МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет» (ОГУ)

Победы пр., д. 13, г. Оренбург, 460018
Тел. (3532) 77-67-70; факс: (3532) 72-37-01
e-mail: post@mail.osu.ru; http://www.osu.ru; http://ory.рф

26.05.2022 № 1626
на № _____ от _____

УТВЕРЖДАЮ
Проректор по научной работе
_____ С.Н. Летута
«26» мая 2022 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертационную работу Вульфина Алексея Михайловича
на тему «Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных»,
представленную на соискание ученой степени доктора технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность

Актуальность темы исследования

Отличительной чертой современного этапа развития мировой экономики является переход к повсеместному использованию цифровых технологий и систем сбора и обработки информации, созданию и внедрению нового поколения промышленных систем автоматизации и контроля технологических процессов, расширению зоны ответственности корпоративных информационно-телекоммуникационных систем, Этот процесс неизбежно сопровождается не только значительным усложнением инфраструктуры этих объектов, но и расширением числа их контактов с внешним миром, расширением среды субъектов информационных отношений: разработчиков IT-систем, системных интеграторов, провайдеров облачных ресурсов, конечных пользователей и т.п.

Как следствие, данные объекты, в особенности, объекты критической информационной инфраструктуры (КИИ), сегодня все чаще становятся мишенью целенаправленных кибератак со стороны различных категорий внешних и внутренних злоумышленников, нередко приводящих к ощутимому материальному и финансовому ущербу.

В связи с этим в настоящее время особую значимость приобретает проблема разработки научной методологии противодействия этой тенденции, позволяющей получить объективную оценку уровня защищенности этих объектов и предложить адекватные защитные меры по снижению существующих рисков информационной безопасности (ИБ) с учетом требований нормативных документов по технико-экономическим характеристикам.

Актуальность этой проблемы отражена, в частности, в таких руководящих документах, как: Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» № 187-ФЗ, Приказы ФСТЭК России №235 и №239, стандарты серии ГОСТ Р МЭК 62443, вышедший в 2021 г. методический документ ФСТЭК России «Методика оценки угроз безопасности информации». В представленных документах особо отмечена необходимость детального анализа рисков множества угроз, уязвимостей и негативных последствий от воздействия этих угроз на информационные активы объекта.

Решение проблемы и обеспечение требований, представленных в документах, сопряжено с непрерывно возрастающими объемами сведений информационных потоков со слабой структурированностью исходных данных, поступающих из различных источников, с отсутствием развитых интеллектуальных средств автоматизации обработки. Эти причины существенно затрудняют решение текущих задач ИБ, отвечающих современным требованиям по производительности и качеству обработки данных, инициируют поиск новых методов и средств защиты информации. На основании вышеизложенного можно сделать однозначный вывод об актуальности решаемой в диссертации проблемы

разработки моделей и методов комплексной оценки рисков ИБ с использованием технологий интеллектуального анализа данных.

Оценка структуры и содержания работы

Диссертационная работа состоит из введения, шести глав, заключения, списка использованных источников и приложений. Основной текст диссертации изложен на 287 страницах, содержит 112 рисунков и 72 таблицы.

Первая глава является обзорной и посвящена анализу современного состояния работ в области комплексной оценки рисков ИБ объектов КИИ. На основании проведенного анализа делается вывод о недостаточной проработанности данной проблематики. Предложен концептуальный подход к решению проблемы комплексной оценки рисков ИБ объектов КИИ, заключающийся в применении методов и технологий интеллектуального анализа данных.

Во второй главе решаются задачи разработки моделей параметризации множества угроз ИБ и уязвимостей ПО, характерных для объектов КИИ.

В основе этих моделей используются методы и технологии семантического анализа текстовых описаний указанных аспектов безопасности программного и аппаратного обеспечения объектов КИИ, методы обнаружения аномалий состояния объектов КИИ и их подсистем, различные варианты построения нечетких когнитивных моделей сложных многокомпонентных объектов.

