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 27.12.2016 г. № 1

О присуждении Нурдинову Руслану Артуровичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Модель количественной оценки рисков безопасности корпоративной информационной системы на основе метрик» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 24 октября 2016 г., протокол № 2 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 Нурдинов Руслан Артурович, 1991 года рождения, в 2013 году с отличием окончил Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» по специальности «Организация и технология защиты информации» (диплом ОК № 35837), в 2016 году окончил очную аспирантуру в Федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Удостоверение о сдаче кандидатских экзаменов выдано 5 июня 2016 года. В настоящее время Нурдинов Руслан Артурович работает инженером-проектировщиком в ООО «Газинформсервис», где проектирует системы защиты информации.

Диссертация выполнена на кафедре безопасных информационных технологий Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».

Научный руководитель – доктор военных наук, профессор КАТОРИН Юрий Федорович, основное место работы: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», профессор кафедры безопасных информационных технологий.

Официальные оппоненты:

БЕЗЗАТЕЕВ Сергей Валентинович, доктор технических наук, доцент, Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», заведующий кафедрой технологий защиты информации,

ГОНЧАРЕНКО Владимир Анатольевич, кандидат технических наук, доцент, Федеральное государственное бюджетное военное образовательное учреждение высшего образования «Военно-космическая академия имени А.Ф.Можайского» Министерства обороны Российской Федерации, профессор кафедры информационно-вычислительных систем и сетей.

Дали положительные отзывы на диссертацию.

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный технологический институт (технический университет)» в своем положительном заключении, подписанном Холодновым Владиславом Алексеевичем, доктором технических наук, профессором, профессором кафедры системного анализа и информационных технологий и утвержденном ректором Шевчиком Андреем Павловичем, доктором технических наук, доцентом, указала, что в целом диссертационная работа Нурдинова Руслана Артуровича представляет собой завершенную научно-исследовательскую работу, выполненную на актуальную тему, которая отличается научной новизной и практической значимостью полученных результатов. В диссертационной работе сформулирована и решена актуальная научная

задача разработки методического аппарата, позволяющего повысить качество выбора защитных мер за счет применения научно-обоснованной формализованной модели количественной оценки рисков. Основные результаты работы, выводы и рекомендации представлены в автореферате, содержание которого достаточно полно отражает суть диссертации. Диссертационная работа Нурдинова Руслана Артуровича соответствует требованиям, установленным п. 9 Положения о присуждении ученых степеней, утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842, предъявляемым к кандидатским диссертациям, а её автор заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». Диссертационная работа и отзыв обсуждены и одобрены на заседании кафедры системного анализа и информационных технологий, протокол № 3 от 28 октября 2016 г.

Соискатель имеет 17 опубликованных работ (все по теме диссертации), из них статей в журналах, рекомендованных Высшей аттестационной комиссией при Министерстве образования и науки Российской Федерации, – 5.

Основные научные результаты опубликованы в 17 научных трудах общим объемом 6,7 п.л., из которых 12 статей объемом 4,4 п.л., выполнены в соавторстве, а 5 статей объемом 1,3 п.л. – лично. Наиболее значимые работы по теме диссертации:

1. **Нурдинов Р.А.** Количественная оценка вероятности реализации угроз нарушения безопасности АСУ технологическими процессами террористическими группировками / Каторин Ю.Ф., **Нурдинов Р.А.**, Зайцева Н.М., Канев А.Н., Иоффе М.А. // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. Т. 3-4 (93-94). С. 3-9. *Личный вклад соискателя – 20%.*

2. **Нурдинов Р.А.**, Обеспечение комплексной безопасности сложных промышленных объектов на базе риск-ориентированных стандартов / Лившиц И.И., **Нурдинов Р.А.**// Информатизация и Связь. 2016. № 1. С. 49-55. *Личный вклад соискателя – 50%.*

3. **Нурдинов Р.А.** Модель количественной оценки рисков безопасности информационной системы / Каторин Ю.Ф., **Нурдинов Р.А.**, Зайцева Н.М. // Новый университет. Серия: Технические науки. 2016. № 3 (49). С. 42-47. *Личный вклад соискателя – 35%.*

