УТВЕРЖДАЮ
проректор по научной работе
ФГБОУ ВО «Тульский государственный университет»
докт. техн. наук, профессор
Воротилин Михаил Сергеевич

«18» июня 2025 г.

ЗАКЛЮЧЕНИЕ

федерального государственного бюджетного образовательного учреждения высшего образования «Тульский государственный университет»

Диссертация «Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок» выполнена на кафедре «Информационная безопасность» федерального государственного бюджетного образовательного учреждения высшего образования «Тульский государственный университет» Министерства науки и высшего образования Российской Федерации.

В период подготовки диссертации соискатель Чернов Денис Владимирович работал в федеральном государственном бюджетном образовательном учреждении высшего образования «Тульский государственный университет» в должности старшего преподавателя кафедры «Информационная безопасность».

В 2014 г. окончил ФГБОУ ВО «Тульский государственный университет» по программе специалитета 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. Отрасль науки - технические науки.

Справка со сведениями о сдаче кандидатских экзаменов выдана в 2025 г. ФГБОУ ВО «Тульский государственный университет».

Научный руководитель – доктор технических наук, доцент Сычугов Алексей Алексеевич, федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет» Министерства науки и высшего образования Российской Федерации, директор института прикладной математики и компьютерных наук, заведующий кафедрой «Информационная безопасность».

По результатам рассмотрения диссертации «Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок» принято следующее.

1. Актуальность темы исследования

В современных условиях технологического развития общества обеспечение информационной безопасности (ИБ) составляет одну из важнейших задач на всех этапах жизненного цикла промышленных систем автоматизации. Критическая информационная инфраструктура (КИИ) стала неотъемлемой частью стратегически важных для государства объектов нефтехимической, энергетической, оборонной, ракетно-космической и других отраслей промышленности, что делает объекты КИИ выгодной мишенью для потенциальных злоумышленников, ставящих своей целью нанести максимально возможный урон технологическим компаниям, отраслям экономики и репутации государства.

В соответствии с положениями Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» к объектам КИИ (ОКИИ) относятся информационные системы (ИС), информационно-телекоммуникационные сети (ИТКС) и автоматизированные системы управления технологическими процессами (АСУ ТП), функционирующие в одной из тринадцати ключевых сфер деятельности (нефтехимической, энергетической, оборонной, ракетно-космической и т.д.). Законом установлена обязанность выполнения владельцами ОКИИ комплекса мероприятий по оценке

их значимости и реализации организационных и технических мер, направленных на обеспечение ИБ ОКИИ.

Одной из важных мер обеспечения ИБ ОКИИ является моделирование угроз безопасности информации (угроз БИ), т.е. выявление совокупности условий и факторов, которые приводят или могут привести к нарушению безопасности обрабатываемой в этих системах информации, а также к нарушению или прекращению функционирования систем и сетей.

Для моделирования угроз БИ ОКИИ, в отношении которых установлена одна из трех категорий значимости, в настоящее время используются хорошо зарекомендовавшие себя риск-ориентированные подходы и методики, например, изложенные в серии стандартов ГОСТ Р ИСО/МЭК 27ххх и «Методике оценки угроз безопасности информации», утвержденной ФСТЭК России от 05.02.2021г (далее – Методика ФСТЭК России от 05.02.2021г.). Указанные стандарты позволяют анализировать угрозы с учетом оценок ущерба от реализации актуальных угроз БИ. Применение существующих подходов и методик определения актуальных угроз БИ, выявления способов их реализации и оценки рисков ИБ требует привлечения высококвалифицированных специалистов в области ИБ, а также значительных временных и иных ресурсов. В современных условиях, с учетом роста масштабов и сложности ОКИИ, в отношении которых не установлена одна из трех категорий значимости (незначимые ОКИИ), при применении вышеуказанных стандартов и методик значительно увеличивается объем разнообразной информации, подлежащей анализу. Это ставит научную задачу дополнительной разработки методов и алгоритмов автоматизации моделирования угроз незначимых 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 экспертов - профессионалов в области ИС, ИТКС, а также АСУ ТП, отличающихся своей многоуровневой структурой.

Решение указанной задачи позволит повысить объективность и достоверность 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. Программная реализация разработанных методов и алгоритмов 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 незначимых 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.

