ОТЗЫВ

на автореферат диссертации Чернова Дениса Владимировича «Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок», представленной на соискание учёной степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Актуальность темы исследования

Тема диссертационной работы Д.В. Чернова является чрезвычайно актуальной в свете современных вызовов, стоящих перед Российской Федерацией. Обеспечение безопасности объектов критической информационной инфраструктуры (КИИ) – приоритетная государственная задача. В условиях постоянного роста сложности кибератак и увеличения их количества, особенно на промышленные системы автоматизации (АСУ ТП), существующие методические подходы требуют адаптации и автоматизации. Автор справедливо отмечает необходимость совершенствования процессов моделирования угроз, особенно для объектов, не имеющих присвоенной категории значимости (незначимые ОКИИ), которые составляют значительный пласт инфраструктуры и часто становятся «точкой входа» для злоумышленников.

Научная новизна и значимость полученных результатов

Автором проведена серьёзная научная работа, в ходе которой получены новые результаты:

1. Разработан метод определения потенциала нарушителя, базирующийся на матрицах идентификаторов угроз, что позволяет формализовать и количественно оценить возможности злоумышленников.

2. Предложен интересный подход к оценке опасности реализации угроз с использованием теоретико-игрового моделирования (модель Штакельберга), что позволяет учитывать стратегическое поведение как атакующего, так и системы защиты.

3. Разработан алгоритм оценки защищённости уязвимых звеньев, учитывающий специфику многоуровневых АСУ ТП.

4. Практическая значимость подтверждается созданием программного комплекса АС «МУИБ» и его успешным внедрением в учебный процесс и деятельность ряда организаций, что подтверждено актами внедрения.

Научная значимость заключается в развитии теоретических основ и методического аппарата информационной безопасности для объектов критической информационной инфраструктуры (КИИ).

Практическая ценность заключается в создании прикладного инструментария, который реально повышает эффективность работы специалистов по информационной безопасности.

Обоснованность и достоверность научных положений, выводов и рекомендаций подтверждаются следующими фактами:

1. Системным обоснованием: Предложенные методы и алгоритмы базируются на глубоком анализе предметной области и не противоречат известным научным положениям других авторов. Использован проверенный математический аппарат (теория игр, экспертные оценки, системный анализ).

2. Апробацией в научной среде: Основные результаты докладывались и обсуждались на ряде международных и всероссийских научно-технических конференций (в период с 2018 по 2024 гг.).

3. Публикациями: По теме диссертации опубликовано 30 научных работ.

4. Практическим внедрением: Разработанные методы и ПО (АС «МУИБ») внедрены в производственные процессы ряда организаций и ВУЗов.

5. Грантовой поддержкой: Работа была поддержана грантом РФФИ (№ 19-07-01107\19) и грантом РТУ МИРЭА (№ 15/2020).

Замечания по автореферату

Несмотря на общее высокое качество работы и несомненную практическую ценность, по тексту автореферата можно сделать следующие 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.

Указанные замечания носят уточняющий характер и не снижают общей высокой оценки диссертационного исследования.

Заключение

Судя по автореферату, диссертация Чернова Дениса Владимировича является завершённой научно-квалификационной работой, выполненной на высоком уровне. Автором решена важная научно-техническая задача повышения эффективности моделирования угроз безопасности информации объектов КИИ.

Работа соответствует паспорту специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность», а также требованиям «Положения о присуждении учёных степеней», предъявляемым к диссертациям на соискание учёной степени кандидата наук.

Считаю, что Чернов Денис Владимирович заслуживает присуждения искомой учёной степени кандидата технических наук по специальности 2.3.6.

Отзыв на диссертацию и автореферат обсуждён и одобрен «24» декабря 2025 г. на заседании кафедры безопасности информационных технологий ФГАОУ ВО «Южный федеральный университет», протокол № 8.

Зав. кафедрой безопасности информационных технологий
Южного федерального университета
кандидат технических наук, доцент
Абрамов Евгений Сергеевич

Е.С. Абрамов
24.12.2025

Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет»
344006, Российская Федерация, Ростовская область, г. Ростов-на-Дону, ул. Большая Садовая 105/42
+7 (863) 305-19-90
info@sfedu.ru

Федеральное государственное автономное образовательное учреждение высшего образования «ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Личную подпись Е.С. Абрамова
ЗАВЕРЕНО:
Начальник сектора
С.А. Остренко
24 12 2025

Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» ОГРН 1026103165241
Управление делами и кадровой работы
14