ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.2.479.07, СОЗДАННОГО 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 30.06.2023 г. № 7

О присуждении Кирилловой Анастасии Дмитриевне, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Оценка рисков информационной безопасности АСУ ТП промышленных объектов с использованием методов когнитивного моделирования» по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите 28.04.2023 г., протокол № 2 диссертационным советом 24.2.479.07, созданным на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий» Министерства науки и высшего образования Российской Федерации, 450076, г. Уфа, ул. Заки Валиди, 32, созданного приказом Министерства образования и науки Российской Федерации № 542/нк от 24.03.2023 г.

Соискатель Кириллова Анастасия Дмитриевна, 23.02.1993 года рождения. В 2017 г. окончила магистратуру ФГБОУ ВО «Уфимский государственный авиационный технический университет» по направлению подготовки 09.04.01 Информатика и вычислительная техника.

В 2022 г. окончила аспирантуру ФГБОУ ВО «Уфимский государственный авиационный технический университет» по направлению подготовки 10.06.01 Информационная безопасность.

Работает ассистентом кафедры вычислительной техники и защиты информации ФГБОУ ВО «Уфимский университет науки и технологий» Министерства науки и высшего образования Российской Федерации.

Диссертация выполнена на кафедре вычислительной техники и защиты информации ФГБОУ ВО «Уфимский университет науки и технологий» Министерства науки и высшего образования Российской Федерации.

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 Аралбаев Ташбулат Захарович, заведующий кафедрой вычислительной техники и защиты информации ФГБОУ ВО «Оренбургский государственный университет»;

2. Доктор технических наук, доцент Баранкова Инна Ильинична, заведующий кафедрой информатики и информационной безопасности ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова»

дали положительные отзывы на диссертацию.

Ведущая организация федеральное государственное автономное образовательное учреждение высшего образования «Омский государственный технический университет», г. Омск, в своем положительном отзыве, подписанном заведующим кафедрой комплексной защиты информации, доктором технических наук, доцентом Ложниковым Павлом Сергеевичем, утвержденном проректором по научной и инновационной деятельности, кандидатом химических наук Фефеловым Василием Федоровичем, указала, что диссертация Кирилловой Анастасии Дмитриевны на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, в которой на основании выполненных автором исследований разработан метод, модели и алгоритмы количественной оценки рисков ИБ АСУ ТП промышленных объектов с использованием технологий когнитивного моделирования и машинного

обучения, применение которых позволяет повысить оперативность и достоверность принимаемых управленческих решений на этапе оценки их уровня защищенности и выбора эффективных контрмер по защите информации.

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

Соискатель имеет 31 опубликованную работу по теме диссертации, в том числе 8 статей в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, либо в научных изданиях, индексируемых базой данных RSCI, 4 научные работы в изданиях, включенных в базу Scopus, 16 статей в других изданиях, получено 3 свидетельства о государственной регистрации программы для ЭВМ. 6 публикаций выполнены соискателем единолично, остальные – при непосредственном участии соискателя.

Общий объем публикаций – 14,625 п.л., авторский вклад – 4,96 п.л.

Наиболее значимые работы по теме диссертации:

1. Система поддержки принятия решений по обеспечению информационной безопасности автоматизированной системы управления технологическими процессами / В.И. Васильев, В.Е. Гвоздев, М.Б. Гузаиров, А.Д. Кириллова // Информация и безопасность. – 2017. – Т. 20, № 4. – С. 618–623.

2. 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. – DOI: 10.17587/it.24.657-664.

3. Васильев В.И., Кириллова А.Д., Кухарев С.Н. Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 4(30). – С. 66–74. – DOI: 10.14529/secur180410.

4. 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. – DOI: 10.14529/secur190406.

5. 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.

6. Васильев В.И., Вульфин А.М., Кириллова А.Д. Анализ и управление рисками информационной безопасности АСУ ТП на основе когнитивного моделирования // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – № 2(37). – С. 1–18. – DOI 10.26102/2310-6018/2022.37.2.022.

7. Decision support system in the task of ensuring information security of automated process control systems / A.D. Kirillova, V.I. Vasilyev, A.V. Nikonov, V.V. Berkholts // CEUR Workshop Proceedings DS-ITNT 2019 – Proceedings of the Data Science Session at the 5th International Conference on Information Technlogy and Nanotechnology. – 2019. – P. 477–486. – DOI: 10.18287/1613-0073-2019-2416-477-486.

8. 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). – Journal of Physics: Conference Series. – 2021. –Vol. 2001. – 012004. – DOI: 10.1088/1742-6596/2001/1/012004.