2. Личное участие автора в получении результатов исследования выразилось в следующем.

1. Выполнен анализ нормативно-правовой и терминологической базы обеспечения БИ ОКИИ. Проведена аналитика наиболее крупных атак на промышленную информационную инфраструктуру. Описана многоуровневая структура ОКИИ.

2. Разработан метод определения потенциала нарушителя ИБ ОКИИ, основанный на применении матриц идентификаторов угроз, которые позволяют количественно описать степень опасности реализации угроз БИ для каждого из возможных нарушителей.

3. Предложен метод количественной оценки степени опасности реализации угроз БИ ОКИИ, который в отличие от существующих имеет в основе оценки вероятностей реализации угроз БИ и ущерба от их реализации. Метод позволяет оценить степень опасности реализации угроз БИ потенциальным нарушителем ИБ по отношению к конкретной ИС, ИТКС или АСУ ТП.

4. Разработан алгоритм определения и оценки защищенности уязвимых звеньев ОКИИ. Алгоритм отличается от известных тем, что использует матрицу защищенности, составленную из оценок показателей защищенности отдельных уязвимых звеньев. Разработанный алгоритм позволяет повысить объективность оценки уровня защищенности ОКИИ.

5. Предложен алгоритм экспертной оценки степени опасности реализации. угроз БИ ОКИИ. В отличие от существующих, разработанный алгоритм основан на применении игр с несовершенной информацией вида «злоумышленник-система защиты информации», где в качестве возможных выигрышей сторон используются оценки потенциала нарушителя ИБ, опасности реализации им угроз БИ, а также оценки защищенности уязвимых звеньев, по отношении к которым потенциальный нарушитель реализует угрозы БИ.

6. Разработана структура и программное обеспечение автоматизированной системы моделирования угроз БИ ОКИИ. 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 более, чем в 2,6 раз по сравнению с отечественной методикой ФСТЭК России, и более, чем в 4 раза по сравнению с зарубежной методикой TRIKE.

3. Научная новизна выполненной работы.

1. Предложен метод определения потенциала нарушителя 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 БИ. Главным отличием от существующих методов является применение предложенного подхода к групповой оценке потенциалов нарушителей согласованным количеством экспертов.

2. Предложен метод количественной оценки степени опасности реализации угроз БИ ОКИИ, основанный на интеллектуальном анализе данных, имеющихся в подсистеме журналирования. Метод позволяет количественно оценить степень опасности реализации угроз БИ потенциальными нарушителями ИБ применительно к конкретному ОКИИ. Разработанный метод дополняет располагаемые оценки специалистов в области ИБ путем формирования экспертных оценок со стороны дополнительно привлекаемых специалистов - профессионалов в области КИИ.

3. Разработан 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.

4. Предложен алгоритм экспертной оценки степени опасности реализации угроз БИ 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 БИ. Предложенный алгоритм позволяет дополнять перечни актуальных угроз БИ, выявленных с использованием известных методик ФСТЭК России.

4. Обоснованность и достоверность научных положений, выводов и результатов подтверждается разносторонним изучением современного состояния предметной области, системным обоснованием предложенных методов и алгоритмов, не противоречащих известным положениям других авторов, апробацией полученных результатов в научных публикациях и докладах на международных и российских научно-практических конференциях, а также при решении практических задач моделирования угроз БИ.

5. Теоретическое значение диссертации заключается в разработке новых методов и алгоритмов моделирования угроз БИ, основанных на подходах и инструментарии методов интеллектуального анализа данных и защиты информации, методов теории игр, экспертных оценок и системного проектирования SADT.

Результаты диссертационного исследования внедрены в учебном процессе кафедры ИБ при проведении лекционных курсов, лабораторных работ, а также при выполнении курсового проектирования по направлению бакалаврской подготовки 10.03.01 «Информационная безопасность», специальности 10.05.03 «Информационная безопасность автоматизированных систем».

Полученные в диссертации теоретические результаты могут быть использованы для дальнейшего решения теоретических и практических задач в области разработки методов моделирования угроз БИ ОКИИ.

6. Практическая ценность результатов работы. Предложенные методы и алгоритмы были успешно использованы автором для моделирования угроз БИ в АО ЦКБА, ООО «Комплексы системы и сети» и ООО «БД Безопасность». Разработанное программное обеспечение внедрено в процессы оценки угроз объектов КИИ АО «НПО «Высокоточные комплексы».