4. **Нурдинов Р.А.** Оценка ущерба от правонарушений в информационной сфере / **Нурдинов Р.А.**, Зайцева Н.М. // Вестник полиции. 2015. № 4. С. 124-132. *Личный вклад соискателя – 50%.*

5. **Nurdinov R.A.** The Quantitative Assessment Model of Information System Risk Based on Metrics / **Nurdinov R.A**., Kanev A.N. // First Information Security and Protection of Information Technologies conference. St. Peterburg, 2015. P. 37-41. *Личный вклад соискателя – 50%.*

6. **Нурдинов Р.А.** Определение уровня защиты объекта на основании анализа информационных рисков / Каторин Ю.Ф., **Нурдинов Р.А.** // Вестник КИГИТ. 2014. № 7 (48). С. 31-40. *Личный вклад соискателя – 50%.*

7. **Нурдинов Р.А.** Обоснование целесообразности выбора средств защиты информации // Современные наукоемкие технологии. 2014. № 5-1. С. 81-82.

Оригинальность содержания диссертации составляет не менее 95% 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.

На автореферат диссертации поступило 12 отзывов, все отзывы положительны:

1. ФГКОУ ВПО «Санкт-Петербургский университет Министерства внутренних дел РФ». Отзыв составил профессор кафедры специальных информационных технологий, д.т.н., профессор Синещук Ю.И. Замечания: система мер защиты сведена только к организационным и техническим средствам защиты; в явном виде не сформулирован критерий достижения цели исследования – повышение качества выбора защитных мер; отсутствует обоснование взаимосвязи и иерархии понятий: безопасности, надежность, информационная безопасность; не раскрыто содержание понятия – «деструктивное состояние».

2. ФГБОУ ВО «Государственный университет морского и речного флота имени адмирала С.О. Макарова». Отзыв составил профессор кафедры комплексного обеспечения информационной безопасности, д.т.н., профессор Гаскаров В.Д. Замечания: в автореферате отсутствуют ссылки на аналогичные или близкие работы по той же тематике, выполненные российскими авторами; также можно отметить ряд незначительных недостатков, таких как наличие нерасшифрованных сокращений или

отсутствие пояснений к структуре многослойного персептрона, представленного в автореферате.

3. ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого». Отзыв составил профессор кафедры информационной безопасности компьютерных систем, к.т.н., профессор Платонов В.В. Замечания: выбор аппроксимирующей функции (формула 2) не обоснован, существует множество нелинейных функций, которые дифференцируемы и имеют аналогичную область значений; при вычислении стоимости активов в формуле 15 не используются веса, поэтому все виды последствий (финансовые, репутационные, производственные и т.п.) считаются равнозначными; не обоснован выбор значения порогового элемента, равного 0,5.

4. АО «Научно-исследовательский институт телевидения». Отзыв составил заместитель генерального директора по информационным технологиям, д.т.н., профессор Кузичкин А.В. Замечания: категории защитных мер приведены в таблице 2 в виде условных обозначений, которые нигде по тексту автореферата не расшифровываются, кроме того, отсутствует обоснование выбора именно этих категорий защитных мер в ходе проводимого экспериментального исследования; отсутствует пояснение, каким образом модели и методики, предложенные в работе, были использованы при разработке модуля управления рисками.

5. ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения». Отзыв составил заведующий кафедрой радиотехнических и оптоэлектронных комплексов, д.т.н., профессор Крячко А.Ф. Замечания: из содержания не ясно, на основе каких данных строился график, представленный на рисунке 4; приведено достаточно краткое описание разработанного модуля управления рисками, не позволяющее в должной мере оценить его оригинальность и значимость.

6. ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ». Отзыв составил заведующий кафедрой систем информационной безопасности, к.т.н., доцент Аникин И.В. С. Замечания: отсутствие в автореферате конкретных примеров сценариев реализации угроз затрудняет понимание разработанной модели оценки рисков; в автореферате не приводится состав комплексов защитных мер, приведенных в таблице 3, что не позволяет в полной мере определить объективность результатов их оценки.

7. ООО «Уральский центр систем безопасности». Отзыв составил менеджер по развитию решений по информационной безопасности, к.т.н. Липатов А.Л. Замечания: в автореферате довольно кратко представлено описание модели сценариев реализации угроз и не приводятся примеры конкретных сценариев; в автореферате отсутствуют сведения о стоимостных показателях, используемых для оценки ущерба.

