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

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

« 09 » 01 2017 г. № 073-09/65/2

**УТВЕРЖДАЮ**

Юсупов Р.М.

# ЗАКЛЮЧЕНИЕ

Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН)

Диссертация «Оценка защищенности и выбор защитных мер в компьютерных сетях на основе графов атак и зависимостей сервисов» выполнена в лаборатории проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук.

В период подготовки диссертации соискатель Дойникова Елена Владимировна работала в ООО "Софея-Спб" в должности заместителя руководителя отдела тестирования (3 года), в ООО "СКАЙРОС ТЕХНОЛОГИИ" в должности инженера по тестированию (1 год), и в СПИИРАН, в должности младшего научного сотрудника (2 года), научного сотрудника (1 год).

В 2009г. окончила с отличием Санкт-Петербургский Государственный Электротехнический университет «ЛЭТИ» им. В.И. Ленина (Ульянова) по специальности «Компьютерная безопасность».

В 2013г. окончила аспирантуру (заочно) в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук.

Удостоверение о сдаче кандидатских экзаменов № 180, выдано в 2013г. Федеральным государственным бюджетным учреждением науки Санкт-Петербургским институтом информатики и автоматизации Российской академии наук.

Научный руководитель – доктор технических наук, профессор Котенко Игорь Витальевич, работает заведующим лабораторией проблем компьютерной безопасности в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук.

По результатам рассмотрения диссертации «Оценка защищенности и выбор защитных мер в компьютерных сетях на основе графов атак и зависимостей сервисов» принято следующее заключение:

В диссертационной работе соискатель Дойникова Е.В. рассматривает проблему оценки защищенности компьютерных сетей для поддержки принятия решений по реагированию на компьютерные инциденты. Выбор данного направления исследований обусловлен тем, что компьютерные сети получают все большее распространение во всем мире. Постоянный рост сложности компьютерных сетей, огромное количество взаимосвязанных сервисов, множество различных событий безопасности, усложняют процесс отслеживания ситуации по безопасности и принятия соответствующих решений по реагированию на инциденты информационной безопасности, что приводит к росту количества успешно проведенных компьютерных атак и, как следствие, к росту величины наносимого ими ущерба. Одним из перспективных направлений в данной области является использование показателей защищенности на основе графов компьютерных атак и зависимостей сервисов сети для оценки защищенности сетей против различных нарушителей и атак, и влияния реализации контрмер на защищенность сетей. Одной из основных проблем данного направления является многообразие источников информации по безопасности и разнообразие воздействующих факторов в современных сетях, а также постоянное изменение ситуации во времени. Таким образом, одной из ключевых задач данной предметной области является разработка комплексной системы показателей и соответствующих методик их вычисления, которые позволят учитывать различные характеристики компьютерных атак, а также различные аспекты функционирования защищаемой системы. В работе разработаны комплекс показателей защищенности компьютерных сетей, алгоритмы их вычисления, а также методики оценки защищенности и выбора контрмер на основе графов атак и зависимостей сервисов, учитывающие различные характеристики объектов оценки защищенности и различные аспекты функционирования защищаемой системы.

В работе лично Дойниковой Е.В. получены **следующие результаты**: (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.

**Обоснованность научных положений**, представленных в диссертационной работе, обеспечена проведением предварительного анализа существующих результатов исследований в данной предметной области. Результаты анализа использовались при формировании плана исследований и перечня необходимых на практике входных данных. Полученные практические положения находятся в непротиворечивом состоянии с результатами актуальных работ исследовательского сообщества. Основные теоретические положения работы изложены в печатных трудах и докладах на научных конференциях.

**Новизна** полученных автором результатов диссертационного исследования заключается в разработке и формализации методик оценки защищенности и выбора защитных мер на основе графов атак и зависимостей сервисов для своевременного принятия решений по реагированию на компьютерные инциденты в рамках систем мониторинга безопасности и управления инцидентами, позволяющих совместно учитывать различные входные данные, получать результат на основе доступных входных данных и автоматизированно уточнять его с появлением новых данных за счет применения иерархического комплекса показателей.

**Практическая ценность** работы состоит в том, что полученные теоретические результаты позволят достичь значительного повышения защищенности компьютерных сетей от атак за счет предоставления лицу, принимающему решения, актуальной и адекватной информации, позволяющей осуществлять проактивное управление инцидентами и событиями безопасности. Разработанная в рамках данного исследования методика должна лечь в основу перспективных систем защиты от сетевых атак, которые: 1) базируются на анализе графов атак и графов зависимостей сервисов; 2) используют большое количество разнородных входных данных для вычисления показателей защищенности и позволяют отражать состояние защищенности сети на различных уровнях детализации и с учетом различных режимов ее функционирования; 3) позволяют обнаруживать слабые места и проверять эффективность контрмер. Одним из основных преимуществ подобных систем оценки защищенности является возможность сокращения временного интервала между обнаружением компьютерных инцидентов и принятием решений по реагированию за счет автоматизации процесса анализа возможных целей атакующего, возможных последствий инцидента и контрмер и т.п., а также учет изменения ситуации во времени за счет анализа событий безопасности. Результаты данного исследования могут быть использованы для защиты компьютерных сетей, как коммерческими организациями, так и государственными. Предлагаемая методика позволит повысить эффективность реагирования на компьютерные инциденты, осуществляемые через сеть Интернет, а также расширить знания об атакующих и, как результат, повысить вероятность их обнаружения. Это особенно актуально в связи с ростом количества хакерских атак и необходимостью противодействия не только компьютерным инцидентам, но и их источникам.