9. Cybersecurity risk assessment based on cognitive attack vector modeling with CVSS Score / V.I. Vasilyev, A.D. Kirillova, A.M. Vulfin, A.V. Nikonov // 2021 International Conference on Information Technology and Nanotechnology (ITNT). – IEEE. – 2021. – P. 1–6. – DOI: 10.1109/ITNT52450.2021.9649191.

10. Кириллова А.Д. Анализ проекта методики моделирования угроз безопасности информации ФСТЭК России // Материалы XIV Всероссийской

молодежной научной конференции «Мавлютовские чтения». – Уфа: РИК УГАТУ. – 2020. – С. 20.

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

На диссертацию и автореферат поступили положительные отзывы:

– **ведущей организации** ФГАОУ ВО «Омский государственный технический университет». *Замечания*: **1.** Эффективность применения предложенных в работе инструментальных средств автоматизации моделирования сценариев атак с последующей оценкой рисков ИБ для АСУ ТП показана на примере АСУ ТП нефтедобывающего предприятия. Вместе с тем, в работе не уделено достаточно внимания вопросам переносимости и масштабируемости предложенных решений на другие промышленные объекты. **2.** Применение аппарата нечетких когнитивных карт сопровождается в работе введением шкалы оценки силы связей между концептами (таблица 2.1, стр. 62), однако не поясняется выбор количества и границ термов, а также не раскрывается обоснование выбора структуры когнитивной модели на рисунке 2.7. **3.** Недостаточно подробно раскрыт процесс выбора весовых коэффициентов вложенной когнитивной модели при оценке эффективности применения выбранных контрмер (рисунок 3.14 и таблица 3.6, стр. 93). **4.** Не раскрыты оценки сравнительных временных затрат на формирование сценариев реализации актуальных угроз ИБ в процессе построения модели угроз для объекта защиты, без применения разработанных решений и с их использованием, приведена лишь оценка их соотношения. 5. Неясно, насколько оправданным при разработке прототипа ИСППР является использование сразу нескольких фреймворков и языковых средств (Matlab, Python, C#).

– **официального оппонента** доктора технических наук, профессора Аралбаева Ташбулата Захаровича, заведующего кафедрой вычислительной техники и защиты информации ФГБОУ ВО «Оренбургский государственный университет». *Замечания*: **1.** В содержании текста диссертации не приведены результаты анализа возможности применения разработанной методики и ее аналогов применительно к распределенным в пространстве АСУ транспортными

трубопроводами нефтегазового сырья и продуктов. **2.** В работе решается задача сценарного моделирования графов реализации атаки с использованием графовой базы данных, однако желательно было бы уточнить порядок и формат формирования запросов к указанной базе данных с учетом требований по репрезентативности и достоверности исходных данных. **3.** В работе недостаточно четко представлен механизм получения конкретных численных оценок снижения рисков при интервальной оценке параметров концептов. **4.** Текст работы, в частности в главе 4, избыточно насыщен материалом пояснительного и иллюстративного характера, часть из которого без ущерба для представления и понимания результатов исследований может быть перемещен в приложение, например, рисунки: 4.7, 4.29. В тексте также встречаются отдельные выражения, редко используемые в научной литературе, в частности, как «эксплуатация контрмер».

– **официального оппонента** доктора технических наук, доцента Баранковой Инны Ильиничны, заведующей кафедрой информатики и информационной безопасности ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». *Замечания*: **1.** При описании нарушителей в сценариях реализации атак следует пользоваться классификацией нарушителей согласно «Методике оценки угроз безопасности информации» ФСТЭК России от 05.02.2021 г. **2.** Разработка алгоритма построения иерархии когнитивных моделей в разд. 2.4 представлена лишь в виде схем сворачивания и декомпозиции нечётких серых когнитивных карт и перечисления этапов, но не представлена в виде итоговой блок-схемы, что затрудняет анализ предложенного решения. **3.** В разделе 3.2 при описании алгоритма построения графовых моделей недостаточно внимания уделено способам сокращения размерности графовой модели – указано лишь на необходимость оперирования перекрестными ссылками компонентов баз данных CVE-CWE-CAPEC-ATT&CK, что не позволяет оценить эффективность данной процедуры. **4.** Предложенный в диссертации метод демонстрирует эффективность в выборе наиболее эффективных вариантов средств защиты при минимальных либо допустимых затратах. Большое количество АСУ ТП относятся

к критической информационной инфраструктуре, для этого типа АСУ ТП критерием оптимизации следует выбирать минимизацию ущерба. **5.** В п.4.4 диссертации указывается, что предложенные решения позволяют: сформировать расширенный список контрмер на основе базы знаний ATT&CK, NVD для каждой из выделенных зон. Группа матриц ATT&CK for ICS описывает тактики и техники, которые используются в атаках на промышленные системы управления, но контрмер она не содержит. **6.** Схема структурно-функциональной организации ИСППР в задачах оценки рисков ИБ АСУ ТП содержит модуль оценки эффективности и выбора контрмер. В диссертации не указано, как этот выбор осуществляется и на какой стадии разработки находится модуль.

