ОТЗЫВ

на автореферат диссертационной работы Дойниковой Елены Владимировны по теме «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»

В современных условиях новые компьютерные угрозы появляются так часто, что для обеспечения безопасности компьютерных сетей все более актуальным становится проактивное реагирование на компьютерные атаки. Для этого важно как прогнозирование возможных атак и их последствий, например, на основе методов аналитического моделирования, так и постоянный мониторинг компьютерной сети и вычисление адекватных показателей защищенности. Поэтому существует необходимость в разработке новых количественных методик оценки защищенности и выбора защитных мер, позволяющих реализовать эти аспекты и учитывающих динамический характер современных систем. Таким образом, задача, решаемая в рассматриваемом диссертационном исследовании, является одной из актуальных задач в области информационной безопасности.

В работе Дойниковой Е.В. в рамках решения данной задачи предлагается выделение разных групп показателей, позволяющих сформировать оценку защищенности системы и выбрать защитные меры с учетом доступных входных данных. Кроме того, в работе разработаны оригинальные методики и алгоритмы оценки защищенности и выбора защитных мер на основе графов

атак и зависимостей сервисов, позволяющие формировать оценку и выбирать защитные меры, используя доступные входные данные, и уточнять их с появлением новых знаний о безопасности. В отличие от существующих аналогов предложенные методики позволяют учитывать большой спектр входных данных и легко могут быть использованы на практике путем интеграции в существующие инфраструктуры предприятий. Это подтверждается их успешным внедрением в деятельность российских предприятий и в международном научно-исследовательском проекте.

Эффективность методик доказывается экспериментами, проведенными для реализующего разработанный подход программного прототипа с использованием различных сценариев атак.

К недостаткам данной работы можно отнести то, что из текста автореферата не ясно, как формируется список контрмер для выбора защитных вариантов. Кроме того, в тексте автореферата не описано, как вычисляется индекс выбора контрмер.

Указанные недостатки не снижают научной и практической ценности представленной диссертационной работы. Полученные результаты обладают новизной и в целом представляют собой законченный цикл исследования от анализа предметной области и разработки теоретических моделей, методик и алгоритмов до проведения экспериментов. Работа удовлетворяет требованиям п. 9 «Положения о порядке присуждения ученых степеней», утвержденного постановлением Правительства РФ № 842 от 24 сентября 2013 г. У автора имеется девять статей в научных изданиях из списка ВАК, а также двенадцать – в журналах, индексируемых в международных базах Scopus и Web Of Science. Считаю, что Дойникова Е.В. заслуживает присуждения ученой степени кандидата технических наук по специальности

05.13.19 — «Методы и системы защиты информации, информационная безопасность».

Доцент кафедры сетей связи и передачи данных СПб ГУТ

к.т.н. О.И. Пантюхин

«2» мая 2017г.

Сведения о составителе отзыва:

ФИО: Пантюхин Олег Игоревич; ученая степень: кандидат технических наук; ученое звание: доцент; место работы: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича; должность: доцент кафедры сетей связи и передачи данных; телефон (рабочий): 8-812-3051284; почтовый адрес: пр.Большевиков д.22, корп.1, г.Санкт-Петербург, 193232; электронная почта: sspd@spbgut.ru.