8. ООО «Инженерно-технологическая сервисная компания». Отзыв составила руководитель проектов, к.т.н. Иващук И.Ю. Замечания: при формировании модели количественной оценки рисков не учитывается отраслевая специфика предприятия, что не позволяет в полной мере определить объективность результатов их оценки и может повлечь за собой ряд ограничений при формировании комплекса защитных мер; в автореферате не раскрыт подход к формированию альтернативных комплексов защитных мер с учетом заявленных ограничений: совместимости и взаимозависимости защитных мер в составе комплекса, а также требований нормативных документов к формируемой СЗИ.

9. ООО «Газпром добыча Ноябрьск». Отзыв составили главный инженер, к.т.н. Кононов А.В. и начальник отдела информационной безопасности Ветлужских Е.О. Замечания: из автореферата не ясно, каким образом формируются альтернативные комплексы защитных мер, и как учитывается совместимость защитных мер в составе комплекса; в автореферате не указано, каким образом определялись объекты обучающей выборки в ходе проведенных экспериментов.

10. АО «Диаконт». Отзыв составил генеральный директор, к.т.н. Федосовский М.Е. Замечания: не приводятся расшифровки некоторых сокращений и обозначений, используемых в автореферате; отсутствует характеристика функциональности модуля управления рисками; не определена возможность и целесообразность адаптации представленных в работе моделей и методик для систем с децентрализованной системой управления.

11. ООО «Газпром нефтехим Салават». Отзыв составил главный специалист отдела информационной безопасности, к.т.н. Павловский А.В. Замечания: в автореферате не приводятся данные, на основе которых осуществлялся расчёт показателей, приведённых в таблице 3, что затрудняет определение корректности приведённых результатов оценки комплексов защитных мер; автор не приводит в автореферате информацию об инструментальном программном обеспечении, использованном для оценки разработанных методик и модели на практике.

12. ЗАО «НПО «Эшелон – Северо-Запад». Отзыв составил директор департамента сертификации и аттестации, к.т.н., Степашкин М.В. Замечания: понимание механизма оценки стоимости активов КИС затруднено вследствие отсутствия примеров и правил определения показателей последствий, характеризующих финансовые, репутационные и иные потери; на рисунке 3 в качестве входных данных методики формирования рационального комплекса защитных мер не отражены ограничения, подлежащие учёту при формировании альтернативных комплексов защитных мер; в автореферате не указано, можно ли использовать предложенную соискателем методику формирования рационального комплекса защитных мер при фиксации пользователем допустимого остаточного риска; рисунок 9 выполнен с рядом недостатков, в том числе: 1) несоответствие подрисуночной надписи («модуль») графическому блоку на рисунке («система»), 2) отсутствие ряда связей (между элементами модуля управления рисками, например, между сервером баз данных и сервером приложений), 3) не отражены границы КИС.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н., доцент Беззатеев С.В. является известным ученым в области разработки методов, методик и моделей оценки безопасности и надежности сложных систем; к.т.н., доцент, Гончаренко А.В. – известный специалист в области моделирования и оценивания устойчивости информационных систем и компьютерных сетей к деструктивным воздействиям, Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный технологический институт (технический университет)» является известной как в России, так и за рубежом организацией в области анализа безопасности и надёжности технических систем.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработан методический аппарат, позволяющий осуществлять рациональный выбор защитных мер для корпоративных информационных систем за счет применения научно-обоснованной формализованной модели количественной оценки рисков;

предложены:

- оригинальная формализованная модель количественной оценки рисков безопасности корпоративной информационной системы, отличающаяся набором связанных переходов ее элементов в деструктивные состояния, рассматриваемых в качестве событий риска. Использование модели позволяет осуществлять переоценку рисков при изменении исходных данных без повторного привлечения экспертов;
- методика формирования рационального комплекса защитных мер для корпоративной информационной системы, отличающаяся применением предложенного в работе показателя затратоемкости активов и разработанной формализованной модели количественной оценки рисков. Применение методики позволяет повысить качество выбора защитных мер за счет минимизации показателя затратоемкости активов;
- уникальная методика количественной оценки вероятности реализации угроз на основе определения метрик нарушителей и защитных мер, отличающаяся использованием комбинации экспертных и нейросетевых методов. Применение методики позволяет повысить точность прогнозирования вероятности событий риска.

