ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.199.01 НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ САНКТ-ПЕТЕРБУРГСКОГО ИНСТИТУТА ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РОССИЙСКОЙ АКАДЕМИИ НАУК ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета 25.05.2017 г. № 1

О присуждении Дойниковой Елене Владимировне, гражданке Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Оценка защищенности и выбор защитных мер в компьютерных сетях на основе графов атак и зависимостей сервисов» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 21 февраля 2017 г., протокол № 1 диссертационным советом Д 002.199.01 на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, 199178, Россия, Санкт-Петербург, 14 линия ВО, дом 39, утвержден приказом Рособрнадзора номер 2472-618 от 8 октября 2010 года.

Соискатель Дойникова Елена Владимировна, 1986 года рождения, в 2009 г. с отличием окончила Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина) по специальности «Компьютерная безопасность» (диплом № ВСА 081292), в 2013 г. окончила заочную аспирантуру в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук. Удостоверение о сдаче кандидатских экзаменов № 180, выдано в 2013 г. Федеральным государственным бюджетным учреждением науки Санкт-Петербургским институтом информатики и автоматизации Российской академии наук. В настоящее время Дойникова Елена Владимировна работает научным сотрудником в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук.

Диссертация выполнена в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук.

Научный руководитель – доктор технических наук, профессор КОТЕНКО Игорь Витальевич, основное место работы: Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), главный научный сотрудник.

Официальные оппоненты:

ИВАНОВ Александр Юрьевич, доктор технических наук, профессор, Федеральное государственное казенное образовательное учреждение высшего образования «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации»;

НОВИКОВ Владимир Александрович, доктор технических наук, Федеральное государственное бюджетное военное образовательное учреждение высшего образования «Военно-космическая академия имени А.Ф.Можайского», кафедра Систем сбора и обработки информации, профессор, лауреат премии Президента Российской Федерации в области науки и инноваций для молодых ученых 2013 года, дали положительные отзывы на диссертацию.

Ведущая организация – акционерное общество «Научно-исследовательский институт «РУБИН», г. Санкт-Петербург, в своем положительном отзыве, подписанном Котенко Денисом Алексеевичем, кандидатом технических наук, заместителем начальника центра специальных работ АО «НИИ «Рубин», Таран Вадимом Владимировичем, кандидатом технических наук, доцентом, главным конструктором комплексной безопасности систем связи АО «НИИ «Рубин» и утвержденном Рунеевым Анатолием Юрьевичем, доктором военных наук, профессором, генеральным директором АО «НИИ «Рубин», указала, что диссертация Дойниковой Е.В. на соискание ученой степени кандидата технических наук является законченной научно-исследовательской работой. Автором в диссертации сформулирована и решена актуальная и практически значимая научная задача – разработка модельно-методического аппарата для оценки защищенности

компьютерных сетей и выбора защитных мер для систем мониторинга безопасности и управления инцидентами.

Соискателем предложены методики оценки защищенности и выбора контрмер, которые позволяют в рамках систем мониторинга безопасности и управления инцидентами получать адекватную оценку защищенности компьютерных сетей, критичных к требованиям безопасности, уточнять ее с появлением новых данных, и эффективно реагировать на инциденты за счет применения иерархического подхода, основанного на комплексном учете показателей различных объектов оценки, применимого в разных режимах работы системы. Для этого также уточнены параметры применяемых моделей объектов оценки, предложена классификация и сформирован комплекс показателей защищенности, разработаны алгоритмы, реализующие отдельные элементы предложенных методик. Текст автореферата полностью соответствует содержанию диссертации. Диссертационное исследование «Оценка защищенности и выбор защитных мер в компьютерных сетях на основе графов атак и зависимостей сервисов» является научно-квалификационной работой и соответствует критериям, изложенным в п. 9 “Положения о присуждении ученых степеней”, утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г., предъявляемых к кандидатским диссертациям, а его автор Дойникова Елена Владимировна заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Соискатель имеет 51 опубликованную работу, в том числе по теме диссертации 51 работа, опубликованных в рецензируемых научных изданиях 26 работ, из них опубликованных в изданиях, рекомендуемых ВАК РФ – 9, в изданиях, индексируемых в международных базах Scopus и Web Of Science – 12.