Третья глава содержит описание предложенных автором метода и алгоритмов качественной оценки рисков ИБ объектов КИИ с использованием технологий семантического анализа текстовых описаний угроз и уязвимостей, размещённых в открытых базах данных БДУ ФСТЭК России, CAPEC, ATT&CK и др. Особое внимание уделяется разработке инструментальных средств и ПО, позволяющих автоматизировать основные этапы обработки слабоструктурированных текстовых данных и получать более достоверные и оперативные оценки рисков ИБ объектов КИИ с учетом факторов неопределенности.

В четвертой главе рассмотрены метод и алгоритмы количественной оценки рисков ИБ объектов КИИ с использованием методов и технологий нечеткого

когнитивного моделирования и машинного обучения. Показаны преимущества применения данного подхода, позволяющие не только повысить достоверность получаемых оценок рисков ИБ, но и существенно повысить оперативность данного процесса за счет применения предложенной методики автоматизации комплексной оценки рисков ИБ с использованием аппарата вложенных нечетких когнитивных карт.

Пятая глава посвящена разработке метода и алгоритмов оценки рисков ИБ объектов КИИ на основе анализа и прогнозирования аномалий в накапливаемых данных о состоянии объекта КИИ и его подсистем с использованием технологий анализа многомерных временных рядов и методов машинного обучения. Показаны возможности применения данного подхода при решении ряда прикладных задач.

Шестая глава является практической и содержит результаты разработки исследовательского прототипа интеллектуальной системы поддержки принятия решений по оценке рисков ИБ объектов КИИ, а также результаты ее применения при решении ряда практических задач по оценке рисков ИБ и уровня защищенности конкретных предприятий и учреждений Республики Башкортостан.

В целом, диссертационная работа имеет четкую логическую структуру, основные разделы последовательны и взаимосвязаны.

Работа хорошо иллюстрирована, имеет список определений основных терминов. Приложения содержат необходимые таблицы с пояснениями основных результатов.

Автореферат достаточно полно раскрывает основное содержание диссертации. Полученные результаты соответствуют специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Новизна полученных результатов

Наиболее существенные новые научные результаты, полученные в диссертации, состоят в разработке научно-обоснованного концептуального подхода, методов, моделей, алгоритмов и методик решения поставленных в диссертации задач. К новым научным результатам, полученным в диссертационном исследовании, следует отнести следующие:

1. Концепция комплексной оценки рисков ИБ объектов КИИ с использованием технологий нечеткого когнитивного моделирования и методов машинного обучения, применение которой позволяет повысить достоверность и оперативность получения качественных и количественных оценок рисков ИБ в условиях влияния сопутствующих факторов неопределенности.

2. Комплекс проблемно-ориентированных моделей параметризации множеств угроз и уязвимостей объектов КИИ, основанных на использовании технологий семантического анализа текстов на естественном языке и обнаружения аномалий в накапливаемых данных о состоянии объектов, применение которых позволяет сократить трудозатраты на анализ открытых баз данных угроз и уязвимостей и повысить оперативность выполнения основных этапов оценки рисков ИБ.

3. Метод, алгоритмы и методика качественной оценки рисков ИБ объектов КИИ, основанные на использовании технологий семантического анализа слабо структурированных текстовых описаний угроз и уязвимостей, применение которых позволяет обеспечить выявление актуальных угроз, уязвимостей и сценариев реализации атак, ранжировать их по степени опасности, автоматизировать и повысить оперативность основных этапов процесса оценки рисков ИБ.

4. Метод, алгоритмы и методика количественной оценки рисков ИБ объектов КИИ, отличающиеся принципами построения и анализа иерархии вложенных нечетких когнитивных карт, учитывающие различные аспекты безопасности программного и аппаратного обеспечения объектов КИИ и особенности их многоуровневой структурно-функциональной организации, позволяющие повысить точность оценок рисков ИБ.

5. Метод и алгоритмы оценки рисков ИБ объектов КИИ на основе обнаружения аномалий временных рядов накапливаемых данных, получаемых в процессе мониторинга состояния объектов КИИ, позволяющие повысить достоверность и оперативность поиска скрытых зависимостей в накапливаемых данных, а также точность априорных экспертных оценок вероятностей реализации угроз и эксплуатации уязвимостей.

