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 29.01.2026 № 3

О присуждении Чернову Денису Владимировичу, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок» по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите 14.11.2025 г., протокол № 11 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, созданного приказом Министерства образования и науки Российской Федерации от 24.03.2023 г. № 542/нк (с изменениями приказами от 18.12.2023 г. № 2368/нк и от 11.06.2024 г. № 581/нк, и от 09.12.2025 г. №1182/нк).

Соискатель **Чернов Денис Владимирович**, 28 февраля 1992 года рождения, работает старшим преподавателем кафедры «Информационная безопасность» института прикладной математики и компьютерных наук федерального государственного бюджетного образовательного учреждения высшего образования «Тульский государственный университет» Министерства науки и высшего образования Российской Федерации.

В 2014 г. окончил ФГБОУ ВО «Тульский государственный университет» по специальности 090105 Комплексное обеспечение информационной безопасности автоматизированных систем. В 2019 г. был прикреплен в ФГБОУ ВО «Тульский государственный университет» для подготовки диссертации на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность. Справка со сведениями о сданных кандидатских экзаменах по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность № 41 от 03.07.2025 г. выдана федеральным государственным бюджетным образовательным учреждением «Тульский государственный университет (ТулГУ)».

Диссертация выполнена на кафедре «Информационная безопасность» ФГБОУ ВО «Тульский государственный университет» Министерства науки и высшего образования Российской Федерации.

Научный руководитель – доктор технических наук, доцент, директор института прикладной математики и компьютерных наук, заведующий кафедрой «Информационная безопасность» Сычугов Алексей Алексеевич, ФГБОУ ВО «Тульский государственный университет».

Официальные оппоненты:

1. Ложников Павел Сергеевич, доктор технических наук, профессор, заведующий кафедрой комплексной защиты информации федерального государственного автономного образовательного учреждения высшего образования «Омский государственный технический университет»;

2. Максимова Елена Александровна, доктор технических наук, доцент, заведующий кафедрой КБ-4 «Интеллектуальные системы информационной безопасности» федерального государственного бюджетного образовательного учреждения высшего образования «МИРЭА – Российский технологический университет», **дали положительные отзывы о диссертации**.

Ведущая организация – автономная некоммерческая организация «Институт инженерной физики», г. Серпухов, в своем положительном отзыве, утвержденным генеральным директором – Первым Вице-президентом Института,

почетным работником науки и техники Российской Федерации, кандидатом технических наук, доцентом Ананьевым Евгением Михайловичем, подписанным заместителем генерального директора Института по специальным проектам, почетным работником науки и высоких технологий Российской Федерации, доктором технических наук, профессором Олегом Игоревичем Атакищевым, главным научным сотрудником Института, почетным работником науки и техники Российской Федерации, почетным специалистом по защите информации, доктором технических наук, доцентом Вадимом Геннадьевичем Грибуниным, начальником научно-методического управления, почетным работником науки и высоких технологий Российской Федерации, кандидатом технических наук, доцентом Алексеем Александровичем Коробковым, указала, что диссертация Чернова Дениса Владимировича на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, содержащей решение актуальной научной задачи, имеющей значение для развития технической отрасли знаний, в рамках теории, технологии и средств обеспечения информационной безопасности и защиты информации, а именно в повышении эффективности процесса моделирования угроз безопасности объектов критической информационной инфраструктуры на основе аппарата экспертных оценок.

Диссертация соответствует требованиям пункта 9, 10, 11, 13, 14 Положения о порядке присуждения ученых степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г. (в редакции от 25.04.2024 г.), а её автор – Чернов Денис Владимирович – заслуживает присуждения ему ученой степени кандидата технических наук по научной специальности 2.3.6. Системы, сети и устройства телекоммуникаций.

Соискатель имеет 30 опубликованных работ, в том числе 4 статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, 10 статей в ведущих зарубежных рецензируемых журналах, индексируемых в базах данных Web of Science и Scopus, 16 статей в других изданиях, 1 свидетельство о регистрации программы ЭВМ. 7 публикаций выполнены соискателем единолично, остальные – при непосредственном участии соискателя.

