Отзыв официального оппонента

доктора технических наук, профессора Ложникова Павла Сергеевича на диссертационную работу Чернова Дениса Владимировича **«Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок»,** представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Актуальность темы исследования

В современных условиях безопасность информации (БИ) является критически важным элементом для промышленных систем. Стратегически важные объекты энергетики, нефтехимии и оборонной промышленности имеют в своем составе и эксплуатируют объекты критической инфраструктуры (ОКИИ). Это привлекает злоумышленников, чьи цели эволюционировали от вреда отдельным компаниям до дестабилизации целых отраслей экономики и реализации угроз национальной безопасности.

Правовое поле для обеспечения БИ КИИ в Российской Федерации определяется положениями Федерального закона от 26.07.2017 № 187-ФЗ, который идентифицирует в качестве ОКИИ информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами (АСУ ТП), функционирующие в тринадцати критически важных сферах. Законодатель возлагает на собственников ОКИИ обязательства по проведению комплекса мероприятий, включая оценку их значимости и реализацию организационно-технических мер по защите.

С методологической точки зрения, одним из фундаментальных элементов обеспечения БИ ОКИИ является процедура моделирования угроз БИ. Данная процедура представляет собой системное выявление совокупности условий и детерминирующих факторов, способных привести к

нарушению конфиденциальности, целостности, доступности обрабатываемой информации, а также к сбоям или полному прекращению функционирования самих систем.

Для ОКИИ, в отношении которых установлена одна из трех категорий значимости, апробированным инструментарием моделирования угроз выступают риск-ориентированные подходы, регламентированные, в частности, серией стандартов ГОСТ Р ИСО/МЭК 27ххх и «Методикой оценки угроз безопасности информации» ФСТЭК России (2021 г.). Указанные нормативно-методические документы позволяют проводить анализ угроз через призму оценки потенциального ущерба от их реализации. Однако их практическое применение сопряжено с необходимостью привлечения высококвалифицированных специалистов в области БИ и значительными ресурсными затратами.

Актуализируется проблема в условиях роста масштабов и структурной сложности ОКИИ, не отнесенных к категории значимости (так называемые «незначимые» ОКИИ). Применение к ним классических методик приводит к экспоненциальному росту объема и номенклатуры анализируемых данных. В этой связи, возникает научная задача разработки специализированных методов и алгоритмов для автоматизации моделирования угроз именно для данной категории объектов. Перспективным вектором развития риск-ориентированного подхода в данном контексте видится создание механизмов обработки больших массивов гетерогенной информации, связанной с оценкой ключевых факторов риска и ущерба. Это требует синтеза знаний и экспертизы не только со стороны специалистов по БИ, но и активного привлечения профильных экспертов в смежных областях — информационных системах, телекоммуникациях и, что особенно важно, в области многоуровневых и структурно сложных АСУ ТП.

Соответствие паспорту научной специальности

Рассмотренные в диссертации Чернова Д. В. вопросы связаны с повышением эффективности процесса моделирования угроз БИ ОКИИ. Объект исследования, его цель и задачи, направления теоретических и экспериментальных исследований, а также область исследования соответствует 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».

Структура и объём диссертации

Диссертация изложена на 148 страницах, состоит из введения, четырёх глав, заключения, списков сокращений, литературы, иллюстраций и таблиц и девяти приложений. Список литературы включает 121 источник на русском и английском языках. Структура и оформление диссертации соответствуют требованиям ГОСТ Р 7.0.11-2011 «Система стандартов по информации, библиотечному и издательскому делу. Диссертация и автореферат диссертации. Структура и правила оформления».

Во *введении* обоснована актуальность и степень разработанности темы исследования, сформулированы цель и задачи работы, показана научная новизна, теоретическая и практическая значимость работы, приведены её апробация, основные положения, выносимые на защиту.

В *первой главе* проведен анализ современного состояния исследований

в области автоматизации процесса моделирования и определения актуальных угроз БИ ОКИИ, рассматриваются современные подходы к моделированию угроз БИ, включающие в себя методы оценки нарушителей и угроз, а также методы выбора защитных мер. Рассматриваются задачи оценки вероятных нарушителей и процесса моделирования угроз БИ. Выделяются основные метрики квалификации и мотивации потенциальных нарушителей БИ ОКИИ.

Во *второй главе* описываются методы, позволяющие проводить мероприятия по моделированию угроз БИ ОКИИ. Предложен метод определения потенциала нарушителя ИБ ОКИИ на основе построения матриц идентификаторов угроз. В качестве идентификаторов угроз в предложенном методе выступают способы реализации УБИ, представленные в Методике ФСТЭК России от 05.02.2021г. Предложены методы количественной оценки степени опасности реализации угроз БИ ОКИИ потенциальными нарушителями ИБ, оценки защищенности уязвимых звеньев ОКИИ и экспертной оценки степени опасности реализации угроз БИ ОКИИ с применением модели игры Штакельберга.

В *третьей главе* осуществляется алгоритмизация процесса построения модели угроз БИ ОКИИ. Данный процесс базируется на анализе потенциала нарушителей, степени опасности исходящих от них угроз и уровня защищенности выявленных уязвимостей. Были разработаны алгоритмы для сканирования безопасности, анализа рисков реализации угроз БИ и оценки защищенности уязвимых элементов. Интеграция указанных алгоритмов позволила предложить комплексный метод оценки опасности реализации угроз БИ для ОКИИ.