Получено 7 положительных отзывов на автореферат:

– ФГАОУ ВО «Пермский национальный исследовательский политехнический университет», заведующий кафедрой автоматики и телемеханики, **д.т.н., профессор Южаков Александр Анатольевич**. *Замечания*: **1.** Из автореферата неясно, каким образом строится исходный граф атак на промышленную сеть АСУ ТП и как выполняется последующий переход к предлагаемой автором графовой модели. **2.** Вторая глава ориентирована на создание нечеткой когнитивной модели количественной оценки рисков, а не метода, как указано в выводе по главе, неясно проверялась ли адекватность предложенной модели.

– ФГБОУ ВО «Астраханский государственный университет им. В.Н. Татищева», декан факультета цифровых технологий и кибербезопасности, **д.т.н., профессор Ажмухамедов Искандар Маратович**. *Замечания*: **1.** В автореферате не раскрыты подробно детали реализации исследовательского прототипа ИСППР. **2.** Не приведены оценки производительности и требуемых вычислительных ресурсов для развертывания данной системы.

– ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С.П. Королева», профессор кафедры «Информационные системы и технологии», **д.т.н., профессор Прохоров Сергей Антонович**. *Замечания*: **1.** Алгоритм построения результирующей нечеткой когнитивной

модели на основе графовых моделей реализации атаки приведен без детализации процедур декомпозиции и сворачивания когнитивных моделей. **2.** При изложении примера оценки рисков ИБ для АСУ ТП нефтедобывающего предприятия (рисунок 11) базовая архитектура объекта приведена без описания выделенных зон безопасности и связывающих их трактов.

– ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», заведующий кафедрой информационной безопасности, **д.т.н., профессор Карташевский Вячеслав Григорьевич**. *Замечания*: **1.** Недостаточно подробно изложены вопросы иерархии (декомпозиции) вложенных нечетких когнитивных карт. **2.** В автореферате также не отражен вопрос о выборе состава контрмер, направленных на снижение рисков ИБ АСУ ТП промышленных объектов.

– ФГАОУ ВО «Омский государственный университет им. Ф.М. Достоевского», профессор кафедры информационной безопасности, **д.ф.-м.н., профессор Гуц Александр Константинович**. *Замечания*: В автореферате не раскрыт вопрос, как учитывается многоуровневая организация АСУ ТП промышленного объекта при построении нечеткой когнитивной модели для оценки его рисков ИБ, какие особенности архитектуры АСУ ТП учитываются при исследовании.

– ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ», профессор отделения интеллектуальных кибернетических систем офиса образовательных программ, **д.т.н., доцент Милославская Наталья Георгиевна**. *Замечания*: Из текста автореферата неясно, насколько трудоемким является процесс подготовки исходных данных и каким должен быть их состав для проведения анализа с помощью разработанных автором средств автоматизации моделирования сценариев атак и оценки рисков ИБ АСУ ТП промышленных объектов.

– ФГАОУ ВО «Самарский национальный исследовательский университет имени С.П. Королёва», профессор кафедры безопасности информационных систем, **д.ф.-м.н., профессор Новиков Сергей Яковлевич**, доцент кафедры

безопасности информационных систем, к.т.н. Бурлаков Михаил Евгеньевич. *Замечания*: **1.** Не рассмотрены механизмы согласования экспертных оценок при оценке достоверности полученных результатов когнитивного моделирования. **2.** Не даны пояснения по качественной и количественной оценке диапазона их разброса.