Основные научные результаты опубликованы в 51 научных трудах общим объемом 20 п.л., из которых 37 работ объемом 17,7 п.л., выполнены в соавторстве, а 14 работ объемом 2,3 п.л. – лично. Наиболее значимые работы по теме диссертации:

1. **Дойникова, Е. В.** Показатели и методики оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов / Е. В. Дойникова // Труды СПИИРАН. – 2013. – Вып. 3 (26). – С. 54–68.
2. **Котенко, И. В.** Вычисление и анализ показателей защищенности на основе графов атак и зависимостей сервисов / И. В. Котенко, Е. В. Дойникова // Проблемы

информационной безопасности. Компьютерные системы. – 2014. – № 2. – С. 19–36. *Личный вклад соискателя – 56%.*

3. **Котенко, И. В.** Динамический перерасчет показателей защищенности на примере определения потенциала атаки / И. В. Котенко, Е. В. Дойникова, А. А. Чечулин // Труды СПИИРАН. – 2013. – Вып. 7 (30). – С. 26–39. *Личный вклад соискателя – 50%.*
4. **Дойникова, Е. В.** Динамическое оценивание защищенности компьютерных сетей в SIEM-системах / Е. В. Дойникова, И. В. Котенко, А. А. Чечулин // Безопасность информационных технологий. – 2015. – № 3. – С. 33–42. *Личный вклад соискателя – 60%.*
5. **Дойникова, Е. В.** Методики и программный компонент оценки рисков на основе графов атак для систем управления информацией и событиями безопасности / Е. В. Дойникова, И. В. Котенко // Информационно-управляющие системы. – 2016. – № 5. – С. 54–65. *Личный вклад соискателя – 75%.*
6. **Котенко, И. В.** Методика выбора контрмер на основе комплексной системы показателей защищенности в системах управления информацией и событиями безопасности / И. В. Котенко, Е. В. Дойникова // Информационно-управляющие системы. – 2015. – № 3. – С. 60–69. *Личный вклад соискателя – 70%.*
7. **Дойникова, Е. В.** Отслеживание текущей ситуации и поддержка принятия решений по безопасности компьютерной сети на основе системы показателей защищенности / Е. В. Дойникова, И. В. Котенко // Изв. вузов. Приборостроение. – 2014. – Т. 57, № 10. – С. 72–77. *Личный вклад соискателя – 50%.*
8. **Kotenko, I.** Security metrics for risk assessment of distributed information systems / I. Kotenko, E. Doynikova // Proceedings of the IEEE 7th International Conference on “Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications”. – 2013. P. 646–650. *Личный вклад соискателя – 60%.*
9. **Doynikova, E.** Countermeasure selection based on the attack and service dependency graphs for security incident management / E. Doynikova, I. Kotenko // Lecture Notes in Computer Science. – Volume 9572. – Springer, 2016. – P.107–124. *Личный вклад соискателя – 75%.*

Оригинальность содержания диссертации составляет не менее 91% от общего объёма текста; цитирование оформлено корректно; заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не

обнаружено; научных работ, выполненных соискателем учёной степени в соавторстве без ссылок на соавторов не выявлено. Недостоверные сведения об опубликованных соискателем ученой степени работах в диссертации отсутствуют .

На автореферат диссертации поступило 5 отзывов, все отзывы положительны:

1) Военная академии связи им. С.М. Буденного. Отзыв составил профессор кафедры (автоматизированных систем специального назначения) Военной академии связи, к.т.н., доцент Авраменко В.С. Замечания: В автореферате не раскрыто, как определяется отклонение спрогнозированной последовательности атаки от реальной, что затрудняет понимание результатов эксперимента. Согласно тексту автореферата показатель AttackerSkillLevel может принимать качественные значения, однако неясно, как они используются в формуле (5). На рисунке 2 обобщенная схема методики оценки защищенности включает выбор контрмер, хотя это отдельный этап, который не входит в оценку защищенности.

