ОТЗЫВ

официального оппонента Гончаренко Владимира Анатольевича
на диссертационную работу НУРДИНОВА Руслана Артуровича
«Модель количественной оценки рисков безопасности корпоративной информационной системы на основе метрик»,
представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

I. Актуальность темы диссертации

Проблема обеспечения безопасности корпоративных информационных систем (КИС) в условиях ограниченного бюджета приобретает все большее значение для государственных и коммерческих организаций.

Выбор наиболее подходящего комплекса защитных мер для КИС может осуществляться на основе анализа рисков информационной безопасности, выполняемого преимущественно с использованием экспертных методов, трудно поддающихся формализации.

Вместе с тем сложность структуры и функциональности современных КИС, многообразие возможных угроз и средств защиты, а также постоянное изменение значимых признаков затрудняют использование неформализованных экспертных методов для оценки рисков безопасности КИС.

Все сказанное позволяет сделать вывод о том, что тема диссертационной работы Нурдинова Р.А., посвященной разработке формализованной модели количественной оценки рисков безопасности КИС на основе метрик, является, несомненно, актуальной, перспективной и своевременной.

II. Научная новизна основных результатов исследований

В диссертации представлено три основных научных результата:

1. Модель оценки рисков безопасности корпоративной информационной системы на основе определения деструктивных состояний ее элементов.
2. Методика формирования рационального комплекса защитных мер для корпоративной информационной системы на основе минимизации значения показателя затратоемкости активов.
3. Методика количественной оценки вероятности реализации угроз нарушителем на основе экспертно-нейросетевого определения метрик.

Новизна первого научного результата состоит в том, что в модели оценки рисков предложен оригинальный набор взаимосвязанных переходов элементов

КИС в деструктивные состояния, выступающих в качестве событий риска. Приведены правила оценки значений вероятности и ущерба для событий риска в предложенной модели.

Во втором научном результате задача выбора рационального комплекса защитных мер формализована как экстремальная задача теории принятия решений. При этом критерием оптимизации является минимизация значения показателя затратоёмкости активов, предложенного в диссертации.

В третьем научном результате предложен новый подход к определению совокупности согласованных метрик, используемых для оценки вероятности реализации угроз нарушителем. Для определения значений весовых коэффициентов метрик используется комбинация экспертных и нейросетевых методов.

III. Теоретическая и практическая значимость результатов исследований

Теоретическая значимость результатов диссертации определяется актуальностью темы исследования и новизной полученных результатов. Предложенные в диссертации модели и методики позволяют повысить эффективность выбора защитных мер для КИС за счет увеличения точности количественной оценки рисков.

Предложенные в диссертации модели и методики вносят определенный вклад в развитие теории рисков информационной безопасности. Это подтверждается их использованием при подготовке учебных материалов для кафедры безопасных информационных технологий Университета ИТМО и ЧОУ ДПО «Центр предпринимательских рисков».

Практическая ценность результатов диссертации состоит в том, что они могут использоваться для оценки рисков информационной безопасности, а также для формирования и совершенствования систем защиты информации КИС. Это подтверждается их внедрением в практику деятельности ООО «Газинформсервис» и ООО «Газпром трансгаз Санкт-Петербург».

Универсальность предложенных моделей и методик позволяет адаптировать их для различных видов информационных и автоматизированных систем.

Предложенные в диссертации модели и методики могут быть использованы при создании автоматизированных систем оценки рисков информационной безопасности и систем поддержки принятия решений по формированию комплексов защитных мер для корпоративных информационных систем.

IV. Достоверность и обоснованность основных результатов исследований

Основные положения, выводы и рекомендации, полученные в диссертации, достаточно обоснованы и аргументированы. Сформулированная в диссер-

тации научно-техническая задача была исследована и решена на основе корректного использования методов системного анализа, теории множеств, теории оптимизации, теории графов, математической статистики, теории вероятностей, теории нейронных сетей.

Обоснованность полученных результатов и выводов достигается:

– корректностью использования апробированного математического аппарата;

– использованием системного анализа, структурного анализа и теоретико-множественного подхода;

– согласованностью полученных результатов с современными практиками в области оценки рисков информационной безопасности;

– проверкой адекватности, вычислительной реализуемости и применимости разработанных моделей и методик.

Достоверность представленных в диссертации научных результатов подтверждается:

– согласованностью результатов вычислительного эксперимента с теоретическими положениями;

– достаточным числом апробаций на научно-технических конференциях и публикаций в рецензируемых научных изданиях;

– положительными результатами внедрения основных научных положений диссертации в практику деятельности научных и производственных организаций.

V. Апробация и публикации

Результаты исследований автора прошли всестороннюю апробацию на 12 научных и практических конференциях, в том числе трех международных.

По тематике диссертации автором опубликовано 17 научных работ, в том числе пять статей в рецензируемых журналах из перечня ВАК («Вопросы оборонной техники. Серия 16», «Информатизация и связь», «Морской вестник», «Современные проблемы науки и образования» – 2 статьи).

VI. Оценка содержания и замечания по диссертационной работе

Диссертация структурирована по традиционному принципу и состоит из введения, четырех глав с описанием результатов исследования, заключения, списка сокращений и условных обозначений, списка литературы и приложений. Текст диссертации изложен на 186 страницах машинописного текста, сопровождается иллюстративными и сводными аналитическими материалами, включая 37 рисунков и 21 таблицу.

