результаты проведенных при этом экспериментов позволили автору выделить ряд наиболее эффективных методов обработки естественного языка. Но хотелось бы видеть более четкие выводы, каким конкретно методам и почему будет предпочтение в последующих главах работы; **2.** Было бы интересно рассмотреть особенности решения задачи суммаризации (реферирования) текстов на примере текстовых описаний угроз БИ и уязвимостей, заимствованных из БДУ ФСТЭК России; **3.** В представленных в 3-й главе функциональных моделях IDEF0 процесса оценки и анализа актуальных УБИ в соответствии с Методикой ФСТЭК России

(рисунки 3.1-3.3) не указаны точки зрения, относительно которых рассматривались представленные модели; на рисунке 3.3 не показаны все стрелки, обозначающие «механизмы»; **4.** Не указаны ограничения на область применения предложенного в 3-й главе метода и алгоритмов определения релевантных угроз БИ для выявленных уязвимостей ПО объекта КИИ (для каких классов объектов КИИ это относится прежде всего); **5.** В явном виде не указаны требуемые вычислительные ресурсы, необходимые для реализации предложенного в работе исследовательского прототипа ИСППР; **6.** Хотелось бы видеть больше примеров построения сценариев реализации угроз БИ для конкретного объекта КИИ, с комментариями степени успешности (опасности) их реализации и выбором контрмер по парированию их последствий;

– **официального оппонента**, доктора технических наук, профессора Болодуриной Ирины Павловны, заведующего кафедрой прикладной математики ФГБОУ ВО «Оренбургский государственный университет». *Замечания*: **1.** В работе приводятся результаты экспериментов по классификации и суммаризации текстовых данных, где для формирования корпуса текстов используются полнотекстовые научные статьи, опубликованные в журнале «Вопросы кибербезопасности». Для более полного раскрытия темы исследований, а также с целью выявления новых типов угроз БИ и уязвимостей ПО, не представленных в рассмотренных источниках информации, рекомендуется использовать дополнительно информацию, размещаемую в открытых реестрах и классификациях уязвимостей ИБ.; **2.** В работе не представлено описание способа определения меры семантической близости текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник реализации угроз БИ на английском (для данных из CVE, CAPEC) и русском (для данных из БДУ ФСТЭК России) языках; **3.** Не получил должного освещения вопрос о выборе метода векторизации текстов (Word2Vec, Doc2Vec, GloVe, Fast Text, USE, BERT), хотя от выбора этого метода во многом зависит решение задачи кластеризации и других поставленных в работе задач; **4.** Не вполне ясно, как должна оцениваться достоверность решений по

оценке актуальных угроз БИ объектов КИИ, принимаемых с помощью разработанной ИСППР;

– **официального оппонента,** кандидата технических наук, доцента Макаряна Александра Самвеловича, заведующего кафедрой кибербезопасности и защиты информации ФГБОУ ВО «Кубанский государственный технологический университет». *Замечания*: **1.** В первой главе (п.1.4) можно было более подробно остановиться на вопросе о выборе косинус-меры для определения семантической близости текстовых описаний; **2.** Вообще говоря, для более точного определения актуальных угроз БИ для конкретного рассмотренного в работе примера целесообразно было бы использовать не только данные БДУ ФСТЭК, но и открытые зарубежные базы данных; **3.** В таблице 4.12 главы 4 следовало указать, в чем выражается оценка несоответствия выданных ИСППР результатов мнению эксперта (специалиста по ИБ); **4.** Не вполне ясны ограничения на область применения предложенных решений (метод, алгоритмы, инструментальные средства); **5.** Целесообразно было бы указать более четкие формулировки относительно необходимой аппаратной платформы, объема вычислительных ресурсов и трудозатрат, квалификации пользователя и т.п., требуемых для развертывания и сопровождения разработанной ИСППР; **6.** Возможно, в 4-й главе следовало привести какие-то дополнительные данные, отражающие экономическую эффективность предложенных автором решений.

Получено 8 положительных отзывов на автореферат:

– ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники», президент, **д.т.н., профессор Шелупанов Александр Александрович,** доцент кафедры комплексной информационной безопасности электронно-вычислительных систем, **к.т.н., доцент Новохрестов Алексей Константинович**. *Замечания*: неясно, каким образом были получены численные оценки временных затрат, связанных с применением предложенных автором алгоритмов и инструментальных средств оценки актуальных угроз БИ:

- так, на стр.5 (в разделе «Практическая значимость») утверждается, что «применение предложенных в работе решений позволяет сократить временные затраты на 40-50%»;

- на стр.92 указано, что «финальная стадия анализа позволяет сократить количество просматриваемых экспертом угроз БИ для каждой отдельной уязвимости ПО более чем в 10-15 раз»;