2) ФГБУН Институт проблем транспорта им. Н.С. Соломенко РАН. Отзыв составил директор ФГБУН Институт проблем транспорта им. Н.С. Соломенко РАН, д.т.н., профессор Малыгин И.Г. Замечания: 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. В автореферате не указано, какие именно открытые базы данных используются в качестве источника входных данных. В автореферате не описано, какие технологии использовались при реализации прототипа, реализующего предложенные методики.

3) Публичное акционерное общество «Информационные телекоммуникационные технологии» (ПАО «ИНТЕЛТЕХ»). Отзыв составил начальник отдела отделения информационной безопасности, к.т.н., доцент Рощин А.А. Замечания: одним из положений, выносимых на защиту, является комплекс показателей защищенности компьютерных сетей на основе графов атак и зависимостей сервисов, однако в автореферате практически не приведены материалы по обоснованию такого выбора; в автореферате отмечается, что итоговая критичность ряда активов определяется путем обхода графа зависимостей сервисов, тем не менее, автор не поясняет причину такого решения и его влияния на итоговый результат.

4) Филиал АО «Концерн радиостроения «Вега» в г. Санкт-Петербурге. Отзыв составил ведущий научный сотрудник, д.т.н., профессор Оков И.Н. Замечания: В реальных системах практически никогда не известны точные значения параметров атакующих действий, таких как вероятности конкретных действий и состояний атакующего, вероятность компрометации узлов графа и т.п. Поэтому возникает вопрос: насколько в предлагаемой методике оценки защищенности неточен вычисленный уровень защищенности компьютерной сети? Отсутствуют оценки сложности реализации предлагаемых технических решений по обеспечению безопасности компьютерных сетей. В автореферате не приведено ни одного численного значения показателей защищенности, что затрудняет оценку степени достигнутого в работе повышения защищенности компьютерных сетей.

5) Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича. Отзыв составил доцент кафедры сетей связи и передачи данных, к.т.н., доцент Пантюхин О.И. Замечания: Из текста автореферата не ясно, как формируется список контрмер для выбора защитных вариантов. В тексте автореферата не описано, как вычисляется индекс выбора контрмер.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н., профессор Иванов А.Ю. является известным ученым в области автоматизированных систем управления и безопасности информационных систем; д.т.н. Новиков В.А. – известный ученый в области защиты специальных информационно-вычислительных систем; ведущая организация, акционерное общество «Научно-исследовательский институт «РУБИН», является известной как в России, так и за рубежом организацией в области разработки, внедрения и эксплуатации современных защищенных сетей связи и автоматизации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработаны

оригинальная методика оценки защищенности, основанная на иерархическом подходе, отличающемся комплексным применением моделей объектов защищенности (в том числе, графов атак и графов зависимостей сервисов), связи между которыми сформированы за счет введения дополнительных параметров моделей; уровни

иерархии определены таким образом, чтобы на каждом уровне получать адекватную оценку защищенности в форме количественных показателей защищенности на основе доступных на текущий момент данных и уточнять ее при поступлении новых данных путем перехода на новый уровень иерархии;

оригинальная методика выбора контрмер, основанная на двухуровневом подходе при котором на этапе проектирования выбираются средства защиты, позволяющие снизить риск до приемлемого уровня, а в режиме эксплуатации выбираются контрмеры для проходящей в реальном времени атаки в случае непредвиденных инцидентов или наличия уязвимостей нулевого дня, что позволяет повысить защищенность компьютерных сетей;

предложены:

комплекс показателей защищенности на основе графов атак и зависимостей сервисов, отличающийся способом классификации показателей на основе объектов оценки, этапов процесса оценки защищенности и различных аспектов безопасности, каждая группа которого позволяет сформировать оценку защищенности с уровнем точности, соответствующем доступным на текущий момент данным;

новые алгоритмы вычисления показателей защищенности в рамках методик оценки защищенности и выбора контрмер, использующие в качестве входных данных разнородную информацию по безопасности (о сети и ее уязвимостях, зависимостях сервисов, атаках, атакующих, событиях, контрмерах, экспертных оценках уязвимостей и контрмер, и оценках из открытых баз данных), и отличающиеся для различных уровней подхода, лежащего в основе предложенных методик; алгоритмы различных уровней иерархически связаны между собой: выходные данные алгоритмов каждого предыдущего уровня используются в качестве входных данных алгоритмов следующего уровня, что позволяет уточнять показатели за счет новых входных данных.

