ОТЗЫВ на автореферат диссертации
Вульфина Алексея Михайловича
«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

В условиях необходимости усиления мер по защите цифрового пространства и создания в России государственной системы защиты информации, проблема обеспечения безопасности объектов критической информационной инфраструктуры приобретает особую актуальность в сфере обеспечения реализации стратегических приоритетов Российской Федерации. Это связано, прежде всего, с эволюционным характером роста динамики инцидентов, что диктует необходимость оперативного реагирования на потоки событий безопасности, оценку и выбор эффективной тактики управления рисками объектов критической информационной инфраструктуры. Специфика угроз такого рода заключается в сложности их формализации и, следовательно, их идентификации лицом, ответственным за ИБ. С этим связана актуальность данной работы — применение методологии интеллектуального анализа данных для комплексной оценки рисков безопасности объектов критической информационной инфраструктуры.

Научная новизна работы связана с такими результатами, как: разработан комплекс проблемно-ориентированных моделей параметризации угроз и уязвимостей объектов КИИ, основанных на использовании технологий интеллектуального анализа данных и обнаружения аномалий в накапливаемых данных мониторинга их состояния; Разработаны метод, алгоритмы и методика 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; Разработаны метод, алгоритмы и методика количественной оценки рисков ИБ объектов КИИ, основанные на построении иерархии вложенных когнитивных карт, соответствующих структурно-функциональной организации объекта КИИ, отличающиеся построением и декомпозицией укрупненной нечеткой когнитивной карты, сценарным моделированием сложных многошаговых целенаправленных кибератак с использованием базы меташаблонов атак с дальнейшей формализацией в виде иерархической НКК; Разработаны метод и алгоритмы оценки рисков ИБ объектов КИИ на основе обнаружения аномалий временных рядов накапливаемых параметров, характеризующих состояние этих объектов, сетевого трафика промышленных сетей и поведения пользователей конечных систем.

Достоверность результатов подтверждается корректным применением методов теории и практики защиты информации, оценки рисков информационной безопасности, когнитивного моделирования, семантического анализа текстов, машинного обучения, а также экспериментальными исследованиями с использованием разработанного автором исследовательского прототипа интеллектуальной системы поддержки принятия решений по оценке рисков информационной безопасности объектов КИИ.

Практическая значимость работы подтверждается разработкой и внедрением алгоритмического, программного и методического обеспечения исследовательского прототипа ИСППР по оценке рисков ИБ объектов КИИ, в составе которой реализован набор предложенных подсистем и модулей.

Убедительны объём и качество публикаций и апробация по теме диссертационной работы.

Замечания:

1. Не достаточно ясно, учитывалась ли хаотичность временного ряда в модели обнаружения аномалий состояния объектов и сущностей в зоне анализируемого объекта КИИ.

2. На рис. 4 стр. 15 автореферата приведена модель обнаружения аномалий состояния подсистем в зоне объекта КИИ. В схема присутствует модуль кластерного анализа вектора признаков состояния объекта. Однако, из текста автореферата не достаточно ясно, какие именно методы кластеризации использует автор.

Вместе с тем, указанные недостатки не снижают общей позитивной оценки диссертационной работы.

Диссертация Вульфина А.М. является законченной научно-квалификационной работой и удовлетворяет требованиям п. 9 «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.

Доктор технических наук, профессор,
заведующий кафедрой систем
информационной безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Воронежский государственный технический университет (ФГБОУ ВО «ВГТУ»)

Остапенко Александр Григорьевич
15.06.2022 г.

Докторская диссертация защищена по специальности
05.09.05 – «Теоретическая электротехника»

Даю согласие на обработку персональных данных.

Подпись профессора Остапенко А.Г. заверяю

Адрес места основной работы: Федерального государственного бюджетного образовательного учреждения высшего образования «Воронежский государственный технический университет (ФГБОУ ВО «ВГТУ»),
394026, Воронеж, Московский проспект, 14,
тел. (+7 4732) 52-34-20, email: sub316@mail.ru