– ФГБОУ ВО «Челябинский государственный университет», заведующий научно-исследовательской лабораторией «Интеллектуальные информационные технологии и системы», **д.т.н., профессор Вохминцев Александр Владиславович**. *Замечания*: **1.** В 3-й главе при формировании корпуса текстов использовались текстовые описания угроз БИ и уязвимостей ПО, представленные в БДУ ФСТЭК России; при этом не совсем понятно, каким образом были получены текстовые описания тактик и техник реализации угроз БИ; **2.** В автореферате упоминается о разработке алгоритмов векторизации и кластеризации текстовых данных, однако, поскольку они не представлены в тексте, то не совсем понятно, каким образом происходит предварительная обработка текстовых описаний;

– ФГАОУ ВО «Омский государственный технический университет», заведующий кафедрой комплексной защиты информации, **д.т.н., профессор Ложников Павел Сергеевич**. *Замечание*: в автореферате не представлен алгоритм кластеризации текстовых описаний угроз БИ и уязвимостей ПО, в связи с чем не совсем ясно, каким образом определялось оптимальное количество этих кластеров;

– ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С.П. Королева», заведующий кафедрой программных систем, **д.т.н., доцент Востокин Сергей Владимирович**. *Замечания*: **1.** Непонятен выбор критерия приоритизации множества угроз БИ для выявленных уязвимостей ПО. **2.** Неясно также, почему в качестве меры оценки семантической близости текстовых описаний выбрана косинусная мера;

– ФГБОУ ВО «Поволжский государственный технологический университет», заведующая кафедрой информационной безопасности, **д.т.н., профессор Сидоркина Ирина Геннадьевна**. *Замечание*: не вполне понятно,

почему для иллюстрации предложенной архитектуры интеллектуальной системы поддержки принятия решений (ИСППР) выбрана нотация UML, представлена только диаграмма компонент;

– ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ», профессор кафедры систем информационной безопасности, **д.т.н., профессор Катасёв Алексей Сергеевич**. *Замечания*: **1.** При рассмотрении нейросетевых моделей трансформеров не приведены параметры их архитектуры, не описана процедура токенизации текстовых описаний; **2.** Некоторые из представленных в автореферате блок-схем алгоритмов (в частности, на рисунках 2, 5, 7) выполнены с нарушением требований ГОСТ;

– ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С.П. Королева», заведующий кафедрой безопасности информационных систем, **к.ф.-м.н., доцент Осипов Михаил Николаевич.** *Замечание*: Наилучший результат в задаче сопоставления текстовых описаний угроз БИ, уязвимостей ПО, техник (тактик) демонстрирует предобученная модель-трансформер, но, поскольку визуализация графовой модели здесь не представлена, это затрудняет последующую оценку применимости данной модели;

– ФГБОУ ВО «Воронежский государственный технический университет», заведующий кафедрой систем информационной безопасности, **д.т.н. профессор Остапенко Александр Григорьевич.** *Замечания (в форме рекомендуемых направлений последующих исследований)*: **1.** Для существующих разновидностей сетевых атак формирование риск-ландшафтов, где третьим измерением выступает риск их успешности в привязке к плоскости пар «вектор атаки – используемая им уязвимость» с ранжированием элементов поверхности ландшафта по вышеуказанному риску **2.** Выработка методических рекомендаций противодействия в виде мер и регламентов: обнаружения и регистрации инцидентов; реагирования на инциденты; ликвидация их последствий для всевозможных пар «вектор - уязвимость» существующих разновидностей сетевых атак, включая формирование из них баз знаний в качестве информационного

обеспечения создаваемого инструментария; **3**. Автоматизация процесса регистрации инцидента и идентификации «пар», лежащих, в его основе, на базе машинного обучения и сформированных баз знаний; **4.** Использование нейроподобных сетей и накопленных в ходе машинного их обучения знаний о программно-технической и организационно-правовой защите КИИ, автоматизация интеллектуальной поддержки для лиц, принимающих решения в ходе сетевого противоборства.

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:

– **предложены** метод и алгоритм оценки актуальных угроз безопасности информации (БИ) и уязвимостей программного обеспечения (ПО) объектов критической информационной инфраструктуры (КИИ) на основе технологий семантического анализа текстов, отличающиеся использованием оригинального способа кластеризации и оценки соответствия (семантической близости) текстовых описаний уязвимостей ПО, угроз БИ , тактик и техник действий нарушителя, содержащихся в Банке данных угроз безопасности информации ФСТЭК России, что позволяет автоматизировать процесс построения сценариев реализации угроз БИ, снизить трудоемкость и когнитивную нагрузку на специалистов по информационной безопасности (ИБ);

– **разработаны** архитектура и программные модули прототипа интеллектуальной системы поддержки принятия решений (ИСППР) на этапе оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ, применение которых позволяет снизить временные затраты и повысить обоснованность решений, принимаемых специалистами по ИБ при формировании перечня уязвимостей ПО и актуальных угроз БИ объектов КИИ;

– **доказана** перспективность использования разработанных метода, алгоритмов и методики оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ, а также инструментальных средств автоматизации процесса оценки актуальных угроз и уязвимостей объектов КИИ, применение которых позволяет сократить временные затраты и повысить объективность оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ, обеспечивая в конечном итоге более обоснованный выбор организационно-технических мер по выполнению нормативных требований к уровню защищенности объектов КИИ.