**Предложенные в диссертационной работе** комплекс показателей защищенности, методика оценки защищенности, и архитектура компонента

оценки защищенности использовались в рамках проекта седьмой рамочной программы (FP7) Европейского Сообщества “Управление информацией и событиями безопасности в инфраструктурах услуг (MASSIF)” (контракт № 257475, 2010-2013). Разработанные комплекс показателей защищенности и методика оценки защищенности используются в рамках учебного процесса в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича. Предложенные методики оценки защищенности и выбора контрмер использовались в рамках научно-инновационной деятельности в ООО «Ароматы безопасности». В Группе Компаний «Омега» используются разработанные методики оценки защищенности и выбора контрмер, и программный прототип системы оценки защищенности и выбора контрмер.

Диссертационная работа соответствует требованиям п. 9 Положения о присуждении ученых степеней и п. 9 Паспорта специальностей ВАК (технические науки) по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Автор имеет девять публикаций в рецензируемых журналах из перечня ВАК, отражающих основные результаты исследования:

1. Дойникова Е. В. Динамическое оценивание защищенности компьютерных сетей в SIEM-системах [Текст] / Е. В. Дойникова, И. В. Котенко, А. А. Чечулин // Безопасность информационных технологий. – М.: ВНИИПВТИ, 2015. – № 3. – С. 33–42.
2. Дойникова, Е. В. Методики и программный компонент оценки рисков на основе графов атак для систем управления информацией и событиями безопасности [Текст] / Е. В. Дойникова, И. В. Котенко // Информационно-управляющие системы. – СПб. : Политехника, 2016. – № 5. – С. 54–65. – doi:10.15217/issn1684-8853.2016.5.54.
3. Дойникова, Е. В. Отслеживание текущей ситуации и поддержка принятия решений по безопасности компьютерной сети на основе системы показателей защищенности [Текст] / Е. В. Дойникова, И. В. Котенко // Изв. вузов. Приборостроение. – СПб. : СПбГУ ИТМО, 2014. – Т. 57, № 10. – С. 72–77. – ISSN 0021-3454.
4. Дойникова, Е. В. Показатели и методики оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов [Текст] / Е. В. Дойникова // Труды СПИИРАН. – СПб. : Наука, 2013. – Вып. 3 (26). – С. 54–68.
5. Котенко, И. В. Анализ защищенности автоматизированных систем с учетом социо-инженерных атак [Текст] / И. В. Котенко, М. В. Степашкин, Е. В. Дойникова // Проблемы информационной безопасности. Компьютерные системы. – СПб. : СПбПУ, 2011. – № 3. – С. 40–57.
6. Котенко, И. В. Вычисление и анализ показателей защищенности на основе графов атак и зависимостей сервисов [Текст] / И. В. Котенко, Е. В. Дойникова // Проблемы информационной безопасности. Компьютерные системы. – СПб. : СПбПУ, 2014. – № 2. – С. 19–36.
7. Котенко, И. В. Динамический перерасчет показателей защищенности на примере определения потенциала атаки [Текст] / И. В. Котенко, Е. В.

Дойникова, А. А. Чечулин // Труды СПИИРАН. – СПб.: Наука, 2013. – Вып. 7 (30). – С. 26–39. – ISSN: 2078-9181.

8. Котенко, И. В. Методика выбора контрмер на основе комплексной системы показателей защищенности в системах управления информацией и событиями безопасности [Текст] / И. В. Котенко, Е. В. Дойникова // Информационно-управляющие системы. – СПб. : Политехника, 2015. – № 3. – С. 60–69. – doi:10.15217/issn1684-8853.2015.3.60.
9. Котенко, И. В. Оценка защищенности информационных систем на основе построения деревьев социо-инженерных атак [Текст] / И. В. Котенко, М. В. Степашкин, Д. И. Котенко, Е. В. Дойникова // Изв. вузов. Приборостроение. – СПб. : СПбГУ ИТМО, 2011. – Т. 54, № 12. – С. 5–9. – ISSN 0021-3454.

В работах [4], [6], [7] описан разработанный соискателем комплекс показателей защищенности и алгоритмы их вычисления. Предложенная соискателем методика оценки защищенности на основе графов атак и зависимостей сервисов представлена в работах [1], [2], [4]. Основные элементы методики выбора контрмер, разработанной соискателем, описаны в работах [3] и [8]. Архитектура и программный прототип предложенной системы оценки защищенности и выбора контрмер приведены в работах [2] и [8].

Автореферат диссертации в целом отражает ее содержание.

Диссертация решает научную задачу разработки модельно-методического аппарата для оценки защищенности компьютерных сетей и выбора защитных мер для систем мониторинга безопасности и управления инцидентами.

Диссертация «Оценка защищенности и выбор защитных мер в компьютерных сетях на основе графов атак и зависимостей сервисов» Дойниковой Елены Владимировны рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Заключение принято на заседании лаборатории компьютерной безопасности.

Присутствовало на заседании: 11 чел.

Результаты голосования: «за» - 11 чел., «против» - 0 чел., «воздержалось» - 0 чел., протокол № 7 от «14» декабря 2016 г.

Заключение составил:
Доктор технических наук, профессор,
зам. дир. по информационной безопасности
тел. +7(921) 953-03-73, e-mail: maa1305@yandex.ru

А.А. Молдовян

Секретарь заседания:
Кандидат технических наук,
с.н.с. лаб. компьютерной безопасности
тел. +7(812) 328-71-81, e-mail: chechulin@comsec.spb.ru

А.А. Чечулин