ОТЗЫВ

официального оппонента,
доктора технических наук, доцента
Максимовой Елены Александровны
на диссертационную работу
Чернова Дениса Владимировича на тему
«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

1. Актуальность работы

Защита критической информационной инфраструктуры (КИИ) сегодня представляет собой одну из приоритетных задач для национальной безопасности государства. В части обеспечения ее кибербезопасности можно выделить два взаимодополняющих направления: превентивное устранение уязвимостей в компонентах КИИ и меры по повышению отказоустойчивости объектов КИИ в условиях, реализованных кибератак. Так как невозможно гарантировать полное отсутствие уязвимостей в сложных гетерогенных объектах КИИ, меры по обнаружению актуальных угроз безопасности информации (БИ) будут всегда востребованы при их проектировании и эксплуатации. В современных подходах к защите КИИ применяется ряд организационных и технических механизмов, таких как создание Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и внедрение средств безопасности, основанных на концепции «нулевого доверия» (Zero Trust). Однако из-за масштаба, длительных жизненных циклов и высокой стоимости модернизации, объекты КИИ зачастую содержат устаревшее программное обеспечение, что делает их уязвимыми для целенаправленных атак даже при наличии периметровых средств защиты.

Поскольку диссертационная работа Чернова Д. В. направлена на создание средства автоматизации процесса моделирования угроз в отношении критической информационной инфраструктуры, выбранная тематика является актуальной.

2. Оценка содержания диссертации, ее завершенность

Диссертационная работа общим объемом в 199 страниц состоит из введения,

4 глав, заключения, списка сокращений, терминов и определений, списка литературы и 9 приложений. Список использованной литературы состоит из 121 наименования.

Во введении (стр. 5-13) дана общая характеристика работы, обоснована актуальность темы исследования, сформулированы цель и задачи, представлены научная новизна, практическая значимость полученных результатов.

В первом разделе (стр. 14-46) сформулированы задачи оценки вероятных нарушителей и процесса моделирования угроз БИ. Проведен анализ современных отечественных и зарубежных методик моделирования угроз БИ.

Во втором разделе (стр. 47-71) приведен метод определения потенциала нарушителя ИБ ОКИИ на основе построения матриц идентификаторов угроз. Также представлены методы количественной оценки степени опасности реализации угроз БИ ОКИИ потенциальными нарушителями ИБ и оценки защищенности уязвимых звеньев ОКИИ в качестве которых выступают программные, аппаратные и программно-аппаратные средства ОКИИ.

В третьем разделе (стр. 72-90) предложены алгоритмы для сканирования уязвимостей ОКИИ, анализа рисков реализации угроз БИ и оценки их актуальности, основанные на оценке защищенности уязвимых звеньев от действий потенциальных нарушителей и реализованных мер защиты.

В четвертом разделе (стр. 91-129) представлена архитектура и программный интерфейс автоматизированной системы моделирования угроз информационной безопасности для ОКИИ, приводятся результаты применения системы, позволяющие повысить эффективность моделирования угроз более чем в 2,7 раз по сравнению с существующими методиками.

В заключении диссертационной работы (стр. 130-131) представлены основные результаты и приведены перспективы дальнейшей разработки темы.

В приложениях диссертационной работы (стр. 149-199) представлены формы опроса экспертной группы, необходимые для функционирования разработанной автоматизированной системы моделирования угроз, результаты работы указанной автоматизированной системы, фрагменты листинга программного обеспечения, а также копии актов внедрения результатов диссертационной работы и свидетельств о государственной регистрации программ для ЭВМ.

Результаты диссертационного исследования прошли апробацию на 9 международных и 1 всероссийской конференции. По проблеме диссертационного исследования автором опубликовано 30 научных работ, в том числе 4 статьи в рецензируемых научных изданиях, рекомендованных ВАК, 10 - в журналах,

входящих в международную систему Scopus и Web of Science; получено 1 свидетельство о государственной регистрации программы для ЭВМ.

Количество личных публикаций в рецензируемых изданиях - 4.

Содержание диссертации в полной мере отражает суть работы и решение поставленных перед автором задач. Диссертация является завершенной научно-квалификационной работой, написанной грамотным научным языком. Диссертация хорошо структурирована, характеризуется логической целостностью и последовательностью изложения материала. Автореферат диссертации полностью отражает содержание диссертации и полученные в ней результаты. По форме, как диссертация, так и автореферат, соответствует требованиям ВАК, предъявляемым к кандидатским диссертациям на соискание ученой степени кандидата технических наук.

3. Новизна полученных результатов

В диссертационной работе были разработаны:

1. Метод определения потенциала нарушителя ИБ ОКИИ, основанный на применении матриц идентификаторов угроз и *отличающийся от существующих методов* применением предложенного подхода к групповой оценке потенциалов нарушителей согласованным количеством экспертов. 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.

2. Метод количественной оценки степени опасности реализации угроз БИ ОКИИ, *основанный на новом подходе* к интеллектуальному анализу данных, имеющихся в подсистеме журналирования и позволяющий количественно оценить степень опасности реализации угроз БИ потенциальными нарушителями ИБ применительно к конкретному объекту КИИ.