Теоретическая значимость исследования обоснована тем, что:

– применительно к проблематике диссертации результативно (т.е. с получением обладающих новизной результатов) **использованы** методы интеллектуального анализа данных и защиты информации, методы обработки естественного языка и экспертных оценок, теории искусственных нейронных сетей, методология объектно-ориентированного анализа и проектирования, модели теории графов и имитационного моделирования;

– **изложены** аргументы и факты, подтверждающие актуальность исследований в области разработки метода и алгоритмов автоматизированной оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ, отличительной особенностью которых является применение технологий интеллектуального анализа текстов для построения возможных сценариев реализации угроз БИ, что позволяет значительно снизить трудоемкость обработки текстовых описаний угроз БИ и уязвимостей ПО, повысить объективность и оперативность принимаемых решений в процессе оценки уровня защищенности объектов КИИ;

– **раскрыты** проблемы, связанные с применением известных методов и алгоритмов оценки актуальных угроз БИ и уязвимостей ПО при решении практических задач, связанных с оценкой уровня защищенности объектов КИИ, не позволяющих в автоматизированном режиме производить обработку больших массивов текстовых описаний угроз БИ и уязвимостей ПО и, как следствие, обеспечить обоснованность и оперативность решений, принимаемых в процессе оценки рисков ИБ и уровня защищенности объектов КИИ;

– **изучены** основные особенности объектов КИИ и нормативные документы ФСТЭК России в области обеспечения ИБ этих объектов, положенные в основу разработки предложенного метода и алгоритма оценки актуальных угроз БИ и уязвимостей ПО;

– **проведена модернизация** известных методов и алгоритмов оценки актуальных угроз БИ и уязвимостей ПО с использованием технологий интеллектуального анализа текстов, выполнена разработка инструментальных программных средств для автоматизации процесса оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ.

Значимость полученных соискателем результатов исследований для практики подтверждается тем, что:

– **разработаны и внедрены** в ЗАО «Республиканский центр защиты информации», ООО «УРАЛТЕХСИСТЕМЫ», ФГБОУ ВО «Уфимский университет науки и технологий» результаты диссертационной работы, в том числе:

- алгоритмы автоматической классификации и реферирования специализированных текстов в области ИБ на основе технологий автоматизированной обработки текстовых описаний;

- метод и алгоритм автоматизированной оценки и приоритизации (ранжирования) множества релевантных угроз БИ для выявленных уязвимостей ПО на основе технологии семантического анализа текстов;

- алгоритм построения структурной модели (в виде графа) сценария реализации актуальных угроз БИ на основе оценки семантической близости текстовых описаний соответствующих угроз БИ, уязвимостей ПО, тактик и техник действий нарушителя;

- прототип ИСППР и программные модули автоматизации процесса построения сценариев реализации актуальных угроз БИ;

– **определены** рекомендации по практическому применению разработанного метода, алгоритмов и инструментальных средств оценки актуальных угроз БИ и

уязвимостей ПО для решения прикладных задач оценки и обеспечения требуемого уровня защищенности объектов КИИ;

– **созданы** архитектура прототипа ИСППР и комплекс программных средств автоматизации оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ, применение которых позволяет сформировать перечень наиболее опасных угроз БИ для выявленных уязвимостей ПО, построить возможные сценарии реализации угроз БИ и, в итоге, обеспечить более обоснованный выбор организационно-технических мер по обеспечению нормативных требований к уровню защищенности объектов КИИ;

– **представлены** теоретические и экспериментальные результаты, подтверждающие научную новизну и практическую значимость предложенных решений.