7. Апробация работы. Основные положения диссертационной работы легли в основу докладов на следующих конференциях: IV Международная научно-техническая конференция «Вопросы кибербезопасности, моделирования и обработки информации в современных социотехнических системах» (Курск, 2018); Международная научно-техническая конференция «Автоматизация» RusAutoCon (Сочи, 2019, 2020, 2021, 2022); 12-я Международная конференция по безопасности информации и сетей, SINConf 2019 (Сочи, 2019); Международная научно-практическая конференция «Электротехнические комплексы и системы» ICOECS 2019 (Уфа, 2019); Международная научно-техническая конференция «Пром-Инжиниринг» ICIEAM (Сочи, 2023, 2024); XIV Национальная научно-техническая конференция (Москва, 2024).

8. Обоснование выбранной специальности и отрасли науки диссертации

Диссертация «Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок» соответствуют следующим пунктам паспорта научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»:

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»

Отрасль науки – технические науки, поскольку приведенные результаты исследований в области безопасности информации существенно повышают эффективность процесса моделирования угроз информационной безопасности ОКИИ при использовании и внедрении указанных результатов.

9. Основные положения диссертационной работы достаточно полно отражены в 30 научных работах, в том числе 4 в изданиях, рекомендованных в Перечне ВАК РФ, 10 в изданиях, входящих в международные базы данных цитирования SCOPUS и Web of Science, 16 научных работах в других изданиях, сборниках трудов и материалах конференций, получено 1 свидетельство о государственной регистрации программы для ЭВМ.

Статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК

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. 81-87. ВАК (Технические науки).

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

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. ВАК (Технические науки).

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. ВАК (Технические науки).

Публикации в изданиях, индексируемых в Web of Science и Scopus

5. Chernov D. Mathematical modeling of information security threats of automated process control systems / Chernov D., Sychugov A. // 2019 International Conference on Electrotechnical Complexes and Systems (ICOECS), Ufa, Russia. 2019. – P. 1-4.

6. Chernov D., Sychugov A. Method of identifying and assessing of automated process control systems vulnerable elements // In Proceedings of the 12th International Conference on Security of Information and Networks (SIN '19). ACM, New York, NY, USA, Article 19. 2019. – P. 1-4.

7. Chernov D., Sychugov A. Problems of information security and availability of automated process control systems // 2019 International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2019. 2019. – P. 1-4.

8. Chernov D., Sychugov A. Development of a Mathematical Model of Threat to Information Security of Automated Process Control Systems // 2019 International Russian Automation Conference (RusAutoCon), Sochi, Russia. 2019. – P. 1-5.

9. Chernov D., Sychugov A. Application of the method of determining the degree of danger of destructive actions to solve the problem of information security of APCs // 2020 International Conference on Electrotechnical Complexes and Systems (ICOECS), Ufa. 2020. – P. 1-4.

10. Chernov D., Sychugov A. Method of determining the danger coefficient of actions of the information security offender of APCs // IOP Conference Series: Materials Science and Engineering. № 919(5), 2020. – P. 1-6.

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

12. 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.

13. Chernov D. Application TRIKE methodology when modeling threats to APCs information security // 2021 International Russian Automation Conference (RusAutoCon), Sochi, Russia. 2022. – P. 1-5.

14. Chernov, D., Sychugov, A., Sovgir, A. Applying a System of Automatic Threat Modeling for APCs at Information Infrastructure Facilities // Lecture Notes in Electrical Engineering, vol 986. Springer, Cham. 2023. – P. 374-385.

В других изданиях, сборниках трудов и материалах конференций:

15. Чернов Д.В., Сычугов А.А. Формализованное представление потенциала нарушителя информационной безопасности АСУ ТП // Научный журнал. Вопросы кибербезопасности, моделирования и обработки информации в современных социотехнических системах. Вып. 6, 2018. – С. 49-55.

16. Чернов Д.В., Сычугов А.А. Современные подходы к обеспечению информационной безопасности АСУ ТП // Известия тульского государственного университета. Технические науки. Вып. 10, 2018. – С.58-64.

