Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)

199178, Санкт-Петербург, 14 линия, 39 Телефон: (812)328-33-11 Факс: (812)328-44-50
E-mail: spiiran@iias.spb.su http://www.spiiras.nw.ru
ОКПО 04683303, ОГРН 1027800514411 ИНН/КПП 7801003920/780101001

ОТЗЫВ

научного руководителя
на диссертационную работу Дойниковой Елены Владимировны «Оценка защищенности и выбор защитных мер в компьютерных сетях на основе графов атак и зависимостей сервисов», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность»

Диссертационная работа Дойниковой Елены Владимировны подготовлена в ходе научных исследований, проводимых в лаборатории Проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН).

Основными результатами, полученными диссертантом, являются:

1. Комплекс показателей защищенности на основе графов атак и зависимостей сервисов.
2. Методика оценки защищенности компьютерных сетей на основе графов атак и зависимостей сервисов
3. Методика выбора защитных мер на основе графов атак и зависимостей сервисов.
4. Архитектура и программная реализация системы оценки защищенности компьютерных сетей и выбора защитных мер на основе предложенных методик.

В процессе работы над диссертацией Дойникова Е.В. самостоятельно изучила существующие подходы к оценке защищенности компьютерных сетей и выбору защитных мер (в том числе на основе методов аналитического моделирования), а также основные принципы построения систем менеджмента информационной безопасности, в том числе систем управления информацией и событиями безопасности.

Во время работы был методически грамотно составлен план исследований, что позволило диссертанту последовательно выполнить все поставленные перед собой задачи и в результате разработать: (1) комплекс новых, модифицированных и существующих показателей для оценки

защищенности и выбора защитных мер; (2) методику оценки защищенности на основе доступных входных данных, включающую алгоритмы вычисления показателей на основе графов атак и зависимостей сервисов; (3) методику выбора защитных мер, отличающуюся возможностью генерации комплекса защитных мер на основе доступных входных данных и его последующего уточнения; (4) архитектуру и программный прототип системы оценки защищенности и выбора защитных мер.

Дойниковой Е.В. в 2009 г. была присуждена квалификация математик в Санкт-Петербургском государственном электротехническом университете «ЛЭТИ» им. В.И. Ульянова (Ленина), на факультете компьютерных технологий и информатики по специальности «Компьютерная безопасность».

В процессе выполнения научной работы Дойникова Е.В. стала победителем конкурсного отбора на предоставление субсидий молодым ученым, молодым кандидатам наук вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга (2013 г., 2015 г.), ее статья была признана лучшей на Седьмой IEEE международной конференции «Интеллектуальное приобретение данных и передовые компьютерные системы: технологии и приложения» (2013 г.), заняла второе место в конкурсе молодых ученых Young School на конференции Positive Hack Days (2014 г.), награждена дипломом с отличием за самое эффективное решение на летней школе Microsoft «Исследуем в облаке» (2014 г.), выиграла конкурс грантов Санкт-Петербурга в сфере научной и научно-технической деятельности (2015 г.), награждена медалью Российской академии наук в области информатики, вычислительной техники и автоматизациии (2015 г.), награждена дипломом Общественной Палаты Санкт-Петербурга как финалист молодежной премии Санкт-Петербурга в области науки и техники (2016 г.).

Диссертант принимал активное участие в российских и международных научных конференциях (MobiSec-2016, CRiSIS-2015, Positive Hack Days-2014, PDP-2014, ARES 2013, IDAACS-2013, ИТУ-2012, PDP-2011 и т. д.) и проектах (РФФИ № 16-37-00338-мол_а 2016-2017 гг., грант РНФ № 15-11-30029 2015-2017 гг., Государственный контракт № 14.604.21.0137 2014-2016 гг., MASSIF 2010-2013 гг., и т. д.), проводимых в лаборатории Проблем компьютерной безопасности. По результатам работы диссертантом опубликовано большое количество работ, в том числе индексируемых в международных базах цитирования Web of Science и Scopus.

В ходе исследований диссертант продемонстрировал ответственность, инициативность, и глубину эрудиции и знаний в области технических дисциплин, и сложился как специалист в своей области. Диссертационная

работа заслуживает высокой оценки по своей новизне, актуальности, теоретической и практической обоснованности.

Полученные теоретические результаты важны для таких фундаментальных задач, как оценка защищенности и анализ рисков в компьютерных сетях, исследование и разработка систем управления информационной безопасностью в компьютерных сетях, анализ процессов обеспечения информационной безопасности. В настоящий момент теоретические результаты диссертационной работы используются для создания монографии по оценке рисков информационной безопасности.

Практическая значимость полученных результатов заключается в том, что реализация разработанных показателей, методик и алгоритмов как компонента систем управления информацией и событиями безопасности позволит снизить уровень потерь организаций при реализации компьютерных атак за счет постоянного отслеживания и пересчета показателей защищенности на основе поступающих данных о событиях в системе и своевременного применения рациональных защитных мер, что приведет к повышению уровня их защищенности.

Данная диссертационная работа является законченной научно-квалификационной работой, содержащей научно обоснованные результаты в области оценки защищенности компьютерных сетей и выбора защитных мер, имеющие существенное значение для экономики страны.

Диссертация выполнена в соответствии с требованиями, предъявляемыми к кандидатским диссертациям п. 9 Паспорта специальностей ВАК (технические науки) по специальности 05.13.19. Дойникова Е. В. имеет 9 статей в научных изданиях, рекомендованных ВАК на соискание ученой степени доктора и кандидата наук («Информационно-управляющие системы», «Безопасность информационных технологий», «Проблемы информационной безопасности. Компьютерные системы», «Известия высших учебных заведений. Приборостроение», «Труды СПИИРАН»), и заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность».

Научный руководитель,
зав. лабораторией
Проблем компьютерной
безопасности СПИИРАН,
д.т.н., профессор
тел. +7(921) 750-43-07, e-mail: ivkote@comsec.spb.ru

И. В. Котенко

16 января 2017 г.

Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ОГРН 1027800515983

заверяю,
Начальник отдела кадров СПИИРАН
Д.В.Токарев
16 января 2017 г.