В *четвертой главе* представлена архитектура автоматизированной системы моделирования угроз информационной безопасности для объектов критической информационной инфраструктуры (АС «МУИБ»). Данная система создана для экспериментальной оценки эффективности разработанных методов и алгоритмов. Дается обзор структуры АС «МУИБ», анализируется ее графический интерфейс и ключевой функционал. Кроме

того, приведены результаты тестирования предложенных решений, полученные с помощью данной системы.

В *заключении* представлены основные результаты и выводы диссертации, а также обозначены перспективы дальнейшей разработки темы диссертации.

Диссертация обладает внутренним единством и написана автором самостоятельно.

Научная новизна и теоретическая значимость работы

В диссертационной работе предложены методы, позволяющие выявить и количественно оценить располагаемый потенциал возможных нарушителей ИБ, а также количественно оценить степень опасности реализации угроз БИ потенциальными нарушителями ИБ применительно к конкретному ОКИИ что, в свою очередь, позволяет повысить достоверность и объективность анализа и оценки актуальных угроз БИ. и дополняет располагаемые оценки специалистов в области ИБ путем формирования экспертных оценок со стороны дополнительно привлекаемых специалистов – профессионалов в области КИИ. Предложенный в данной работе 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, позволяет дополнять перечни актуальных угроз БИ, выявленных с использованием известных методик ФСТЭК России.

Практическая значимость работы

Разработанные алгоритмы и программное обеспечение

автоматизированной системы моделирования угроз БИ ОКИИ, позволяют повысить эффективность построения моделей угроз БИ и выбора состава мер защиты по сравнению с известными методиками. Применение разработанной системы позволяет поддерживать актуальность сведений о возможных угрозах БИ, потенциальных нарушителях ИБ и необходимых СЗИ.

Работа выполнена при финансовой поддержке РФФИ в рамках гранта № 19-07-01107\19 «Разработка математических моделей и методов построения интеллектуальных распределенных адаптивных систем обеспечения ИБ» и РТУ МИРЭА в рамках гранта № 15/2020 «Разработка методов и алгоритмов моделирования угроз БИ», её теоретические и практические результаты внедрены и используются в научно-исследовательском и образовательном процессе в ФГБОУ ВО «Тульский государственный университет», что подтверждается соответствующим актом внедрения.

Степень обоснованности научных положений и достоверности полученных результатов

Обоснованность научных и практических результатов диссертации Чернова Д. В. подтверждена использованием фундаментальных и прикладных работ отечественных и зарубежных учёных по теме исследования, применением современных методов анализа информации, вычислительных методов и программных средств.

Апробация работы и публикации

Основные результаты диссертационной работы были представлены на международных и всероссийских конференциях, по теме диссертации имеется 30 публикаций, включая 4 научных статьи, опубликованных в рецензируемых научных журналах, определённых ВАК, 10 научных публикаций в изданиях,

индексируемых в Web of Science и SCOPUS. Получено 1 свидетельство о государственной регистрации программы для ЭВМ. Публикации автора с достаточной полнотой отражают основное содержание, результаты и выводы диссертационной работы.

Автореферат диссертации полностью отражает её содержание и результаты при одновременном сохранении структуры построения.

Замечания и вопросы

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.

Высказанные замечания не носят принципиального характера и не снижают общего положительного впечатления от материала диссертации.

Заключение

Диссертационная работа Чернова Дениса Владимировича представляет собой самостоятельную и законченную научно-квалификационную работу, выполненную на актуальную тему и обладающую признаками новизны и практической значимости. Полученные результаты и научно обоснованные решения, которые изложены в диссертации, применимы в ОКИИ с целью повышения эффективности моделирования угроз БИ, а также позволяют поддерживать актуальность сведений о возможных угрозах БИ, потенциальных нарушителях ИБ и необходимых СЗИ. Содержание диссертации соответствует паспорту научной специальности 2.3.6. - Методы и системы защиты информации, информационная безопасность.

Диссертация обладает структурным единством, содержит новые научные результаты и положения, выдвигаемые для публичной защиты, и свидетельствует о личном вкладе автора в исследование. Разделы диссертации взаимосвязаны и логично дополняют друг друга. Полученные автором результаты достоверны. Выводы и заключения, сделанные диссертантом, обоснованы и соответствуют представленным в работе результатам. Диссертационная работа Чернова Д.В. на тему «Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных

оценок» соответствует требованиям п. 9 Положения о порядке присуждения ученых степеней, утверждённого Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г. (в редакции Постановления Правительства РФ от 25.01.2024 г. № 62), предъявляемым к диссертации на соискание ученой степени кандидата технических наук.

Считаю, что Чернов Денис Владимирович заслуживает присвоения ученой степени кандидата технических наук по научной специальности 2.3.6. - Методы и системы защиты информации, информационная безопасность.

Даю согласие на обработку моих персональных данных.

Официальный оппонент, доктор технических наук (05.13.19 - Методы и системы защиты информации, информационная безопасность), профессор, заведующий кафедрой комплексной защиты информации ФГАОУ ВО «Омский государственный технический университет».

22 декабря 2025 г. Ложников Павел Сергеевич

Адрес места основной работы: Федеральное государственное бюджетное образовательное учреждение высшего образования «Омский государственный технический университет». Адрес: 644050, Россия, г. Омск, пр. Мира, д. 11. Телефон: Рабочий телефон: +7 (3812) 65-37-43.
E-mail: pslozhnikov@omgtu.ru

Подпись:
Заверяю:
Начальник управления персонала