Научная новизна результатов исследований подтверждена патентом на изобретение и 17 свидетельствами о государственной регистрации программ для ЭВМ.

Степень достоверности результатов исследования

Достоверность основных выводов и результатов диссертационного исследования подтверждается следующими фактами:

– обсуждением результатов исследования на профильных международных и российских конференциях, в частности, на Международной научно-технической конференции «International Conference on Industrial Engineering, Applications and Manufacturing» (2017, Saint-Petersburg, Russia, 2018, Moscow, Russia); IEEE International Symposium on Signal Processing and Information Technology (2017, Bilbao, Spain);

– апробацией полученных результатов в организациях и учреждениях, подтвержденными актами внедрения и использования;

– использованием признанных методов теории и практики защиты информации, оценки рисков информационной безопасности, когнитивного моделирования, семантического анализа текстов, машинного обучения;

- экспериментальными исследованиями с использованием разработанного автором исследовательского прототипа интеллектуальной системы поддержки принятия решений по оценке рисков информационной безопасности объектов КИИ.

Основные результаты, полученные в диссертации, опубликованы в 24 статьях в изданиях, входящих в перечень ВАК, 19 статьях в изданиях, индексируемых в базах Scopus и Web of Science, 2 монографиях, сборниках трудов научных конференций различного уровня, защищены патентом на изобретение и 17 свидетельствами о государственной регистрации программ для ЭВМ.

Значимость полученных результатов для науки и практики

Теоретическая значимость результатов, полученных в диссертации, заключается в том, что они носят фундаментальный характер, вносят существенный вклад в решение проблемы комплексной оценки рисков ИБ

объектов КИИ с использованием современных технологий интеллектуального анализа данных и методов машинного обучения. На основе предложенного в работе подхода разработана научно-обоснованная методология: научная концепция, система моделей, методов, алгоритмов и методик комплексной оценки рисков ИБ - применение которой позволяет получить объективную оценку уровня защищенности объектов КИИ в условиях воздействия внешних и внутренних угроз, оценить неблагоприятные последствия от воздействия этих угроз и сформировать адекватные защитные меры по снижению рисков ИБ с учетом требований существующих нормативных документов.

Практическая значимость результатов диссертации заключается в разработке и внедрении оригинальных технических и технологических решений в виде алгоритмического, программного и методического обеспечения исследовательского прототипа интеллектуальной системы поддержки принятия решений по оценке рисков информационной безопасности объектов КИИ, в составе которого реализован набор предложенных автором обеспечивающих и функциональных подсистем и модулей.

Результаты диссертационных исследований позволяют автоматизировать основные этапы процесса комплексной оценки рисков ИБ, обеспечивают повышение достоверности и оперативности получения оценок рисков ИБ и способствуют более обоснованному выбору комплекса мер по снижению рисков ИБ и обеспечению требуемого уровня защищенности объектов КИИ. Полученные результаты прошли практическую апробацию, подтвержденную актами об их внедрении и использовании в ряде организаций и учреждений Республики Башкортостан.

Значимость полученных результатов исследований для практики подтверждается тем, что разработанные методы, алгоритмы и их программные позволяют повысить качество проектно-исследовательских разработок систем защиты информации КИИ, а также эффективность их эксплуатации. В частности, применение способа мониторинга целостности данных, получаемых с бортовых систем летательных аппаратов (ЛА), позволило снизить оценку риска ИБ для

информационно-управляющих систем ЛА на 45 % и обеспечить оценку вероятности успешного распознавания атаки с помощью системы мониторинга целостности данных на уровне 0,85-0,98, алгоритмы обнаружения аномалий в данных мониторинга состояния АСУ ТП нефтедобычи позволяют корректно классифицировать до 78-95 % состояний, в том числе вызванных воздействием злоумышленника.