17. Чернов Д.В., Сычугов А.А. Формализация модели нарушителя информационной безопасности АСУ ТП // Известия тульского государственного университета. Технические науки. Вып. 10, 2018. – С. 22-27.

18. Чернов Д.В., Сычугов А.А. Анализ современных требований и проблем обеспечения информационной безопасности автоматизированных систем управления технологическими процессами // Нейрокомпьютеры. Разработка, применение. М.: Радиотехника, №8, 2018. – С. 38-46.

19. Чернов Д.В., Сычугов А.А. Метод определения и оценки уязвимых звеньев автоматизированных систем управления технологическими процессами // Радиотехника. Научный журнал. М.: Радиотехника. Том 83, №8(11), 2019. – С. 67-74.

20. Чернов Д.В., Сычугов А.А., Анчишкин А.П. Метод анализа состояния технологических процессов // Радиотехника. Научный журнал. М.: Радиотехника. №8(11), 2019. – 59-66.

21. Чернов Д.В., Сычугов А.А. Формализованное представление модели угроз информационной безопасности АСУ ТП // Радиотехника. Научный журнал. М.: Радиотехника. Том 83, №6(7), 2019. – С. 74-80.

22. Чернов Д.В., Сычугов А.А. Определение коэффициента опасности деструктивных действий нарушителя информационной безопасности АСУ ТП // Информационно-измерительные и управляющие системы. М.: Радиотехника. №4, 2020. – С. 49-57.

23. Чернов Д.В., Сычугов А.А. Определение коэффициента опасности деструктивных действий нарушителя информационной безопасности // Фундаментальные проблемы управления производственными процессами в условиях перехода к индустрии 4.0. Челябинск: Издательский центр ЮУрГУ. 2020. – С. 206-207.

24. Чернов Д.В., Сычугов А.А. О комплексном подходе к построению системы информационной безопасности АСУ ТП // Технологические инновации и научные открытия. Сборник научных статей по материалам IV Международной научно-практической конференции. Уфа: Изд. НИЦ Вестник науки, 2020. – С. 53-57.

25. Чернов Д.В., Сычугов А.А. Оценка действий нарушителя информационной безопасности автоматизированной системы управления технологическими процессами // Инновационные научные исследования в современном мире: теория, методология, практика / Сборник научных статей по материалам III Международной научно-практической конференции. Уфа: Изд. НИЦ Вестник науки, 2020. – С. 64-69.

26. Chernov D., Sychugov A. Method of determining the danger coefficient of actions of the information security offender of APCS // International scientific conference CAMSTECH-2020: Advances in material science and technology, Krasnoyarsk Science and Technology City Hall. Krasnoyarsk, Russia, 2020. – С. 1-5.

27. Совгирь А.В., Чернов Д.В. Анализ процессов управления инцидентами информационной безопасности. // Материалы XX Всероссийской научно-технической конференции «Техника XXI века глазами молодых ученых и специалистов» / под. ред. А.В. Прохорцева. Тула: Изд-во ТулГУ, 2022. – С. 390-395.

28. Чернов Д.В. Современные подходы к анализу угроз информационной безопасности в условиях цифровизации общества // Промышленная революция 4.0: взгляд молодежи: Тезисы докладов Юбилейной 5-ой межрегиональной научной сессии молодых исследователей, Тула, 20–22 ноября 2023 года. – Тула: Тульский государственный университет, 2023. – С. 258-260.

29. Чернов Д.В., Котов В.В., Борзенкова С.Ю. Построение комплексной системы информационной безопасности АСУ ТП // Машиностроение: сетевой электронный научный журнал. Т.10, №2. 2023. – С. 27-32.

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

Свидетельства о государственной регистрации программы для ЭВМ:

1. Свидетельство о государственной регистрации программы для ЭВМ № 2022611043. Моделирование угроз информационной безопасности АСУ ТП / Чернов Д.В., Сычугов А.А. – заявл. 11.01.2022; зарег. 18.01.2022.

Диссертация Чернова Дениса Владимировича соответствует п. 14 Положения о порядке присуждении ученых степеней:

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

- соискатель ссылается на авторов и источники заимствования.

