УТВЕРЖДАЮ

[redacted]а Военной академии

[redacted]учной работе

В.Гель

ОТЗЫВ

на автореферат диссертации Дойниковой Елены Владимировны "Оценка защищенности и выбор защитных мер в компьютерных сетях на основе графов атак и зависимостей сервисов" на соискание ученой степени кандидата технических наук по специальности 05.13.19 "Методы и системы защиты информации, информационная безопасность"

В настоящее время проблема оценки защищенности информационных систем является актуальной как для аттестации согласно требованиям действующих нормативных документов, так и для повышения эффективности управления информационной безопасностью предприятий. Хотя в этой области существует большое количество стандартов и исследований, предлагаемые в них методики по-прежнему имеют ряд недостатков, связанных со сложностью и неоднозначностью входных данных. Таким образом, все еще существует проблема создания комплексной количественной методики оценки защищенности и выбора защитных мер и автоматизированных средств, работающих на их основе.

Основной целью рассматриваемой работы заявляется повышение эффективности управления защищенностью компьютерных сетей за счет усовершенствования методик, моделей и алгоритмов оценки защищенности и выбора защитных мер. Для этого соискателем были разработаны оригинальная классификация показателей защищенности, методики и алгоритмы оценки защищенности и выбора защитных мер на основе графов атак и графов зависимостей сервисов. А также разработаны архитектура и прототип программного средства, реализующего предложенные методики.

На основе теоретического анализа полученных результатов и с помощью экспериментов с использованием разработанного соискателем программного средства были подтверждены обоснованность результатов исследования и достижение поставленной цели. Данные результаты могут представлять интерес для разработчиков и администраторов перспективных систем защиты компьютерных сетей.

В автореферате были обнаружены следующие недостатки:

1. В автореферате не раскрыто, как определяется отклонение спрогнозированной последовательности атаки от реальной, что затрудняет понимание результатов эксперимента.

2. Согласно тексту автореферата показатель AttackerSkillLevel может принимать качественные значения, однако неясно, как они используются в формуле (5).

3. На рисунке 2 обобщенная схема методики оценки защищенности включает выбор контрмер, хотя это отдельный этап, который не входит в оценку защищенности.

Представленная в автореферате диссертационная работа, несмотря на указанные недостатки, является завершенным самостоятельным научным исследованием, обладает

актуальностью и новизной, и выполнена в соответствии с требованиями п.9 “Положения о порядке присуждения ученых степеней”, утвержденного постановлением Правительства РФ № 842 от 24 сентября 2013 г. Дойникова Е.В. заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 “Методы и системы защиты информации, информационная безопасность”.

Профессор кафедры (автоматизированных систем специального назначения) Военной академии связи
к.т.н., доцент В.С. Авраменко

«2» мая 2017 г.

Сведения о составителе отзыва:

Авраменко Владимир Семенович, кандидат технических наук, доцент; профессор кафедры Военной академии связи; адрес: Тихорецкий пр., д.3, Санкт-Петербург, 194064;
тел.: 82479437; электронная почта: vsavr@yandex.ru.