Общий объем публикаций – 22,64 п. л., авторский вклад – 12,49 п. л. Наиболее значимые работы по теме диссертации:

1. Чернов Д. В. Методики оценки угроз безопасности информации автоматизированных систем управления технологическими процессами // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. Научный журнал. № 9, 2021. – С. 81-88.

2. Чернов Д.В. О выборе мер обеспечения информационной безопасности автоматизированных систем управления технологическими процессами / Чернов Д.В., Сычугов А.А. // Моделирование, оптимизация и информационные технологии. Научный журнал. №9(2), 2021. – С. 1-9.

3. Чернов Д. В. Применение диаграмм Эйлера-Венна при решении задачи выбора мер защиты АСУ ТП // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. Научный журнал. №7, 2021. – С. 127-131.

4. Чернов Д.В. Метод количественной оценки опасности реализации угроз безопасности информации объектов критической информационной инфраструктуры потенциальными нарушителями // Моделирование, оптимизация и информационные технологии. Научный журнал. №13 (2), 2025. – С. 1-11.

5. Чернов Д. В. Автоматизированная система моделирования угроз информационной безопасности / Д. В. Чернов, А. А. Сычугов, А. В. Чернова // Союз машиностроителей России. Национальная научно-техническая конференция. №1. 2025. – С. 26-31.

6. Chernov D. Determining the Hazard Quotient of Destructive Actions of Automated Process Control Systems Information Security Violator / Chernov D., Sychugov A. // 2020 International Russian Automation Conference (RusAutoCon), Sochi, Russia. 2020. – P. 566-570.

7. Chernov D. Definition of Protective Measures of Information Security of Automated Process Control Systems // 2021 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), 17-21 May, Sochi, Russia. 2021. – P. 1-5.

8. Chernov D. Application TRIKE methodology when modeling threats to APCs information security // Lecture Notes in Electrical Engineering, vol 986. Springer, Cham. 2023. – P. 374-385.

9. Свидетельство о государственной регистрации программы для ЭВМ «Моделирование угроз информационной безопасности АСУ ТП». Автор Чернов Денис Владимирович. 18 января 2022 г., РФ, №2022611043. Заявка №2022610172.

В диссертации отсутствуют недостоверные сведения об опубликованных соискателем ученой степени работах, в которых изложены основные научные результаты диссертации; соискатель ссылается на авторов и источники заимствования.

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

– **ведущей организации** автономной некоммерческой организации «Институт инженерной физики», г. Серпухов. *Замечания:* 1. В автореферате указано наличие 7 приложений, в то время как в тексте диссертации содержатся 9 приложений. 2. В первой главе на странице 36 приводится описание термина уязвимое звено. Можно было подробнее рассмотреть существующие способы их выявления. 3. В первой и второй главах рассмотрены различные методы и алгоритмы моделирования угроз БИ. Несомненно, результаты проведенных при этом экспериментов позволили автору выделить ряд наиболее эффективных методов оценки актуальности и опасности реализации угроз БИ. Но хотелось бы видеть более четкие выводы, каким конкретно методам и почему будет предпочтение в последующих главах работы. 4. В тексте диссертации не указано в каком формате используется база данных угроз БИ. 5. В таблице 3.2 диссертации на странице 89 приводятся сокращение КЗ и ОКЗ. Если для аббревиатуры ОКЗ приведена расшифровка, то для сокращения КЗ расшифровка отсутствует. 6. В таблице 4.12 приводится перечень защитных мер, необходимых к внедрению в ОКИИ в целях устранения выявленных актуальных угроз. Однако далее в тексте не приводятся наименования конкретных средств защиты информации и их производителей необходимых к внедрению. 7. Из текста диссертации не вполне

ясно, должна ли предлагаемая система моделирования угроз использоваться в качестве основной системы оценки опасности реализации угроз безопасности информации для объекта КИИ или же в качестве дополнения к существующим системам. 8. В явном виде не указаны требуемые вычислительные ресурсы, необходимые для реализации, предложенной в работе автоматизированной системы.