Личный вклад соискателя в работы, опубликованные в соавторстве:

В работах |17|, |23|, |26| предложены основные математические зависимости, положенные в основу метода количественной оценки опасности деструктивных действий потенциального нарушителя БИ АСУ ТП, относящихся к ОКИИ, на базе вычислений критичности по методике анализа видов и последствий потенциальных дефектов FMEA.

В работе |20| проанализированы существующие методы отбора признаков. Проведены экспериментальные исследования метода анализа состояния технологических процессов.

В работах |6|, |19| предложен и математически описан подход к поиску уязвимых элементов в АСУ ТП, относящихся к ОКИИ на основе внешних факторов и вероятностей реализации уязвимостей в отношении уязвимых звеньев.

В работах |5|, |15| смоделирован подход к защите автоматизированных систем управления технологическими процессами на основе игры Штакельберга в

стратегической форме. Разработана абстрактная математическая модель угроз БИ АСУ ТП, относящихся к ОКИИ.

В работах |16|, |24| предложены методологические и технические принципы построения комплексных систем обеспечения БИ АСУ ТП, относящихся к ОКИИ.

В работах |10|, |21| получены математические зависимости, положенные в основу разработанных методов определения потенциальных нарушителей БИ АСУ ТП, относящихся к ОКИИ.

В работе |14| разработаны структура и программная реализация автоматизированной системы моделирования угроз БИ ОКИИ.

В работах |7|, |18| разработана схема требований к организационным и техническим мерам защиты информации АСУ ТП, относящихся к ОКИИ. Сформулирована математическая модель метода решения задачи определения вероятности появления нештатной ситуации в ОКИИ.

В работах |9|, |11| разработан подход к постановке задачи определения коэффициента опасности деструктивных действий потенциальных нарушителей АСУ ТП, относящихся к ОКИИ, позволяющий оценить вероятность реализации злоумышленником атаки на один из уровней АСУ ТП, а также получены основные математические зависимости.

В работах |8|, |25| провел анализ вербальных и вероятностных методов определения оценок опасности реализации угроз БИ потенциальными нарушителями. Предложен метод определения оценки, основанный на анализе уровня ущерба, превышение которого приведет к неконтролируемым последствиям для функционирования АСУ ТП, относящихся к ОКИИ.

В работе |27| предложены этапы процесса реагирования на угрозы БИ ОКИИ.

В работах |2|, |29| предложен и формализован комплексный подход к построению системы БИ АСУ ТП, относящихся к ОКИИ.

В работе |30| проведен анализ результатов применения автоматизированной системы в рамках обеспечения БИ субъектов КИИ. Анализ проведен на основании качественных и количественных критериев оценки, полученных от специалистов в области БИ, уполномоченных на выполнение процессов моделирования угроз ОКИИ.

Из работ, опубликованных в соавторстве, соискателем в диссертации использованы только те положения, которые разработаны им лично.

Диссертационная работа Чернова Д.В. имеет научную и практическую значимость и является научно-квалификационной работой, в которой решена актуальная научная задача разработки методов и алгоритмов автоматизации моделирования угроз, 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 объектам КИИ, с использованием знаний и опыта как экспертов - специалистов в области ИБ, так и дополнительно привлекаемых на этой стадии экспертов - профессионалов в области КИИ. Указанная научная задача имеет важное значение для обеспечение информационной безопасности субъектов критической информационной инфраструктуры Российской Федерации.

Диссертация соответствует требованиям, предъявляемым к кандидатским диссертациям, согласно п. 9-14 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г. (с последующими изменениями).

Диссертация «Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок» Чернова Дениса Владимировича рекомендуется к защите на соискание ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Заключение принято на расширенном заседании кафедры «Информационная безопасность» федерального государственного бюджетного образовательного учреждения высшего образования «Тульский государственный университет» Министерства науки и высшего образования Российской Федерации.

Присутствовало на заседании 15 чел. Результаты голосования: «за»-15 чел., «против»-0 чел., «воздержалось»- 0 чел. протокол №13 от «08» 07 2025 г.

Зам. заведующего кафедрой
«Информационная безопасность»,
д.т.н., профессор Токарев Вячеслав Леонидович

Секретарь Кузнецова Ольга Алексеевна

Подпись Токарева В.Л., Кузнецовой О.А.
Специалист по кадровой работе
Докторова С.Н.
"08" 07 2025