3. Алгоритм определения и оценки защищенности уязвимых звеньев ОКИИ, *отличающийся от известных* тем, что использует матрицу защищенности, составленную на основе оценок показателей защищенности уязвимых звеньев, что позволяет повысить объективность выявления актуальных угроз.

4. 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.

Научная новизна полученных соискателем результатов соответствует пунктам 3, 8, 10 паспорта специальности 2.3.6.

Положения, выносимые на защиту, дают достаточно ясное представление о проведенных исследованиях и являются новыми научными результатами.

4. Обоснованность и достоверность научных положений выводов и рекомендаций, сформулированных в диссертации

Научные положения, выводы и рекомендации базируются на общепризнанных и апробированных научных теориях: теории алгоритмов, методах интеллектуального анализа данных и защиты информации, теории игр, методах экспертных оценок и системного проектирования SADT. В работе присутствуют ссылки на все заимствованные положения.

Подходы соискателя к решению поставленной задачи логично и системно взаимосвязаны и обусловливают непротиворечивость результатов исследования. Сказанное позволяет констатировать, что научные результаты диссертационного исследования вполне обоснованы.

Достоверность работы подтверждается результатами, полученными с использованием предлагаемой в работе автоматизированной системы, и их сопоставлением с результатами других авторов, проводящих исследования в этой области, а также использованием для перекрестной проверки корректности методик моделирования угроз БИ, являющихся утвержденными стандартами в отрасли.

Достоверность научных положений, выводов и рекомендаций, сформулированных в диссертации, следует также из фактов успешного практического применения предложенных Д.В. Черновым методов и алгоритмов, что удостоверено актами о внедрении результатов исследования; подтверждается положительным рецензированием научных работ автора при их опубликовании в журналах, рекомендованных ВАК, а также обсуждением результатов работы на всероссийских и международных научных конференциях.

Таким образом, анализ содержания работы позволяет сделать вывод о достаточно высокой степени обоснованности и достоверности основных научных положений, выводов и практических рекомендаций, приведенных в диссертации.

5. Практическая значимость работы

Практическая значимость результатов диссертационного исследования заключается в том, что их применение позволяет как оценить степень опасности реализации угроз БИ, представленных в общедоступных базах данных, так и проконтролировать эффективность используемых мер защиты объектов КИИ, в отношении которых не установлена категория значимости.

Практическая значимость результатов диссертационного исследования подтверждена тем, что полученные в ходе исследования результаты были внедрены в учебный процесс ТулГУ, производственный процесс АО ЦКБА, а также в процесс обеспечения мероприятий по моделированию угроз БИ в ООО «БД Безопасности» и ООО «Комплексы системы и сети», что подтверждается соответствующими актами внедрения.

Теоретическая и практическая значимость результатов диссертационной работы подтверждается также тем, что работа выполнялась 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».

Полученные в работе результаты могут использоваться для повышения безопасности объектов КИИ как на этапе их проектирования, так и на этапе их внедрения. Кроме того, результаты работы могут использоваться для оценки полноты и эффективности внедренных мер защиты объектов КИИ на этапе их эксплуатации.

6. Замечания

1. В работе (стр. Т6 автореферата, стр 27 диссертации) описана методика ранжирования потенциальных нарушителей х 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.

Необходимо отметить, что приведенные замечания не влияют на общую положительную оценку диссертации.

Работа соискателя обладает внутренним единством, содержит новые научные результаты и положения, выдвигаемые для публичной защиты и свидетельствующие о личном вкладе автора в науку.

7. Заключение

Диссертация Чернова Дениса Владимировича, представленная на соискание ученой степени кандидата технических наук, является завершенной научно-квалификационной работой, в которой решена важная научная задача разработки

специализированных методов и алгоритмов для автоматизации процесса моделирования угроз объектов КИИ, не имеющих категории значимости, что имеет существенное значение для выбора мер защиты, позволяющих минимизировать негативные последствия от реализации актуальных угроз БИ.

Диссертация выполнена на высоком научно-техническом уровне и основана на методах теории алгоритмов, методах интеллектуального анализа данных и защиты информации, теории игр, методах экспертных оценок и системного проектирования SADT.

Автореферат полностью удовлетворяет требованиям, предъявляемым к кандидатским диссертациям, соответствует п. 9-11, п. 13, 14 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842 (с изменениями и дополнениями), а ее автор, заслуживает присуждения 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, доцент,
заведующий кафедрой КБ-4
«Интеллектуальные системы
информационной безопасности»
ФГБОУ ВО «МИРЭА – Российский
технологический университет» Максимова Елена Александровна

e-mail: maksimova@mirea.ru
Тел.: +79616982279

Докторская диссертация защищена по специальности:
2.3.6 - Методы и системы защиты информации, информационная безопасность

Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА - Российский технологический университет» ФГБОУ ВО «РТУ МИРЭА», Проспект Вернадского, д.78, г. Москва. ЦФО, 119454. тел. -7 (499) 600-80-80

Подпись Максимовой Елены Александровны, заведующего кафедрой КБ-4 «Интеллектуальные системы информационной безопасности» Федеральною государственного бюджетного образовательного учреждения высшего образования «МИРЭА - Российский технологический университет», доктора технических наук, доцента заверяю:

заместитель первого проректора РТУ МИРЭА Ю.А. Ефимова