– **официального оппонента** доктора технических наук, профессора Ложникова Павла Сергеевича, заведующего кафедрой «Комплексная защита информации» федерального государственного автономного образовательного учреждения высшего образования «Омский государственный технический университет». *Замечания*: 1. Во введении (раздел 1.4) описаны различные методы оценки потенциала нарушителя БИ ОКИИ, а именно методика регулятора и методика ранжирования. В тоже время, предложенные в работе методы определения потенциала нарушителя и оценки опасности реализации ими угроз БИ ориентированы на ОКИИ. Насколько предложенные методы могут быть адаптированы для других критически важных объектов инфраструктуры (например, объектов ТЭК или финансового сектора), где также присутствуют многоуровневые системы? В чем будут основные ограничения такой адаптации? 2. В диссертации на странице 57 в таблице 2.4. предложены границы градаций критерия значимости технологического процесса на основании строгих интервальных диапазонов для каждой лингвистической оценки значимости свойства технологического процесса. Каким образом получены указанные значения? 3. В диссертации на странице 60 приводится описание значения идентификатора в случае если уязвимость в ОКИИ не выявлена. Идет ли в этом случае речь об уязвимостях нулевого дня? 4. Английские аббревиатуры систематически вводятся без расшифровки, например, CVSS на стр. 28 или названия классов задач резки TRIKE, PASTA, STRIDE, NIST и т. д.) на стр. 37. Часть из них приведена в списке сокращений на стр. 132, но не все. 5. На стр. 61 произведение векторов $G_{k,n}$ и $A_{k,m}$ определяет матрицу защищенности уязвимого звена на каждом из k – уровней АСУ ТП, хотя речь во второй главе идет об ОКИИ.

Указанное замечание справедливо и для рис. 3.2 стр. 77 блока «Сбор информации об АСУ ТП» алгоритма работы сканера безопасности.

– **официального оппонента** доктора технических наук, доцента Максимовой Елены Александровны, заведующего кафедрой КБ-4 «Интеллектуальные системы информационной безопасности» федерального государственного бюджетного образовательного учреждения высшего образования «МИРЭА– Российский технологический университет». *Замечания*: 1. В работе описана методика ранжирования потенциальных нарушителей (стр. 27 диссертации) и рейтинговый метод оценки угроз, исходящих от нарушителей на основании которых делается вывод о необходимости разработки метода и алгоритма определения потенциала нарушителя, учитывающего возможные негативные последствия от атак. При этом в литературе описан ряд способов, методов и методик определения потенциала нарушителя безопасности информации на основании реализуемых им уязвимостей программного обеспечения. Таким образом, недостаточно дать только оценку ущерба от реализации атак, но и учитывать эксплуатация каких уязвимостей приводит к указанному ущербу. 2. Не рассмотрено применение предложенных методов и алгоритмов для моделирования угроз объектов КИИ, имеющих ту или иную категорию значимости, что позволило бы расширить область применения разработанной автоматизированной системы. 3. Основной акцент работы направлен на угрозы БИ, представленные в отечественных банках данных угроз. При этом не рассмотрен вопрос применения зарубежных источников описаний угроз и уязвимостей программных, аппаратных и программно-аппаратных средств (MITRE ATT&CK, CAPEC и пр.). 4. При разработке метода количественной оценки опасности реализации угроз (стр. 51 диссертации) не приводится описание множества угроз. Не полностью раскрыто как оценивается вероятность того, что угроза будет реализована в ОКИИ. 5. В тексте диссертационной работы (стр. 60 диссертации) вектор, отражающий возможные уязвимые звенья, формируется в зависимости от отсутствия или наличия информации о конкретной уязвимости по результатам работы сканера безопасности. Из текста диссертации непонятно, о каких конкретно уязвимостях идет речь, включают ли они в себя уязвимости