доказана экспериментально перспективность использования предложенного подхода и методик на его основе для построения систем управления защищенностью компьютерных сетей;

введены:

- новая классификация показателей, основанная на категориях и объектах оценки;
- требования к входным данным, применяемым для конкретизации параметров моделей объектов оценки;
- требования к программно-аппаратному обеспечению, необходимому для установки и корректного функционирования разработанной системы оценки защищенности и выбора контрмер;

Теоретическая значимость исследования обоснована тем, что:

доказаны сформулированные в работе теоретические утверждения результатами проведенных экспериментов с использованием разработанного программного прототипа, реализующего предложенные модели и методики. Эти утверждения составляют основу разработанных методик оценки защищенности и выбора защитных мер;

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов)

использованы аппарат и методы теории графов, теории вероятностей, теории принятия решений, экспертного анализа;

изложены методологические и методические основы использования аналитического моделирования для задачи оценки защищенности и выбора защитных мер;

раскрыты

основные проблемы применения существующих методов оценки защищенности и выбора контрмер для компьютерных сетей;

проблемы получения и обработки входных данных для оценки защищенности, а также особенности современных компьютерных сетей, влияющие на требования к методикам оценки защищенности и выбора контрмер;

применимость аналитических моделей для оценки защищенности и выбора контрмер, недостатки существующих моделей, проблемы их совместного применения;

изучены существующие модели (в форме графов), методики, алгоритмы и показатели качественной и количественной оценки защищенности компьютерных сетей и выбора контрмер, предложенные различными исследователями, при этом отдельное внимание уделено рассмотрению вопросов их применения в рамках систем мониторинга безопасности и управления инцидентами;

проведена модернизация существующих методов, методик и алгоритмов оценки защищенности и выбора контрмер на основе аналитического моделирования и количественных показателей защищенности.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены следующие результаты диссертационной работы:

• комплекс показателей защищенности, показатели которого разделены на классы в зависимости от учитываемых входных данных и категорий оценки, позволяющий получить адекватную оценку характеристик различных объектов;

• методика оценки защищенности компьютерной сети, основанная на комплексном учете данных из разных источников для формирования оценки защищенности и выбора защитных мер в любой момент времени с соответствующей степенью точности;

• 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) при формировании компонента анализа защищенности перспективной системы мониторинга безопасности и управления инцидентами;

• комплекс показателей защищенности компьютерных сетей на основе графов атак и зависимостей сервисов;

• методика оценки защищенности компьютерных сетей на основе графов атак и зависимостей сервисов;

используются кафедрой Защищенных систем связи (ЗСС) ФГБОУ высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» в рамках учебного процесса на старших курсах обучения бакалавров по направлению подготовки 10.03.01 «Информационная безопасность» по дисциплинам «Программно-аппаратные средства обеспечения информационной безопасности» (рабочая программа дисциплины, регистрационный №02.34.15/1753) и «Основы информационной безопасности» (рабочая программа дисциплины, регистрационный №10.14/94) при чтении курсов лекций, проведении практических и лабораторных работ.

• методика оценки защищенности на основе графов атак и зависимостей сервисов, использовалась для получения комплекса показателей, адекватно характеризующих защищенность компьютерной сети;

• методика выбора защитных мер на основе графов атак и зависимостей сервисов, использовалась для поддержки принятия решений по реагированию и позволила ускорить процесс выбора рациональных защитных мер и сократить потери организации из-за остановки бизнес-процессов в результате успешной реализации атакующих действий;

использовались в рамках научно-инновационной деятельности в ООО «Ароматы безопасности».

