ОТЗЫВ

на автореферат диссертации Кучкаровой Наили Вакилевны на тему «Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Вопросы обеспечения информационной безопасности (ИБ) объектов критической информационной инфраструктуры (КИИ) в последние годы находятся в центре внимания регуляторов (ФСТЭК России, ФСБ), ИТ-компаний - разработчиков и поставщиков программно-аппаратных средств защиты информации, ситуационных центров мониторинга ИБ (Security Operations Centers, SOC). Важность решения данной задачи обусловлена высокой социальной, политической, экономической и экологической значимостью этих объектов, а также их значимостью для обеспечения обороны страны и национальной безопасности. Одним из важных этапов обеспечения ИБ объектов КИИ является оценка уровня их защищенности (устойчивого функционирования) в условиях возможного воздействия внешних и внутренних угроз безопасности информации (БИ), с последующим формированием необходимых контрмер по противодействию этим угрозам. В соответствии с Методикой ФСТЭК России от 05.02.2021 г., определение перечня актуальных угроз БИ и сценариев их реализации должно осуществляться экспертами с учетом фактически выявленных или потенциально возможных уязвимостей программного обеспечения (ПО), а также тактик и техник реализации этих уязвимостей, которые могут быть использованы возможным нарушителем. В качестве дополнительных данных при выполнении указанных действий Методика рекомендует использовать открытые данные об угрозах и уязвимостях объектов КИИ, которые содержатся в Банке данных угроз безопасности информации (БДУ) ФСТЭК России в виде текстовых описаний определенного формата. Учитывая большой объем информации, накопленной в БДУ (это десятки тысяч уязвимостей ПО и сотни угроз БИ), а также то, что обработка этой информации производится специалистом по ИБ, как правило, в ручном режиме, это неизбежно сопровождается большими временными затратами и появлением возможных ошибок, связанных с человеческим фактором. Таким образом, тема диссертационной работы Кучкаровой Н.В., посвященная разработке средств автоматизации оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ с использованием современных технологий обработки естественного языка, является актуальной и востребованной.

К основным результатам работы, обладающим научной новизной, относятся:

- алгоритмы автоматической классификации и суммаризации текстов, содержащихся в специализированных открытых источниках в области ИБ;
- метод и алгоритм автоматизированной оценки и приоритизации (ранжирования) множества релевантных угроз БИ для выявленных уязвимостей ПО;
- алгоритм построения графовой модели сценария реализации актуальных угроз БИ на основе оценки семантической близости текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник действий нарушителя;
- архитектура и состав программных модулей интеллектуальной системы поддержки принятия решений (ИСППР), реализующих предложенные в работе метод и алгоритмы оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ.

Практическая значимость работы заключается в том, что применение предложенных инструментальных средств позволяет повысить полноту и достоверность результатов оценки актуальных угроз БИ и уязвимостей объектов КИИ, существенно сокращая временные затраты и когнитивную нагрузку на специалиста по ИБ.

Полученные результаты по своему содержанию соответствуют паспорту научной специальности 2.3.6. Следует отметить высокий уровень публикаций автора – опубликовано 14 работ, из них 4 статьи в журналах из Перечня рецензируемых научных изданий ВАК, получены 2 свидетельства о государственной регистрации программ для ЭВМ.

В качестве замечания по тексту автореферата можно указать, следующее:

1. Наилучший результат в задаче сопоставления текстовых описаний угроз БИ, уязвимостей ПО, техник (тактик) демонстрирует предобученная модель-трансформер, но, поскольку визуализация графовой модели здесь не представлена, это затрудняет последующую оценку применимости данной модели.

2. Из описания второй главы непонятны результаты исследования методов кластеризации. Какие методы оказались предпочтительными к решаемой задачи.

3. В описании третьей главы не представлена функциональная модель процесса оценки и анализа актуальных угроз БИ в соответствии с Методикой ФСТЭК.

Однако, указанные замечания не снижает общей высокой оценки уровня диссертационной работы, которая выполнена на актуальную тему, обладает научной новизной и практической ценностью.

Считаю, что представленная диссертация является завершенной научно-квалификационной работой и соответствует требованиям п. 9 Положения ВАК о порядке присуждения ученых степеней, а ее автор, Кучкарова Наиля Вакилевна, заслуживает присуждения ей ученой степени

кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Кандидат физико-математических наук, доцент,
заведующий кафедрой безопасности информационных систем,
федеральное государственное автономное
образовательное учреждение высшего образования
«Самарский национальный исследовательский
университет имени академика С. П. Королёва»

Осипов Михаил Николаевич

06.09.2023

Кандидатская диссертация защищена
по специальности 01.02.04. – Механика деформируемого твердого тела

Даю согласие на обработку персональных данных

Адрес места основной работы: 443011, г. Самара, ул. Академика Павлова, 1, Корпус 22, к. 411.

Рабочий телефон: +7 (846) 337-99-41

Адрес эл. osipov7@yandex.ru

Кандидат физико-математических наук, доцент,
доцент кафедры безопасности информационных систем,
федеральное государственное автономное
образовательное учреждение высшего образования
«Самарский национальный исследовательский
университет имени академика С.П. Королёва»

Иванов Дмитрий Владимирович

06.09.2023

Кандидатская диссертация защищена
по специальности 05.13.18 – Математическое моделирование, численные методы и комплексы программ

Даю согласие на обработку персональных данных

Адрес места основной работы: 443011, г. Самара, ул. Академика Павлова, 1, Корпус 22, к. 411.

Рабочий телефон: +7 (846) 337-99-41

Адрес эл. dvi85@list.ru

Подпись Иванова Д.В. удостоверяю.
Начальник отдела сопровождения деятельности ученых советов Самарского университета
Бояркина У.В.
«06» 09 2023 г.