Рекомендации по использованию результатов и выводов диссертации

Результаты представленной работы рекомендуются к использованию в организациях, которые выполняют аудит информационной безопасности объектов КИИ, реализуют и внедряют комплекс мер по обеспечению требуемой защищенности этих объектов:

– в организациях в сфере обеспечения кибербезопасности объектов финансового сектора;

– в организациях и предприятиях топливно-энергетического комплекса для обнаружения аномалий в данных мониторинга состояния АСУ ТП нефтедобычи, в частности, в ООО «Уральский центр систем безопасности» в г. Екатеринбург и его филиалах;

– при реализации проектов, связанных с обеспечением информационной безопасности корпоративной информационной сети образовательных организаций, в учебном процессе и при проведении научно-исследовательских работ, в частности, в Уфимском государственном техническом университете, в Оренбургском государственном университете.

Замечания по диссертационной работе

Диссертация не лишена недостатков, в частности:

1. Одной из особенностей концепции исследований работы является разработка комплексного подхода к исследованию рисков. Комплексность предполагает наличие некоторой совокупности объектов. Из текста диссертации не ясно в какой мере является полным и достаточным множество предлагаемых моделей методов и алгоритмов для обеспечения требуемой безопасности объектов информатизации.

2. Объектом исследования является многоуровневая распределенная информационно-управляющая система. Структура таких систем предполагает иерархический характер рисков. Из текста диссертации неясно, каким образом предполагается применить предложенный автором подход для построения систем защиты информации с учетом с учетом совмещенности рисков нижнего и верхнего уровня.

3. Предложенный автором подход универсален, автором предложен целый ряд аспектов по его применению. В связи с этим было бы целесообразным обобщить направления эффективного приложения результатов исследований, например, к задачам оценки, прогнозирования и принятия решений по минимизации временных и стоимостных затрат на построение систем защиты с учетом комплексного анализа рисков ИБ.

4. В описании результатов исследований автор не всегда использует достаточно привычную для ИБ терминологию, в частности, «остаточные и приемлемые риски, модели угроз», по тексту автореферата имеются отдельные неточности в определении выводов, например (стр.7 автореферата), «Применение модели оценки степени опасности новых уязвимостей на основе прогнозирования набора метрик позволяет получить оценку степени их опасности (и набора ее метрик)», что в некоторых случаях затрудняет восприятие результатов.

5. Из работы не вполне ясно, как оценивалась достоверность полученных оценок рисков ИБ объектов КИИ с учетом разброса исходных экспертных оценок.

Вместе с тем, данные замечания не снижают общей высокой оценки полученных результатов, научной и практической ценности диссертации.

Заключение

На основе вышеизложенного можно сделать вывод о том, что диссертация Вульфина Алексея Михайловича является завершенной научно-квалификационной работой, в которой на основании выполненных автором исследований разработаны научно-обоснованные технические и технологические решения, направленные на решение актуальной проблемы разработки моделей и методов комплексной оценки

рисков информационной безопасности объектов КИИ с использованием методов и технологий интеллектуального анализа данных, внедрение которых вносит значительный вклад в развитие страны. Диссертация соответствует требованиям п. 9 «Положения о присуждении ученых степеней», а ее автор – Вульфин Алексей Михайлович – заслуживает присуждения ему ученой степени доктора технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Отзыв с учетом предложений и замечаний, высказанных при обсуждении диссертации Вульфина А.М., подготовил заведующий кафедрой вычислительной техники и защиты информации Федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет», доктор технических наук, профессор - Аралбаев Ташбулат Захарович.

Докторская диссертация защищена по специальности 05.13.06 – Автоматизация и управление технологическими процессами и производствами (промышленность).

Отзыв обсужден и утвержден на заседании кафедры вычислительной техники и защиты информации Федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет». Протокол №12 от 24 мая 2022 года.

Заведующий кафедрой
вычислительной техники и защиты информации,
доктор технических наук, профессор Т.З. Аралбаев

Даю согласие на обработку персональных данных.
Адрес организации: 460018, Оренбургская область, г. Оренбург, просп. Победы, д. 13. Рабочий телефон: 8 (3532) 37-25-51, адрес эл. почты: vtzi@mail.osu.ru

«Подпись заведующего кафедрой вычислительной техники
и защиты информации - Аралбаева Ташбулата Захаровича заверяю»

Главный ученый секретарь-начальник отдела
диссертационных советов ОГУ, д.т.н., профессор А.П. Фот
25 мая 2022 г