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:

– **предложен** метод количественной и качественной оценки рисков информационной безопасности (ИБ) автоматизированных систем управления технологическими процессами (АСУ ТП) промышленных объектов на основе моделирования сценариев атак с использованием технологий когнитивного моделирования и методов машинного обучения, отличающийся применением шаблонов открытых баз знаний для формализации описания объекта атаки, перечня актуальных угроз и уязвимостей в виде иерархии графовых моделей и баз данных, что позволяет автоматизировать и унифицировать их представление в виде последовательности действий, совокупности методов и средств (тактик и техник), позволяющих потенциальному нарушителю реализовать атаку на АСУ ТП промышленного объекта;

– **разработана** архитектура исследовательского прототипа интеллектуальной системы поддержки принятия решений (ИСППР) в задачах оценки рисков ИБ АСУ ТП промышленных объектов, а также программная реализация инструментальных средств автоматизации моделирования сценариев атак и оценки рисков ИБ АСУ ТП, применение которых позволяет повысить оперативность и достоверность оценки рисков ИБ, что обеспечивает обоснованность выбора контрмер на этапах проектирования и внедрения комплексных систем защиты информации АСУ ТП промышленного объекта;

– **доказана** целесообразность и исследованы свойства разработанного метода, моделей, алгоритмов и методики количественной оценки рисков ИБ АСУ ТП, а также инструментальных средств автоматизации моделирования сценариев атак в составе ИСППР, применение которых для решения прикладных задач позволит повысить достоверность и оперативность количественной оценки рисков ИБ и, в конечном итоге, эффективность выбора контрмер на этапах проектирования и внедрения комплексных систем защиты информации АСУ ТП промышленных объектов.

Теоретическая значимость исследования обоснована тем, что:

– применительно к проблематике диссертации результативно (то есть с получением обладающих новизной результатов) **использованы** методы системного анализа, оценки рисков ИБ, теории графов, когнитивного моделирования и машинного обучения;

– **изложены** аргументы и факты, подтверждающие актуальность подхода к обеспечению ИБ АСУ ТП и разработки метода, моделей и алгоритмов количественной оценки рисков АСУ ТП промышленных объектов, отличительным признаком которых является применение нечеткого когнитивного моделирования и методов машинного обучения для оценки уровня защищенности выделенных зон АСУ ТП промышленного объекта, что позволяет определить рациональное распределение затрат на реализацию, внедрение и сопровождение контрмер с учетом их функциональных ограничений.

– **раскрыты** противоречия, связанные с применениям существующих методов и алгоритмов оценки рисков ИБ при решении практических задач управления рисками ИБ промышленного предприятия, не позволяющие количественно оценить реальные потери от реализации угроз ИБ АСУ ТП промышленных объектов и, как следствие, обосновать эффективный выбор контрмер; кроме того их применение осложнено высокой степенью неопределенности и трудоемкостью процедуры формализации факторов, влияющих на уровень ИБ АСУ ТП промышленных объектов;

– **изучены** основные особенности АСУ ТП промышленных объектов,

обуславливающие необходимость поиска рационального метода количественной оценки рисков ИБ АСУ ТП с целью повышения защищенности промышленных объектов;

– **проведена модернизация** известных методов и алгоритмов оценки рисков ИБ с использованием технологий когнитивного моделирования и методов машинного обучения, а также выполнена разработка инструментальных программных средств для автоматизации моделирования сценариев атак и оценки рисков ИБ АСУ ТП промышленных объектов.

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

– **разработаны и внедрены** в ФГБОУ ВО «Уфимский университет науки и технологий», ООО «Инженерный центр систем безопасности», ЗАО «Республиканский центр защиты информации», ООО «НПП ОЗНА-Инжиниринг» результаты диссертационной работы, в том числе:

1) когнитивная модель количественной оценки рисков ИБ АСУ ТП промышленных объектов и алгоритм ее построения на основе иерархии вложенных нечетких когнитивных карт;

2) метод и алгоритмы количественной оценки рисков ИБ с использованием технологий сценарного моделирования атак и методов машинного обучения;

3) алгоритмы и инструментальные средства количественной оценки рисков ИБ АСУ ТП на основе моделирования сценариев атак;

4) методика количественной оценки рисков ИБ АСУ ТП на основе моделирования сценариев атак с применением технологий когнитивного моделирования и методов машинного обучения;

5) исследовательский прототип ИСППР и программная реализация средств автоматизации моделирования сценариев атак.

– **определены** практические рекомендации применения разработанного метода, моделей, алгоритмов и инструментальных средств оценки рисков ИБ АСУ ТП промышленных объектов для решения прикладных задач количественной оценки рисков ИБ промышленных систем автоматизации;

– **создана** архитектура исследовательского прототипа ИСППР и программная реализация инструментальных средств автоматизации оценки рисков ИБ и моделирования сценариев атак, позволяющая извлечь информацию о слабых местах инфраструктуры АСУ ТП, наиболее опасных уязвимостях и потенциальных слабостях компонент системы, выявить наиболее успешные для нарушителя потенциальные сценарии атак, оценить их последствия для промышленного предприятия;

– **представлены** предложения по дальнейшему развитию полученных результатов, связанные с совершенствованием предложенных алгоритмов, моделей и методик оценки рисков ИБ АСУ ТП и развитием разработанного прототипа ИСППР с целью повышения оперативности и достоверности получения количественных оценок рисков ИБ АСУ ТП для различных промышленных объектов, а также совершенствование методических рекомендаций по выбору эффективного набора контрмер.