нулевого дня? 6. Считаю излишним представление в тексте диссертации листинга программного кода (Приложение 7, стр. 174-197 диссертации), так как скан свидетельства о государственной регистрации соответствующей программы расположен в Приложении 8 (стр. 198-199 диссертации). 7. В тексте диссертации некорректно выполнены: междустраничные переносы таблиц (таблицы 1.1, 1.2, 1.6 и др.), оформление названий рисунков (рис. 1.1-1.6), оформление ряда названий пунктов (стр. 14, 21, 27, 32, 35 и т.д.). 8. В тексте диссертационной работы не в полном объеме представлены ссылки на публикации соискатели, что затрудняет понимание того, в каких работах автора представлены полученные основные научные результаты.

Получено **семь положительных** отзывов на автореферат:

1. **Федеральное государственное автономное образовательное учреждение высшего образования «Томский государственный университет систем управления и радиоэлектроники»** (г. Томск), Президент ФГАОУ ВО «Томский государственный университет систем управления и радиоэлектроники», директор Института системной интеграции и безопасности, член-корреспондент Российской академии наук, доктор технических наук, **Шелупанов Александр Александрович.** *Замечания:* 1. Из автореферата неясно, обоснование выбора модели игры Штакельберга в качестве основы для экспертной оценки степени опасности реализации угроз, не указаны преимущества и достоинства данной модели, не представлен и сравнительный анализ существующих методов и подходов. 2. Учитывая относительно широкий круг вопросов, предлагаемый экспертной комиссии для оценки действий нарушителей и текущей защищенности объекта КИИ, возникает правомерный вопрос, как предложенные методы и алгоритмы моделирования угроз справляются с увеличением количества опрошенных экспертов?

2. **Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М. В. Ломоносова»** (г. Москва), кандидат физико-математических наук, доцент кафедры информационной безопасности факультета

вычислительной математики и кибернетики **Чижов Иван Владимирович.** *Замечания:* 1. На странице 13 автореферата приводится аббревиатура СРВ, описание которой отсутствует в тексте. 2. Не раскрыт состав разработанных программных средств, не указаны используемые языки программирования. 3. В автореферате при описании методов количественной оценки опасности реализации угроз и защищенности уязвимых звеньев используются достаточно сложные математические зависимости (формулы (3)-(8), (10)-(13)), однако не всегда ясно, какова чувствительность итоговых оценок к выбору экспертных весов и параметров. Представление краткого анализа устойчивости или влияния ключевых параметров повысило бы убедительность полученных результатов.

3. **Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет»** (г. Таганрог), кандидат технических наук, доцент, заведующий кафедрой безопасности информационных технологий **Абрамов Евгений Сергеевич**. *Замечания:* 1. В работе делается акцент на применимость разработанных методов для «незначимых» объектов КИИ. Однако из текста автореферата не совсем ясно, существуют ли принципиальные ограничения для использования предложенной методики и ПО АС «МУИБ» для моделирования угроз в отношении значимых объектов КИИ (первой, второй или третьей категории), или же методика является универсальной. 2. На странице 14 приводится сравнительная оценка эффективности моделирования угроз, где разработанная АС «МУИБ» показывает значительное преимущество по показателю «ВЗ» (время затраченное). Хотелось бы уточнить, учитывает ли данный показатель время, необходимое на предварительную подготовку экспертов и заполнение ими анкет, так как предложенный метод опирается на групповое экспертное оценивание, что организационно может быть затратным процессом.

4. **Федеральное государственное бюджетное образовательное учреждение высшего образования «Новосибирский государственный технический университет»** (г. Новосибирск), кандидат технических наук, доцент, заведующий кафедрой защиты информации **Иванов Андрей Валерьевич**.

