ОТЗЫВ

на автореферат диссертации Чернова Дениса Владимировича «Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Диссертация Чернова Д.В. посвящена актуальной научной задаче совершенствования методов и алгоритмов моделирования угроз информационной безопасности объектов критической информационной инфраструктуры, в отношении которых принято решение об отсутствии необходимости присвоения им категорий значимости. Актуальность исследования определяется стремительным внедрением средств автоматизации критических процессов в промышленные системы, что создает предпосылки к возникновению новых и более опасных угроз безопасности информации и требует разработки новых и совершенствования существующих подходов к моделированию угроз. В современных условиях особую актуальность приобретает необходимость разработки алгоритмов, позволяющих автоматизировать процесс оценки нарушителей и опасности реализации ими угроз в отношении объектов критической информационной инфраструктуры, что позволит снизить сложность реализации этих процедур в силу отсутствия соответствующего программного обеспечения на рынке средств защиты информации и ограниченного объёма кадрового рынка специалистов в области информационной безопасности.

Научная ценность работы заключается в развитии теоретических знаний и разработке новых методов и алгоритмов моделирования угроз с применением подходов и инструментария теории защиты информации, теории игр, экспертных оценок и системного анализа для построения моделей угроз объектов критической информационной инфраструктуры. Ключевой особенностью разработанных методов и алгоритмов является состязательная природа оценки актуальности угроз, включающая элементы игры между нарушителем и системой защиты объекта, что

позволяет выявлять большее количество актуальных угроз и соответственно предложить более комплексный подход к обеспечению информационной безопасности объекта.

Теоретическая значимость работы определяется разработкой математического аппарата определения потенциала нарушителя и фактических уязвимых звеньев, функционирующих в том числе на различных уровнях АСУ ТП. Автором предложены оригинальные алгоритмы, обеспечивающие оценку защищенности уязвимых звеньев и опасности реализации угроз в отношении объектов критической информационной инфраструктуры, что имеет существенное значение для современной теории защиты информации.

С практической точки зрения представленная работа демонстрирует конкурентные результаты в области оценки опасности реализации угроз и соответственно определения актуальных угроз объектов критической информационной инфраструктуры, а также формирования рекомендаций администратору информационной безопасности о необходимости внедрения соответствующих защитных мер. Экспериментальные исследования подтверждают повышение показателя эффективности моделирования угроз с применением разработанной автоматизированной системы более чем в 2,6 раз суммарного числа выявленных актуальных угроз и предложенных мер защиты в час по сравнению с методикой ФСТЭК и более чем в 4 раза по сравнению с зарубежной методикой TRIKE, что является существенным шагом в развитии существующего комплекса мер противодействия актуальным угрозам информационной безопасности.

По автореферату диссертации можно сделать следующие замечания:

1. Автореферат не содержит достаточного анализа вычислительной сложности предложенных алгоритмов, что не позволяет полно и точно оценить эффективность метода в условиях с ограниченными вычислительными ресурсами.

2. В работе недостаточно раскрыты вопросы масштабируемости предложенных методов и алгоритмов при увеличении количества возможных нарушителей режима безопасности информации незначимого объекта КИИ выше экспериментально исследованных десяти.

Указанные замечания носят рекомендательный характер и не влияют на общую высокую оценку диссертационной работы Чернова Д.В., представляющей завершенное научное исследование с очевидной теоретической и практической ценностью.

На основании вышеизложенного считаю, что представленная диссертация является завершенной научно-квалификационной работой и соответствует требованиям п. 9-11, п. 13, 14 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842 (с изменениями и дополнениями), предъявляемым к диссертациям на соискание ученой степени кандидата наук, а ее автор, Чернов Денис Владимирович, заслуживает присуждения ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

к.т.н. доцент, заведующий кафедрой защиты информации ФГБОУ ВО «Новосибирский государственный технический университет» Иванов А.В.

Иванов Андрей Валерьевич

Кандидатская диссертация защищена в 2015 году по специальности:
05.13.19 «Методы и системы защиты информации, информационная безопасность»

Даю согласие на обработку моих персональных данных Иванов А.В.

«17» 12 2025 г.

Место работы: Федеральное государственное бюджетное образовательное учреждение высшего образования «Новосибирский государственный технический университет».

Почтовый адрес: 630073, г. Новосибирск, пр-т К.Маркса, 20

Телефон: +7 383 346 08 53

E-mail: andrej.ivanov@corp.nstu.ru

ПОДПИСЬ ЗАВЕРЯЮ
Начальник отдела кадров
О. К. Пустовалова