доказана перспективность использования диагонального метода Левенберга-Марквардта для настройки весовых коэффициентов, характеризующих степень важности метрик нарушителей и защитных мер.

введены:

- набор связанных переходов элементов корпоративной информационной системы в деструктивные состояния, рассматриваемых в качестве событий риска;
- наборы взвешенных метрик: первый позволяет осуществлять оценку интегрального показателя степени опасности нарушителя, второй позволяет осуществлять оценку интегрального показателя степени реализации превентивных и корректирующих защитных мер;
- новый показатель затратоемкости активов, определяемый отношением суммы реальных затрат на защитные меры и предполагаемых затрат (остаточного риска) к стоимости защищаемых активов.

Теоретическая значимость исследования обоснована тем, что:

доказана перспективность использования разработанных моделей и методик в научной и практической деятельности, их непротиворечивость и согласованность с современными практиками в области оценки рисков информационной безопасности;

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) **использованы** логические приемы образования понятий, методы системного и структурного анализа, теории множеств, теории оптимизации и теории графов, методы математической статистики, теории вероятностей, теории нейронных сетей и метод анализа иерархий;

изложены основные понятия предметной области оценки рисков безопасности информационных систем, а также методологические основы применения разработанных моделей и методик оценки рисков;

раскрыты проблемные аспекты применения существующих экспертных и формализованных методик и моделей оценки рисков. Основные вопросы связаны с получением объективных количественных оценок недостаточной точностью и субъективностью экспертных методов с одной стороны и высокой трудоёмкостью проработки моделей оценки для реальных информационных систем с другой стороны. Также затронута проблема использования статистических данных для оценки рисков, возникающая ввиду их неполноты, неоднородности и неточности;

изучены существующие методы машинного обучения применительно к решению задачи настройки весовых коэффициентов метрик нарушителей и защитных мер, при этом отдельное внимание уделено рассмотрению методов, основанных на коррекции ошибок, применяемых для обучения искусственных нейронных сетей.

проведена модернизация существующей методологической основы построения формализованной модели оценки рисков безопасности корпоративной информационной системы, реализованной в разработанном программном модуле, которая заключается:

- в определении инфраструктурной модели корпоративной информационной системы, представляющей собой неориентированный граф, вершинами которого являются элементы корпоративной информационной системы (технические средства,

линии связи, программное обеспечение, информационные активы), а рёбрами – связи между данными элементами;

- в определении модели сценариев реализации угроз корпоративным информационным системам, представляющей собой ориентированный граф, вершинами которого являются классы источников угроз и деструктивные состояния элементов корпоративной информационной системы, а дугами – причинно-следственные связи переходов элементов в деструктивные состояния;
- в синтезе модели оценки рисков на основе инфраструктурной модели корпоративной информационной системы и модели сценариев реализации угроз по предложенным формализованным правилам.

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

разработаны и внедрены (указать степень внедрения) следующие результаты диссертационной работы:

1. Модель количественной оценки рисков безопасности корпоративной информационной системы внедрена в производственный процесс ООО «Газпром трансгаз Санкт-Петербург». Модель использована при реализации программного модуля управления рисками информационной безопасности в составе системы автоматизации процессов управления информационной безопасностью, что позволило повысить эффективность и результативность процесса управления рисками информационной безопасности в компании.
2. Методика формирования рационального комплекса защитных мер внедрена в производственный процесс ООО «Газинформсервис». Методика используется при проектировании систем защиты для автоматизированных и информационных систем, что позволило повысить эффективность проектируемых и внедряемых компанией комплексных решений по обеспечению информационной безопасности.
3. Методики и модели оценки рисков безопасности корпоративной информационной системы, а также результаты сравнительного анализа подходов к оценке рисков информационной безопасности внедрены в учебный процесс ЧОУ ДПО «Центр предпринимательских рисков». Использование данных результатов позволило повысить качество и глубину проработки материалов курса «Управление

информационной безопасностью» по вопросам управления рисками информационной безопасности, что нашло положительный отклик у слушателей курса.