Замечания: 1. Автореферат не содержит достаточного анализа вычислительной сложности предложенных алгоритмов, что не позволяет полно и точно оценить эффективность метода в условиях с ограниченными вычислительными ресурсами; 2. В работе недостаточно раскрыты вопросы масштабируемости предложенных методов и алгоритмов при увеличении количества возможных нарушителей режима безопасности информации незначимого объекта КИИ выше экспериментально исследованных десяти.

5. **Федеральное государственное бюджетное образовательное учреждение высшего образования «Рязанский государственный радиотехнический университет имени В. Ф. Уткина»** (г. Рязань), кандидат технических наук, доцент кафедры Информационная безопасность **Конкин Юрий Валериевич**. *Замечания:* 1. Наименования осей графика и их значения на рисунке 5 автореферата выполнены слишком мелко, что затрудняет его читабельность. 2. В таблице 5 на странице 14 автореферата приводятся сокращения ИАФ, УПД, ОПС, ЗНИ и другие без описания в тексте автореферата. 3. Недостаточное описание в тексте автореферата алгоритма определения потенциала нарушителя, приведенного на рисунке 1.

6. **Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный технический университет»** (г. Самара), кандидат технических наук, доцент, заведующий кафедрой «Электронные системы и информационная безопасность» **Карпова Надежда Евгеньевна.** *Замечания:* 1. Из текста автореферата не понятно, каким образом получены данные сравнительных результатов работы предложенного решения с альтернативными методиками моделирования угроз 2. На стр. 14 автореферата указано, что случае моделирования угроз для ОКИИ – информационных систем или информационной-телекоммуникационных сетей необходимо рассматривать только уровень 1 в качестве возможного для реализации актуальных угроз потенциальными нарушителями, однако не указано верхний уровень или полевой рассматривается в качестве первого. Указанное замечание справедливо также и для таблицы 2 автореферата.

7. **Федеральное государственное бюджетное образовательное учреждение высшего образования «Владивостокский государственный университет»** (г. Владивосток), кандидат экономических наук, доцент, заведующий кафедрой информационной безопасности **Шумик Екатерина Георгиевна.** *Замечания:* 1. В автореферате описан способ определения уровней значимости технологических процессов на основании оценки совокупности их свойств в соответствии с функцией желательности Харрингтона, однако явно не указано, используется ли данный способ для оценки уровня значимости информационного процесса. 2. В тексте автореферата явно не указано, какие меры обеспечения безопасности объекта КИИ реализует разработанное программное обеспечение, согласно требованиям Приказа ФСТЭК № 239.

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. Ведущая организация и оппоненты не имеют совместных проектов и публикаций с соискателем.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- предложены: метод определения потенциала нарушителя информационной безопасности объекта критической информационной инфраструктуры (ИБ ОКИИ), основанный на применении матриц идентификаторов угроз. Метод позволяет выявить и количественно оценить располагаемый потенциал возможных нарушителей ИБ, что, в свою очередь, позволяет повысить достоверность и объективность анализа и оценки актуальных угроз безопасности информации. Главным отличием от существующих методов является применение предложенного подхода к групповой оценке потенциалов нарушителей согласованным количеством экспертов; метод количественной оценки степени опасности реализации угроз безопасности информации ОКИИ, основанный на интеллектуальном анализе данных, имеющихся в подсистеме журналирования. Метод позволяет количественно оценить степень опасности реализации угроз БИ

потенциальными нарушителями применительно к конкретному ОКИИ. Разработанный метод дополняет располагаемые оценки специалистов в области ИБ путем формирования экспертных оценок со стороны дополнительно привлекаемых профильных специалистов в области КИИ;

– **разработаны**: алгоритм определения и оценки защищенности уязвимых звеньев ОКИИ. Алгоритм отличается от известных тем, что использует матрицу защищенности, составленную на основе оценок показателей защищенности уязвимых звеньев, что позволяет повысить объективность выявления актуальных угроз; алгоритм экспертной оценки степени опасности реализации угроз безопасности информации ОКИИ, который, в отличие от существующих, основан на применении игр с несовершенной информацией вида «злоумышленник – система защиты информации», где в качестве возможных выигрышей сторон используются оценки потенциала нарушителя, опасности реализации им угроз БИ, а также оценки защищенности уязвимых звеньев, по отношению к которым потенциальный нарушитель реализует угрозы безопасности информации. Алгоритм позволяет дополнять перечни актуальных угроз безопасности информации, выявленных с использованием известных методик ФСТЭК России;