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 Методике оценки угроз безопасности информации ФСТЭК России в соответствии с которой предложено реализовать процесс оценки рисков путем построения иерархии нечетких когнитивных карт применительно к зональной модели АСУ ТП и формализовать таким образом процедуру количественной оценки рисков ИБ АСУ ТП и моделирования сценариев атак как в пределах каждой из зон, так и для всего объекта в целом; кроме того, для реализации процесса оценки рисков ИБ АСУ ТП используются приведенные в Методике оценки угроз безопасности информации ФСТЭК России и базе данных MITRE ATT&CK тактики и техники, а также дополнительную информацию из Банка данных угроз безопасности информации ФСТЭК России и баз данных шаблонов компьютерных атак, применение которых позволяет формально

описать сценарии эксплуатации уязвимостей и автоматизировать построение цепочки возможных действий нарушителя на промежуточных узлах АСУ ТП;

– **использовано** сопоставление предложенной в диссертации методики оценки рисков ИБ АСУ ТП с существующими аналогами, показавшее, что применение известных методик осложняется высокой степенью неопределенности в процедурах выделения основных факторов, влияющих на защищенность АСУ ТП: появление новых угроз и уязвимостей; возможности потери актуальности данных в ходе анализа рисков. Разработанная в диссертации методика в значительной степени свободна от отмеченных недостатков.

– **установлено** совпадение авторских результатов с результатами, представленными в независимых источниках, в задачах оценки риска ИБ АСУ ТП промышленного объекта.

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 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 96,47 %.

Диссертационная работа Кирилловой Анастасии Дмитриевны «Оценка рисков информационной безопасности АСУ ТП промышленных объектов с использованием методов когнитивного моделирования» соответствует п. 9

Положения о порядке присуждения ученых степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г. (с последующими изменениями), 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. 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. 10. «Модели и методы оценки защищенности информации и информационной безопасности объекта».

Диссертация Кирилловой А.Д. является законченной научно-квалификационной работой, в которой содержатся научно обоснованные результаты решения задач количественной оценки рисков ИБ АСУ ТП промышленных объектов и обеспечения интеллектуальной поддержки принятия решений на этапе выбора эффективных контрмер по защите информации, имеющих важное практическое значение.

В ходе защиты диссертации были высказаны следующие критические замечания:

1. Комплекс защитных мер (контрмер) может быть организован различными способами: как по составу, так и по их конфигурации. Более того, сами защитные меры могут иметь уязвимости, которые могут быть эксплуатированы злоумышленниками. В рамках доклада недостаточно полно раскрыты вопросы выбора соответствующих контрмер с учетом вышесказанного.

2. Существует группа стандартов ГОСТ Р 57700, регламентирующая создание цифровых моделей. К сожалению, в докладе не прозвучало, учитывались ли в процессе разработки требования этих стандартов.

Соискатель Кириллова А.Д. согласился с высказанными замечаниями и подтвердил, что разработка прототипа программного обеспечения основывалось

на серии ГОСТ, в том числе на ГОСТ Р 57100-2016 «Системная и программная инженерия. Описание архитектуры», ГОСТ Р 57193-2016 «Системная и программная инженерия. Процессы жизненного цикла систем» и ГОСТ Р 57700.22-2020 «Компьютерные модели и моделирование. Классификация». При описании архитектуры прототипа интеллектуальной системы поддержки принятия решений разработан ряд моделей, раскрывающих основные понятия и свойства системы, ее элементы и отношения между ними. Использован принцип модульности и унификации интерфейсов для взаимодействия с внешними системами.

На заседании 30.06.2023 г. диссертационный совет принял решение за разработку метода, моделей и алгоритмов количественной оценки рисков ИБ АСУ ТП промышленных объектов и обеспечения интеллектуальной поддержки принятия решений на этапе выбора эффективных контрмер по защите информации присудить Кирилловой А.Д. 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 16 человек, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 19 человек, входящих в состав совета, проголосовали: за – 16, против – 0.

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

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

30 июня 2023 года