ОТЗЫВ

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

Диссертационная работа Вульфина Алексея Михайловича посвящена актуальной проблеме разработки и применения моделей и методов интеллектуального анализа данных к оценке качественных и количественных показателей защищенности и рисков информационной безопасности (ИБ) объектов критической информационной инфраструктуры (КИИ), обладающих на практике многоуровневой иерархической архитектурой и многообразием применяемых средств ИТ, средств АСУ ТП, разветвленными системами телекоммуникаций. Поэтому поставленная в работе цель повышения достоверности и оперативности технологий и процедур комплексной оценки рисков ИБ объектов КИИ и решаемые в ней задачи, несомненно, являются актуальными.

В диссертации предложена новая концепция комплексной оценки рисков ИБ объектов КИИ на основе методов и технологий интеллектуального анализа данных. Разработан комплекс проблемно-ориентированных моделей параметризации угроз и уязвимостей объектов КИИ, отличающийся применением ансамбля гетерогенных моделей машинного обучения при оценке опасности уязвимостей и построении детекторов аномалий с использованием дополнительной информации из открытых баз знаний и технологий анализа текстовых описаний, что позволяет снизить трудоемкость и автоматизировать низкоуровневое моделирование сценариев эксплуатации уязвимостей и реализации угроз, одновременно обеспечивая видимость и контекст потенциальной атаки.

В автореферате изложены цель и задачи диссертационного исследования, представлены основные научные положения, выносимые на защиту, обладающие новизной; охарактеризованы применяемые методы исследования,

раскрыто практическое значение результатов для организаций и учреждений различного профиля.

Из полученных научных результатов следует выделить метод, алгоритмы и методику качественной оценки уровня рисков ИБ объектов КИИ, основанные на использовании технологий семантического анализа текстовых описаний угроз и уязвимостей, отличающиеся подходом к формализации слабоструктурированных текстовых описаний с помощью гетерогенных нейросетевых моделей вложений в виде графовой семантической модели, что позволяет обеспечить выявление потенциальных угроз, уязвимостей и сценариев реализации атак с возможностью их ранжирования по приоритетам, а также автоматизировать основные этапы процедуры оценки рисков.

К достоинствам работы также следует отнести общую последовательность и логичность изложения результатов от концепции до конечной реализации, а также имеющийся у автора патент на способ и систему защиты информации.

Замечания по тексту автореферата:

1. Из текста автореферата не ясно, какова связь оценки риска, обозначенной как R_i на стр. 11 и моделями-регрессорами оценки степени опасности с теми же обозначениями R_i на рис. 2 (стр. 13)?
2. Из описаний ориентированных графов G на стр. 13 и НКК на стр. 15 не ясно, какие вершины графов соединяются рёбрами, и каким образом определяются направления ребер?
3. На стр. 15 сказано, что комплекс моделей анализа аномалий в поведении пользователей конечной системы разработан с целью оценки угрозы нарушения конфиденциальности и целостности информации. Как в этом случае оцениваются угрозы нарушения доступности?
4. При описании графа НКК на стр. 15 используется кортеж множеств $<C, F, W>$, но далее речь ведётся об элементах $X_i(t)$. Множество этих элементов, видимо, тоже нужно включить в этот кортеж.

5. В формуле (2) на стр. 16 для $X_i(t)$ – значения переменной состояния i-го концепта C_i используется обозначение $\tilde{X}_i(t)$ (с волной). Это же происходит и с переменными W_{ij} – в определении они без волны, а в формуле с волной. Чем обусловлена разность в обозначениях?
6. При пояснении формулы (2) на стр. 16 автор говорит о весах связей $\tilde{W}_i$. Видимо, речь идёт о $\tilde{W}_{ji}$.

Однако приведенные замечания не снижают научной ценности и практической значимости полученных в диссертационной работе результатов.

Диссертационная работа Вульфина А.М. является законченной научно-квалификационной работой, обладает научной и практической значимостью и соответствует требованиям п. 9-11, 13, 14 Положения ВАК «О присуждении ученых степеней», предъявляемым к докторским диссертациям, а ее автор – Вульфин Алексей Михайлович – заслуживает присуждения ученой степени доктора технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Кандидат технических наук, доцент,
заведующий кафедрой защиты
информации Высшей школы
электроники и компьютерных наук
ФГАОУ ВО «Южно-Уральский
государственный университет
(национальный исследовательский
университет)» Соколов Александр Николаевич

Кандидатская диссертация защищена по специальности 05.12.21 – Радиотехнические системы специального назначения, включая технику СВЧ и технологию их производства.

Даю согласие на обработку персональных данных. 03.06.202

Подпись Соколова А.Н. заверяю:

Адрес места основной работы: 454080, г. Челябинск, пр. Ленина, д. 76
Рабочий телефон: +7 (351) 267-93-55
Адрес эл. почты: sokolovan@susu.ru

Верно
Ведущий док овед