– **экспериментально доказана** эффективность и обоснованность применения разработанных методов, алгоритмов и автоматизированной системы для решения задачи дополнительной разработки методов и алгоритмов автоматизации моделирования угроз не являющихся значимыми ОКИИ, основанных на развитии риск-ориентированного подхода в направлении обработки больших объемов располагаемой разнородной информации, связанной с оценкой ключевых факторов, влияющих на величину риска и ущерба от реализации угроз, с использованием знаний и опыта как экспертов – специалистов в области ИБ, так и дополнительно привлекаемых на этой стадии профильных экспертов в области ИС, ИТКС, а также АСУ ТП, отличающихся своей многоуровневой структурой.

Теоретическая значимость исследования обоснована тем, что:

– применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) **использованы** методы

интеллектуального анализа данных и защиты информации, методы теории игр, экспертных оценок и системного проектирования SADT;

– **изложены** аргументы и факты, подтверждающие актуальность разработки математических методов и алгоритмов выявления совокупности условий и факторов, которые приводят или могут привести к нарушению безопасности информации (БИ), а также к нарушению или прекращению функционирования ОКИИ, отличающихся своей многоуровневой структурой;

– **раскрыты** недостатки существующих методик моделирования и оценки опасности реализации угроз БИ ОКИИ, а также необходимость повышения объективности и достоверности оценок актуальности угроз и рисков БИ с использованием профессиональных знаний специалистов в области ОКИИ и разработанных методов и алгоритмов обработки этой информации, что в свою очередь позволит оценить влияние основных риск-образующих факторов на последствия (ущерб) от реализации актуальных угроз БИ;

– **изучены** современные подходы к моделированию угроз БИ ОКИИ, уделено внимание нарушителей ИБ и методам оценки их потенциала, а также существующим методам оценки опасности реализации угроз, на основании чего сделан вывод о необходимости программной реализация разработанных методов и алгоритмов, которая позволит создать инструментальные средства автоматизации процесса моделирования угроз БИ, способные дополнять существующие риск-ориентированные подходы и методики в рамках определения нарушителей, представляющих наибольшую опасность для не являющихся значимыми ОКИИ, актуальных угроз БИ, а также возможных контрмер противодействия им с целью минимизации ущерба от реализации угроз БИ, что, в свою очередь, позволит повысить эффективность процесса моделирования угроз БИ и выбора комплекса защитных мер в соответствии с предъявляемыми нормативными требованиями;

– **проведена модернизация** известных методов определения потенциала нарушителя, и защищенности уязвимых звеньев с помощью аппарата экспертных оценок, а также подходов к оценке опасности реализации угроз с использованием

моделирования взаимодействия пары «злоумышленник – СЗИ» в виде игры, основанной на модели Штакельберга.

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

– **разработаны и внедрены** в процессы моделирования угроз БИ ОКИИ в ООО «Комплексы системы и сети», ООО «БД Безопасность», ООО «МК Сервис» и в учебный процесс ФГБОУ ВО «Тульский государственный университет». Разработанное программное обеспечение внедрено в процессы оценки угроз в АО Центральное конструкторское бюро аппаратостроения: метод определения потенциала нарушителя ИБ ОКИИ на основе построения матриц идентификаторов угроз; метод количественной оценки степени опасности реализации угроз БИ ОКИИ потенциальными нарушителями ИБ с использованием оценок вероятностей реализации угроз БИ и ущерба от их реализации; алгоритм определения уязвимых звеньев ОКИИ и оценки их защищенности на основе предложенных матриц защищенности; алгоритм экспертной оценки степени опасности реализации угроз БИ ОКИИ; структура и программное обеспечение автоматизированной системы моделирования угроз БИ ОКИИ;