4. Модель количественной оценки рисков безопасности корпоративной информационной системы и методика формирования рационального комплекса защитных мер для корпоративной информационной системы внедрены в учебный процесс кафедры безопасных информационных технологий Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Данные результаты использованы при подготовке учебных материалов по дисциплинам «Организация и управление службой защиты информации» и «Технологии обеспечения информационной безопасности объекта».

определены возможности и перспективы практического использования полученных результатов диссертации при проектировании систем защиты информации;

создан программный модуль управления рисками информационной безопасности, подтверждающий корректность предложенных в диссертационной работе модели оценки рисков и методики количественной оценки вероятности реализации угроз нарушителем на основе экспертно-нейросетевого определения метрик;

представлены предложения и направления для дальнейших научных исследований, которые заключаются в адаптации разработанных моделей и методик для различных классов информационных и автоматизированных систем.

Оценка достоверности результатов исследования выявила:

идея базируется на обобщении передового опыта в области оценки рисков информационной безопасности и выбора защитных мер для информационных и автоматизированных систем и компьютерных сетей, на анализе трудов отечественных и зарубежных специалистов в этой области;

теория построена на известных принципах, проверенных данных и фактах с использованием современных апробированных методов исследования. Основные результаты диссертации опубликованы в рецензируемых научных изданиях,

апробированы на международных и всероссийских конференциях и внедрены в практику деятельности научных и производственных организаций;

использованы действующие стандарты и передовые практики, применяемые при формировании систем защиты информации. Базовые наборы метрик нарушителей и защитных мер сформированы на основе положений действующих ГОСТ и руководящих документов ФСТЭК России. При этом предложенная в диссертации методика количественной оценки вероятности реализации угроз нарушителем на основе экспертно-нейросетевого определения метрик может быть использована для актуализации базовых наборов метрик на основе данных об инцидентах информационной безопасности.

для экспериментальных работ показана воспроизводимость результатов вычислительных экспериментов, выполненных на современном оборудовании, возможность отбора значимых метрик в процессе обучения, а также возможность обучения на неполных, неточных, нечисловых и неоднородных данных об инцидентах информационной безопасности;

установлено качественное и количественное соответствие результатов вычислительных экспериментов теоретическим выводам и экспериментальным результатам, полученным другими авторами в опубликованных работах по смежным областям исследования.

Личный вклад соискателя состоит в:

- анализе предметной области оценки рисков безопасности информационных систем;
- сравнении существующих подходов и математических методов количественной оценки рисков информационной безопасности, выявлении проблем и ограничений в их применении;
- постановке научной задачи и частных задач исследования;
- разработке формализованной модели оценки рисков безопасности корпоративной информационной системы на основе определения деструктивных состояний ее элементов;

- определении показателя качества выбора защитных мер и системы ограничений при разработке методики формирования рационального комплекса защитных мер;
- сборе, обработке и анализе результатов экспертных оценок для определения начальных значений весовых коэффициентов метрик с использованием метода анализа иерархий;
- экспериментальном исследовании по настройке весовых коэффициентов метрик с использованием разработанного программного кода;
- разработке программного модуля управления рисками, позволяющего автоматизировать процедуры оценки рисков безопасности корпоративной информационной системы на основе предложенных в диссертации моделей и методик;
- выступлениях на научно-технических конференциях и подготовке основных публикаций по выполненной работе.

Выводы

Диссертационный совет считает, что Нурдинов Руслан Артурович в своей диссертационной работе решил актуальную научную задачу разработки методического аппарата, позволяющего повысить качество выбора защитных мер за счет применения научно-обоснованной формализованной модели количественной оценки рисков, имеющую важное значение для науки и практики.

Диссертационная работа Нурдинова Руслана Артуровича соответствует пунктам 7 и 10 паспорта специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность», и требованиям, установленным п. 9 Положения о присуждении ученых степеней, утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842, предъявляемым к кандидатским диссертациям.

На заседании 27.12.2016 г. диссертационный совет принял решение присудить Нурдинову Руслану Артуровичу ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 22 человек, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 20, против 0, недействительных бюллетеней 2.

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

Ученый секретарь диссертационного совета
кандидат технических наук, доцент Фаткиева Роза Равильевна
27.12.2016 г.