• методики оценки защищенности компьютерной сети и выбора защитных мер;

• архитектура и программная реализация системы оценки защищенности компьютерной сети и выбора защитных мер;

используются ГК «Омега» в рамках рабочего процесса при управлении безопасностью компьютерной сети организации.

определены возможности и перспективы практического использования полученных результатов диссертации при разработке систем управления безопасностью компьютерных сетей;

создан подход к оценке защищенности и выбору защитных мер для компьютерных сетей на основе методов аналитического моделирования, позволяющий совместно учитывать характеристики анализируемых объектов и в каждый момент времени получать оценку защищенности и выбирать защитные меры, и лишенный недостатков известных методик;

представлены предложения и направления для дальнейших научных исследований, в основу которых могут быть положены разработанные методики, модели и алгоритмы.

Оценка достоверности результатов исследования выявила:

для экспериментальных работ

достоверность полученных результатов, которая была подтверждена проведением предварительного анализа существующих исследований в данной предметной области, корректным применением научно-методического аппарата, апробацией основных результатов диссертации в печатных трудах и докладах на международных и всероссийских конференциях, теоретическим анализом разработанных алгоритмов, положительными результатами экспериментальных исследований алгоритмов, моделей и методик и сравнительного анализа предложенных методик с существующими аналогами;

теория построена на известных принципах, проверенных данных и фактах с использованием современных известных и апробированных методов исследования, согласуется с опубликованными частными результатами других исследователей;

идея базируется на анализе работ отечественных и зарубежных исследователей в области оценки защищенности компьютерных сетей и выбора защитных мер;

использованы полученные характеристики для сравнения с данными, приведенными в современной научной литературе по анализу защищенности;

установлено качественное и количественное соответствие результатов решения задачи разработки модельно-методического аппарата для оценки защищенности компьютерных сетей и выбора защитных мер для систем мониторинга безопасности и управления инцидентами. При этом подтверждены преимущества предложенного подхода перед результатами, полученными другими авторами.

использованы современные методики сбора и обработки исходной информации, представительные выборочные совокупности с обоснованием подбора объектов (единиц) наблюдения и измерения и т.п.)

Личный вклад соискателя состоит в:

- анализе современного состояния дел в области оценки защищенности и выбора контрмер;
- исследовании и классифицировании существующих показателей защищенности и методик их вычисления на основе моделей умышленных атак в компьютерных сетях в виде графов атакующих действий и моделей распространения воздействия атаки в сети в виде графов зависимостей сервисов;
- постановке задачи разработки методик оценки защищенности и выбора контрмер на основе графов атак и зависимостей сервисов;
- разработке комплекса показателей защищенности с учетом различных входных данных, таких как модели компьютерной сети, атакующих действий, нарушителей и инцидентов безопасности, и на различных уровнях функционирования защищаемой системы (статическом и динамическом);
- разработке методики оценки защищенности компьютерных сетей на основе графов атак и зависимостей сервисов;
- разработке алгоритмов вычисления показателей защищенности;
- разработке методики выбора защитных мер для реагирования на компьютерные атаки с учетом доступных данных;
- построении архитектуры и реализации программного прототипа системы оценки защищенности компьютерных сетей и выбора защитных мер на основе предложенных методик.
- экспериментальной оценке предложенных алгоритмов и методик, и сравнении их с существующими аналогами.
- подготовке основных публикаций по выполненной работе.

Диссертационный совет считает, что Дойникова Е.В. в своей диссертационной работе решила научную задачу разработки модельно-методического аппарата для оценки защищенности компьютерных сетей и выбора защитных мер для систем

мониторинга безопасности и управления инцидентами, имеющую важное социально-экономическое и хозяйственное значение.

На заседании 25.05.2017 г. диссертационный совет принял решение присудить Дойниковой Е.В. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 23 человек, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 23, против нет, недействительных бюллетеней нет.

Председатель диссертационного совета
доктор технических наук,
член-корреспондент РАН Юсупов Рафаэль Мидхатович

Ученый секретарь диссертационного совета
доктор технических наук Кулешов Сергей Викторович
25.05.2017 г.