– **определены** рекомендации по практическому применению результатов диссертационной работы для реализации мероприятия по моделированию угроз БИ с применением средств автоматизации на каждом из уровней ОКИИ и по противодействию актуальным угрозам БИ ОКИИ;

– **разработаны** метод определения потенциала нарушителя ИБ ОКИИ, основанный на применении матриц идентификаторов угроз, метод количественной оценки степени опасности реализации угроз БИ ОКИИ с использованием оценки вероятностей реализации угроз БИ и ущерба от их реализации, алгоритмы определения и оценки защищенности уязвимых звеньев ОКИИ и экспертной оценки степени опасности реализации угроз БИ ОКИИ, основанные на применении игр с несовершенной информацией, а также структура и программное обеспечение автоматизированной системы моделирования угроз БИ ОКИИ, что обеспечивает повышение эффективности процесса моделирования угроз БИ ОКИИ, выявление актуальных угроз БИ и

дополнительных мер защиты необходимых к внедрению в целях минимизации негативных последствий от реализации актуальных угроз БИ потенциальными нарушителями;

– **представлены** результаты экспериментальной оценки и показатели эффективности применения разработанных методов, алгоритмов и автоматизированной системы подтверждающие практическую значимость предложенных решений. Результаты сравнительной оценки эффективности применения данной системы для конкретной промышленной АСУ ТП показали, что ее применение обеспечивает повышение показателя эффективности построения моделей угроз БИ по соотношению числа выявленных актуальных угроз БИ и предложенных мер по сравнению с другими методиками.

Оценка достоверности результатов исследования выявила:

– **для экспериментальных работ** использованы разработанные диссертантом программные средства, персональные компьютеры, а также специально подготовленные наборы экспертных оценок;

– **теоретическая часть работы** базируется на использовании известных методик, методов, подходов и принципов моделирования угроз БИ, методов интеллектуального анализа данных и защиты информации. Она опирается на результаты вычислительных экспериментов, а также на проверяемые и апробированные данные и факты. Положения согласуются с опубликованными ранее работами и экспериментальными результатами других авторов, что обеспечивает научную обоснованность и преемственность представленных выводов;

– **идея базируется** на результатах анализа современного состояния исследований в области оценки нарушителей и угроз БИ, современных подходах к определению и оценки защищенности уязвимых звеньев, а также анализе современных реализаций систем моделирования угроз БИ, применяемых на ОКИИ;

– **использованы** экспериментальные данные автоматизированной системы управления технологическими процессами, обеспечивающей выпуск продукции, а также наборы угроз БИ, опубликованные в сети связи международного обмена

Интернет, что позволило провести комплексный анализ эффективности предложенных решений. Результаты экспериментальной оценки показали, что предложенные методы и алгоритмы по точности определения актуальных угроз БИ ОКИИ не уступают существующим аналогам, при этом они демонстрируют более высокие показатели эффективности процесса моделирования угроз и числа предлагаемых мер защиты;

– **установлено** совпадение авторских результатов с результатами решений задач моделирования угроз БИ ОКИИ и оценки опасности реализации угроз БИ, представленных в независимых исследованиях, при этом улучшены показатели эффективности построения моделей угроз БИ по соотношению числа выявленных актуальных угроз БИ и предложенных мер защиты, таких как общее количество выявленных актуальных угроз БИ для всех уровней ОКИИ, общее количество мер защиты предложенных для минимизации последствий реализации актуальных угроз БИ, общее количество времени затраченного на получение результатов моделирования угроз.

Личный вклад соискателя состоит: в постановке целей и задач исследования, анализе современного состояния научных разработок в области моделирования угроз безопасности объектов критической информационной инфраструктуры; разработке концепции, методов, алгоритмов и структуры автоматизированной системы моделирования угроз, представленных в диссертационной работе; организации и проведении экспериментов для оценки эффективности предложенных решений; получении и интерпретации результатов на каждом этапе исследования, их апробации и подготовке основных публикаций по теме диссертации.

