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

Тема диссертационной работы Кучкаровой Н.В. посвящена актуальному на сегодняшний день направлению исследований в области информационной безопасности (ИБ), связанному с разработкой автоматизированных средств оценки и анализа угроз безопасности информации (БИ) и уязвимостей программного обеспечения (ПО) объектов критической информационной инфраструктуры (КИИ), к числу которых относятся автоматизированные системы управления технологическими процессами (АСУ ТП) промышленных объектов. Важность решения этой задачи отмечается в ряде нормативно-правовых документов (Федеральный закон «О безопасности критической информационной инфраструктуры», Приказы ФСТЭК России №31, №235, №239, «Методика оценки угроз безопасности информации» ФСТЭК России от 05.02.2021 г.). В настоящий момент процедуры оценки угроз БИ и уязвимостей ПО, как одной из составляющих процесса оценки рисков ИБ объектов КИИ, выполняются экспертами, как правило, в «ручном», либо частично автоматизированном режиме. При этом производится сопоставление объемных текстовых описаний угроз БИ и выявленных на объекте уязвимостей ПО, содержащихся в Банке данных угроз безопасности информации (БДУ) ФСТЭК России, что требует от эксперта высокой квалификации и значительных затрат времени. Выходом из сложившейся ситуации является возможность использования современных технологий автоматизированной обработки естественного языка (Text Mining), применение которых позволит расширить полноту поиска необходимой информации в БДУ ФСТЭК России, одновременно повышая оперативность и достоверность результатов работы эксперта. С учетом вышеизложенного, можно сделать вывод об актуальности и востребованности данного научного исследования.

К наиболее значимым научным результатам, полученным автором, относятся:

1. Алгоритмы автоматической классификации и суммаризации текстов, содержащихся в специализированных открытых источниках в области ИБ.
2. Метод и алгоритм автоматизированной оценки и приоритизации множества релевантных угроз БИ для выявленных уязвимостей ПО объекта КИИ на основе технологии семантического анализа текстов.
3. Алгоритм построения графовой модели сценария реализации актуальных угроз БИ объекта КИИ на основе оценки семантической близости текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник действий возможного нарушителя.
4. Архитектура и программное обеспечение ИСППР, реализующие предложенные в работе метод и алгоритмы оценки актуальных угроз БИ объектов КИИ.

Практическая ценность диссертации подтверждается применением полученных результатов при решении ряда прикладных задач по оценке актуальных угроз БИ объектов КИИ, на что получены акты внедрения.

Результаты исследований опубликованы в 14 работах, в том числе в 4 статьях в журналах, входящих в Перечень ВАК рецензируемых научных изданий категории К1 по научной специальности 2.3.6, что также подтверждает высокий уровень диссертации.

В качестве замечаний по автореферату можно отметить следующее:

- в 3-й главе при формировании корпуса текстов использовались текстовые описания угроз БИ и уязвимостей ПО, представленные в БДУ ФСТЭК России; при этом не совсем понятно, каким образом были получены текстовые описания тактик и техник реализации угроз БИ;
- в автореферате упоминается о разработке алгоритмов векторизации и кластеризации текстовых данных, однако, поскольку они не представлены в тексте, то не совсем понятно, каким образом происходит предварительная обработка текстовых описаний.

Вместе с тем, указанные замечания не снижают общей положительной оценки научной ценности и практической значимости представленной работы.

Считаю, что диссертационная работа Кучкаровой Н.В., представленная на соискание ученой степени кандидата технических наук, выполнена на актуальную тему, она 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.

Доктор технических наук, доцент,
заведующий научно-исследовательской лабораторией
«Интеллектуальные информационные технологии и системы»,
Федеральное государственное бюджетное
образовательное учреждение
высшего образования
«Челябинский государственный университет»

Вохминцев Александр Владиславович

29.08.2023

Докторская диссертация защищена
по специальности 05.13.01 – «Системный анализ, управление и обработка информации (в информационных и технических системах)».

Даю согласие на обработку персональных данных.

Адрес места основной работы: 454001, г. Челябинск, ул. Братьев Кашириных, д.129, каб.330

Рабочий телефон: +7(351) 799-72-88

Адрес эл. почты: vav@csu.ru

Подпись Вохминцева А.В.
удостоверяю
специалист по кадрам