ОТЗЫВ

на автореферат диссертации Дойниковой Елены Владимировны на тему «Оценка защищенности и выбор защитных мер в компьютерных сетях на основе графов атак и зависимостей сервисов»,

представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Актуальность темы. В настоящее время предприятия различного профиля все больше полагаются в своей деятельности на компьютерные сети. Это, в свою очередь, привело к росту количества умышленных компьютерных атак. Успешности таких атак способствует рост количества выявленных уязвимостей программно-аппаратного обеспечения и доступных эксплоитов. Чтобы не допустить серьезных потерь важно своевременно и адекватно реагировать на происходящие в компьютерной сети предприятия изменения, в том числе на изменения конфигурации сети, появление новых уязвимостей, обнаружение инцидентов безопасности. Отследить все происходящие изменения и оценить их потенциальное влияние на работоспособность системы вручную практически невозможно. Поэтому создание методик и инструментов оценки защищенности и выбора контрмер, способных обработать информацию из различных источников, предоставить ее оператору в удобном для восприятия виде и рекомендовать рациональные защитные меры на сегодняшний день особенно важно. Таким образом, работа Дойниковой Е.В. посвящена решению актуальной научной задачи разработки методик и алгоритмов оценки защищенности компьютерных сетей и выбора защитных мер для мониторинга безопасности и управления инцидентами.

Научная новизна работы определяется разработкой методик оценки защищенности и выбора защитных мер, основанных, в отличие от существующих аналогов, на совместном использовании графов атак и графов зависимостей сервисов, что позволяет одновременно учитывать при выборе защитных мер как их эффективность с точки зрения предотвращения развития атаки, так и возможный побочный ущерб от их реализации.

Теоретическая и практическая значимость результатов работы состоит в том, что предложенные методики, отличающиеся от уже существующих комплексным учетом множества характеристик объектов оценки на основе взаимосвязанных моделей предметной области, позволяют как в рамках отдельного программного средства, так и в качестве компонента систем мониторинга безопасности и управления инцидентами

осуществлять всесторонний мониторинг защищенности компьютерных сетей и выбирать рациональные защитные меры, что актуально и широко применимо для управления безопасностью компьютерных сетей коммерческих организаций.

Обоснованность научных положений, представленных в автореферате, подтверждается апробацией на ведущих российских и международных научных конференциях и публикацией в рецензируемых изданиях, рекомендованных ВАК, а также в изданиях, индексируемых в международных базах Scopus и Web Of Science.

Результаты работы использовались в проекте Европейского Сообщества (контракт № 257475), внедрены в деятельность организаций ООО «Ароматы безопасности» и ГК «Омега», а также внедрены в учебный процесс СПб ГУТ.

По работе можно сделать следующие **замечания**:

1. В формулировке задачи исследования указана разработка методик в рамках системы мониторинга безопасности и управления инцидентами, однако связь с данными системами при описании методик и прототипа раскрыта недостаточно.
2. В автореферате не указано, какие именно открытые базы данных используются в качестве источника входных данных.
3. В автореферате не описано, какие технологии использовались при реализации прототипа, реализующего предложенные методики.

Однако данные замечания не снижают ценности представленных научных результатов и не влияют на общую положительную оценку работы.

Заключение. На основе содержания автореферата можно сделать вывод, что диссертация Дойниковой Е.В. представляет собой законченное научное исследование, а его результаты являются теоретически и практически значимыми, и обладают научной новизной. Работа соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» и отвечает требованиям, предъявляемым к кандидатским диссертациям, в соответствии с Положением о порядке присуждения ученых степеней, утвержденным постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г., а автор работы заслуживает присуждения ученой степени кандидата технических наук.

Директор ФГБУН Института проблем транспорта им. Н.С. Соломенко РАН
д.т.н. профессор

И.Г. Малыгин

Дата: 17 апреля 2017 го

Сведения о составителе отзыва:

Фамилия, имя, отчество: Малыгин Игорь Геннадьевич

Ученая степень: доктор технических наук

Ученое звание: профессор

Место работы: ФГБУН Институт проблем транспорта им. Н.С. Соломенко РАН

Должность: директор ФГБУН Института проблем транспорта им. Н.С. Соломенко РАН

Телефон (рабочий): (812) 321 95 68

Почтовый адрес: 12-я линия ВО, д.13, г. Санкт-Петербург, 199178, ФГБУН Институт проблем транспорта им. Н.С. Соломенко Российской академии наук

Электронная почта: info@iptran.ru