Оценка достоверности результатов исследования выявила:

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

– **идея базируется** на Методике оценки угроз безопасности информации ФСТЭК России, в соответствии с которой предложено реализовать процесс оценки актуальных угроз БИ посредством построения сценариев реализации угроз БИ на основе автоматизированной процедуры сопоставления выявленных уязвимостей ПО, тактик (техник) и потенциально существующих релевантных угроз БИ, построения графовой модели сценариев реализации угроз БИ с использованием приведенных в Банке данных угроз безопасности информации (БДУ) и Методике оценки угроз безопасности информации ФСТЭК России текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник действий нарушителя, применение которых позволяет автоматизировать процесс оценки актуальности угроз БИ на основе построения сценариев реализации угроз БИ объекта КИИ;

– **использовано** сопоставление предложенных в диссертации решений для автоматизированной оценки актуальных угроз БИ с экспертным способом оценки

актуальных угроз БИ, которое показало, что применение известных методик не в полной мере соответствует требованиям ФСТЭК России или же приводит к возникновению субъективных ошибок и снижению скорости обработки текстовых данных, что устранено в предлагаемых решениях;

– **установлено** качественное совпадение авторских результатов с результатами, представленными в независимых источниках, при улучшении количественных показателей эффективности при решении задач оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ.

Личный вклад соискателя состоит в участии на всех этапах научного исследования: планировании, постановке целей и задач исследования, проведении серий вычислительных экспериментов, анализе результатов этих экспериментов, обработке и интерпретации полученных результатов на каждом этапе исследования, в подготовке основных публикаций по выполненной работе.

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

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

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

– соискатель ссылается на авторов и источники заимствования;

– оригинальность диссертационной работы составляет 97,41 %.

Диссертационная работа Кучкаровой Наили Вакилевны «Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов» соответствует п. 9 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 21 апреля 2016 года № 335), предъявляемых к кандидатским диссертациям.

Тема работы и содержание исследований соответствуют паспорту научной

актуальных угроз БИ, которое показало, что применение известных методик не в полной мере соответствует требованиям ФСТЭК России или же приводит к возникновению субъективных ошибок и снижению скорости обработки текстовых данных, что устранено в предлагаемых решениях;

– **установлено** качественное совпадение авторских результатов с результатами, представленными в независимых источниках при решении задач оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ.

Личный вклад соискателя состоит в участии на всех этапах научного исследования: планировании, постановке целей и задач исследования, проведении серий вычислительных экспериментов, анализе результатов этих экспериментов, обработке и интерпретации полученных результатов на каждом этапе исследования, в 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 кандидата технических наук;

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

– соискатель ссылается на авторов и источники заимствования;

– оригинальность диссертационной работы составляет 97,41 %.

Диссертационная работа Кучкаровой Наили Вакилевны «Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов» соответствует п. 9 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 21 апреля 2016 года № 335), предъявляемых к кандидатским диссертациям.

Тема работы и содержание исследований соответствуют паспорту научной

специальности 2.3.6. Методы и системы защиты информации, информационная безопасность по пунктам: п. 1 «Теория и методология обеспечения информационной безопасности и защиты информации»; п. 3 «Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса»; п. 8 «Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения»; п. 15. «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Диссертация Кучкаровой Н.В. является законченной научно-квалификационной работой, в которой содержатся научно обоснованные результаты решения задач оценки актуальных угроз безопасности информации и уязвимостей ПО, обеспечения инструментальными средствами автоматизации данного процесса на этапе оценки уровня защищенности объектов критической информационной инфраструктуры, имеющих важное практическое значение.

В ходе защиты диссертации были высказаны следующие критические замечания:

1. Было бы желательно в будущем попытаться исследовать свойства меры семантической близости с точки зрения семантического дифференциала.

2. Интересно было рассмотреть и сравнить другие подходы к определению семантической близости текстовых данных и устойчивости предлагаемых решений.

3. В рамках парадигмы Индустриализация 4.0 создаются «безлюдные» технологии, а в данной работе основное внимание уделяется экспертной оценке и роли человека в принятии решений.

Соискатель Кучкарова Н.В. согласилась с высказанными замечаниями и подтвердила необходимость исследования в дальнейшем других подходов к определению семантической близости текстовых описаний, оценке свойств меры

семантической близости с точки зрения семантического дифференциала, а также оценке устойчивости полученных решений. Относительно третьего замечания: в «безлюдных» технологиях окончательное решение в ответственных приложениях (а это в первую очередь относится к объектам КИИ) остается за человеком. Предложенная в работе ИСППР обеспечивает специалисту по ИБ интеллектуальную поддержку на этапе принятия решений, применение которой существенно снижает когнитивную нагрузку на человека и субъективность оценок в принятии итогового решения.

На заседании 22.09.2023 г. диссертационный совет принял решение:

–за решение актуальной задачи повышения достоверности и оперативности оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ на основе технологий интеллектуального анализа текстов, имеющей важное практическое значение с точки зрения обеспечения обоснованного выбора организационно-технических мер, направленных на выполнение нормативных требований к защищенности объектов КИИ,

присудить Кучкаровой Наиле Вакилевне ученую степень кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

При проведении тайного голосования диссертационный совет в количестве 14 человек, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 19 человек, входящих в состав совета, проголосовали: за – 14, 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

22 сентября 2023 года