В конце каждой главы диссертации приведены выводы и рекомендации. В заключении представлены основные научные и практические результаты исследования.

Список литературы включает 180 источников, включая российские и международные стандарты, а также научные и методические труды в области информационной безопасности и теории рисков.

Основные результаты исследования, выводы и рекомендации представлены в автореферате, который достаточно полно отражает содержание диссертации.

К тексту диссертации и автореферата имеется ряд замечаний, основные из которых перечислены ниже.

1. В списке основных публикаций в автореферате изменены последовательности фамилий соавторов публикаций, оформление списка не вполне соответствует требованиям ГОСТ.

2. При построении предметной области оценки рисков безопасности ИС в нотации UML, представленной на рис.1 (стр.17), необходимо было опираться на существующие диаграммы из ГОСТ Р ИСО/МЭК 15408-1-2008. Так, в диаграмме отсутствует один из важных объектов «Владельцы», защитные меры в соответствии с ГОСТ, в первую очередь уменьшают риски, а не последствия.

3. Тема диссертации, первый и четвертый раздел диссертации сформулированы в терминах только первого этапа *менеджмента рисков безопасности* (в соответствии со стандартом ISO/IEC 27005:2011), а именно *оценки рисков*. В то же время цель исследования, научная задача, объект и предмет исследования, часть результатов исследования (например, методика формирования рационального комплекса защитных мер) посвящены второму этапу управления рисками – *обработке рисков*, а именно выбору защитных мер.

4. Схема процесса управления рисками на рис.2 (стр.22) искаженно представляет *этап оценки рисков* по стандарту ISO/IEC 27005:2011, который включает *анализ риска* (risk analysis), состоящий из *идентификации риска* (risk identification) и *расчета (количественной оценки) риска* (risk estimation), а также *оценивание риска* (risk evaluation).

5. Предложенное в диссертации на стр.34 понятие «деструктивное состояние» не совсем удачно, поскольку прилагательное «деструктивный», т.е. разрушительный, относится к действию, а состояние – это совокупность основных параметров и характеристик какого-либо объекта. Правильнее было бы говорить об опасных и катастрофических состояниях, а также о деструктивных траекториях состояний.

6. В соответствии с законом 149-ФЗ «Об информации, информационных технологиях и о защите информации» законодательные защитные меры не относятся к организационным (стр.45).

7. Непонятна концепция структурной диаграммы типов элементов КИС (рис.6, стр.49), в соответствии с которой информационные активы хранятся на технических средствах (ТС), а обрабатываются программным обеспечением (ПО) – в рассмотренных случаях информационные активы рассматриваются, скорее всего, как два разных уровня представления данных.

8. В классификации деструктивных состояний на стр.54 отсутствуют состояния с нарушениями целостности ТС и ПО, впрямую обозначенными в РД Гостехкомиссии «Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации». Кроме того, осуществление НСД к ТС и ПО у автора в соответствии с табл.5 связано исключительно с воздействием нарушителя, хотя нарушение целостности указанных элементов может произойти из-за воздействия естественных источников угроз.

9. Одно из заявленных положений, выносимых на защиту – методика количественной оценки вероятности реализации угроз на основе экспертно-нейросетевого определения метрик – формально не обозначено ни в автореферате, ни в третьей главе диссертации в виде отдельного подраздела или некоторого описания алгоритма, последовательности шагов. Остается только по косвенным признака догадываться, что конкретно имел в виду автор под третьим защищаемым положением.

VII. Заключение по диссертационной работе

В целом, диссертация Нурдинова Руслана Артуровича представляет собой завершенное научное исследование, выполненное на достаточно высоком научном уровне.

Результаты работы достаточно полно опубликованы в 17 работах, из них пять – в ведущих рецензируемых изданиях, рекомендованных ВАК. Автореферат и научные публикации полностью отражают содержание работы.

Автором в диссертации сформулирована и решена актуальная научная задача разработки методического аппарата, позволяющего осуществлять рациональный выбор защитных мер для корпоративных информационных систем за счет применения научно-обоснованной формализованной модели количественной оценки рисков. Представленные в диссертации модели и методики обладают научной новизной и представляют значимость для науки и практики.

Содержание диссертации соответствует пунктам 7 и 10 паспорта научной специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Учитывая актуальность выполненных исследований, научную новизну и практическую значимость полученных результатов, считаю, что представленная диссертационная работа полностью удовлетворяет требованиям п. 9 «По-

ложения о порядке присуждения ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24.09.2013 г. № 842, предъявляемым к диссертациям на соискание ученой степени кандидата наук, а ее автор – Нурдинов Руслан Артурович – заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент:
профессор кафедры информационно-вычислительных систем и сетей
федерального государственного бюджетного военного образовательного
учреждения высшего образования «Военно-космическая академия
имени А.Ф.Можайского» Министерства обороны Российской Федерации

к.т.н., доцент Владимир Анатольевич Гончаренко

«7» декабря 2016 года

Контактные данные:
197198, Россия, г. Санкт-Петербург, ул. Ждановская, д. 13
тел. 8-911-242-0119, e-mail: vlango@mail.ru

Подпись Гончаренко В.А. заверяю.

Начальник отдела кадро
Военно-космической [illegible] Можайского