В целом, диссертация Чернова Дениса Владимировича «Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок» представляет собой завершенную научно-квалификационную работу, в которой содержится решение актуальной научной задачи, заключающейся в разработке методов и алгоритмов

автоматизации моделирования угроз безопасности информации для не являющихся значимыми ОКИИ.

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

– соблюдены установленные Положением о порядке присуждения ученых степеней критерии, которым должна отвечать диссертация на соискание ученой степени кандидата 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 83,12 %.

В ходе защиты диссертации были высказаны следующие критические замечания:

1. В диссертационной работе недостаточно внимания уделено практическим аспектам применения разработанного программного обеспечения, реализующего метод и алгоритмы автоматизации моделирования угроз для конкретных, не являющихся значимыми, объектов КИИ, а также соответствию предложенных решений требованиям регуляторов.

Соискатель Чернов Д. В. согласился с замечанием и привёл собственную аргументацию:

Разработанное программное обеспечение автоматизированной системы моделирования угроз БИ ОКИИ внедрено в производственные процессы обеспечения ИБ на ряде промышленных предприятий и организаций, а также в учебный процесс ФГБОУ ВО «Тульский государственный университет». Результаты сравнительной оценки эффективности применения данной системы для конкретной промышленной АСУ ТП показали, что ее применение обеспечивает повышение показателя эффективности построения моделей угроз БИ по соотношению числа выявленных актуальных угроз БИ и предложенных мер защиты по сравнению с отечественными и зарубежными методиками. Разработанный метод и алгоритмы расширяют возможности действующей

методики ФСТЭК России и позволяют дополнить перечни актуальных угроз, выявляемых с ее помощью.

Результаты внедрены в производственные процессы обеспечения ИБ предприятий, а также в учебный процесс ФГБОУ ВО «Тульский государственный университет».

Диссертационная работа Чернова Дениса Владимировича на тему «Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок» соответствует п. 9 Положения о присуждении ученых степеней (утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842 (в редакции от 25.01.2024 г.), 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 Чернова Д.В. на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, в которой содержатся научно обоснованные результаты решения научной задачи, заключающейся в разработке методов и алгоритмов автоматизации моделирования угроз не являющихся значимыми ОКИИ, основанных на развитии риск-ориентированного подхода в направлении обработки больших объемов располагаемой разнородной информации, связанной с оценкой ключевых факторов, влияющих на величину риска и ущерба от реализации угроз, с использованием знаний и опыта как экспертов в области ИБ, так и дополнительно привлекаемых на этой стадии экспертов в области ИС, ИТКС, а также АСУ ТП,

отличающихся своей многоуровневой структурой, что имеет существенное значение для выбора мер защиты, позволяющих минимизировать негативные последствия от реализации актуальных угроз безопасности информации в условиях возможного воздействия деструктивных факторов.

На заседании 29.01.2026 г. диссертационный совет принял решение:

– за решение актуальной научной задачи, заключающейся в разработке методов и алгоритмов автоматизации моделирования угроз не являющихся значимыми ОКИИ, основанных на развитии риск-ориентированного подхода в направлении обработки больших объемов располагаемой разнородной информации, связанной с оценкой ключевых факторов, влияющих на величину риска и ущерба от реализации угроз, с использованием знаний и опыта как экспертов – специалистов в области ИБ, так и дополнительно привлекаемых на этой стадии профильных экспертов в области ИС, ИТКС, а также АСУ ТП, отличающихся своей многоуровневой структурой, что имеет существенное значение для выбора мер защиты, позволяющих минимизировать негативные последствия от реализации актуальных угроз безопасности информации, присудить Чернову Денису Владимировичу 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 6 доктора наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 18 человек, входящих в состав совета, проголосовали: за – 13, против – 1.

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

Ученый секретарь
диссертационного совета
д-р техн. наук Вульфин Алексей Михайлович

29 января 2026 года