

УТВЕРЖДАЮ

Проректор по ИР
Университета ИТМО
д.т.н., профессор

В. О. Никифоров

«29» *июль* 2016 г.

ЗАКЛЮЧЕНИЕ

Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики (Университета ИТМО) Министерства образования и науки Российской Федерации.

Диссертация «Модель количественной оценки рисков безопасности корпоративной информационной системы на основе метрик» выполнена соискателем Нурдиновым Русланом Артуровичем в Университете ИТМО на кафедре «Безопасные информационные технологии».

В 2013 г. Нурдинов Р.А. окончил Университет ИТМО по специальности «Организация и технология защиты информации», по диплому специалист по защите информации. В период подготовки диссертации Нурдинов Р.А. работал инженером-проектировщиком в ООО «Газинформсервис».

В настоящее время является аспирантом очной формы обучения на кафедре «Безопасные информационные технологии» Университета ИТМО.

Справка об обучении № 49/2016, выдана в 2016 г. ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».

Научный руководитель – Каторин Юрий Федорович, доктор военных наук, профессор, ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», кафедра «Безопасные информационные технологии», профессор.

По итогам рассмотрения принято следующее заключение:

1. Личное участие соискателя Нурдинова Р.А. заключается в самостоятельном исследовании проблемы количественной оценки рисков безопасности корпоративной информационной системы, в ходе которого проанализирован ряд отечественных и зарубежных источников, выявлены недостатки и ограничения существующих подходов к оценке рисков информационной безопасности. Соискателем предложена оригинальная модель оценки рисков безопасности корпоративной информационной системы на основе системы согласованных метрик. Также Нурдиновым Р.А. проведено экспериментальное исследование, в ходе которого осуществлялась аппроксимация

функции вероятности реализации угроз нарушителем на основе данных об инцидентах информационной безопасности.

2. Достоверность результатов, полученных в диссертационной работе, достигается использованием современного и апробированного математического аппарата, системно-структурным анализом описания объекта исследований, непротиворечивостью полученных выводов и их согласованностью с современными практиками в области информационной безопасности.

3. Научная новизна диссертационной работы заключается в следующем:

- разработана оригинальная формализованная модель количественной оценки рисков безопасности КИС, отличающаяся набором связанных переходов ее элементов в деструктивные состояния, рассматриваемых в качестве рисков событий;
- разработана методика, позволяющая повысить качество выбора защитных мер для корпоративной информационной системы, отличающаяся применением предложенного в работе показателя затратоемкости активов;
- для повышения точности прогнозирования вероятности реализации угроз нарушителем впервые применен специальный вариант алгоритма обратного распространения ошибки на основе диагонального метода Левенберга-Марквардта..

Практическую значимость диссертационной работы составляют предложенные модели и методики, которые позволяют повысить качество выбора защитных мер для корпоративной информационной системы и могут быть реализованы в виде модуля управления рисками безопасности корпоративной информационной системы. Результаты исследования внедрены в образовательных учреждениях и коммерческих предприятиях.

4. Ценность диссертационной работы Нурдинова Р.А. заключается в решении актуальной научной задачи, а именно в разработке методического аппарата, позволяющего осуществлять рациональный выбор защитных мер для корпоративных информационных систем за счет применения научно-обоснованной формализованной модели количественной оценки рисков.

5. Диссертационная работа Нурдинова Р.А. соответствует требованиям, установленным п.14 «Положения о присуждении ученых степеней». Приведены ссылки на цитируемые источники. Отмечена степень вклада соискателя в научные работы, выполненные в соавторстве.

6. Диссертационная работа Нурдинова Р.А. соответствует требованиям п. 9 Положения о присуждении ученой степени и п. 7, 10 Паспорта специальностей ВАК (технические науки) по специальности 05.13.19 Методы и системы защиты информации, информационная безопасность.

7. Материалы диссертационного исследования изложены в 17 работах, в том числе в 5 статьях, опубликованных в ведущих рецензируемых научных журналах и изданиях, рекомендованных ВАК:

- Нурдинов Р.А., Каторин Ю.Ф., Зайцева Н.М., Канев А.Н., Иоффе М.А. Количественная оценка вероятности реализации угроз нарушения безопасности АСУ технологическими процессами террористическими группировками // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. Т. 3-4 (93-94). С. 3-9. (0,5 п.л./ 0,4 п.л.).
- Нурдинов Р.А., Лившиц И.И. Обеспечение комплексной безопасности сложных промышленных объектов на базе риск-ориентированных стандартов // Информатизация и Связь. 2016. №1. С. 49-55. (0,5 п.л./ 0,2 п.л.).
- Нурдинов Р.А., Вихров Н.М., Нырков А.П., Каторин Ю.Ф., Шнуренко А.А., Башмаков А.В., Соколов С.С. Анализ информационных рисков // Морской вестник. 2015. № 3 (55). С.81-85. (0,5 п.л./ 0,2 п.л.).
- Нурдинов Р.А. Определение вероятности нарушения критических свойств информационного актива на основе CVSS метрик уязвимостей [Электронный ресурс] // Современные проблемы науки и образования. 2014. № 3. URL: <http://www.science-education.ru/117-13290> (дата обращения: 30.05.2014). (0,5 п.л.).
- Нурдинов Р.А., Батова Т.Н. Подходы и методы обоснования целесообразности выбора средств защиты информации [Электронный ресурс] // Современные проблемы науки и образования. 2013. № 2. URL: <http://www.science-education.ru/ru/article/view?id=9131> (дата обращения: 21.11.2015). (0,5 п.л./ 0,3 п.л.).

Публикации Нурдинова Р.А. посвящены проблемам оценки рисков информационной безопасности и выбора защитных мер для корпоративных информационных систем. В них раскрыты основные положения результатов, полученных в диссертационной работе Нурдинова Р.А., а именно:

- модель оценки рисков безопасности корпоративной информационной системы на основе определения деструктивных состояний ее элементов.
- методика формирования рационального комплекса защитных мер для корпоративной информационной системы на основе минимизации значения показателя затратоемкости активов.
- методика количественной оценки вероятности реализации угроз нарушителем на основе экспертно-нейросетевого определения показателей защищенности.

Диссертация «Модель количественной оценки рисков безопасности корпоративной информационной системы на основе метрик» Нурдинова Руслана Артуровича 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 кафедры «Безопасные информационные технологии».

Присутствовало на заседании 36 чел.

Результаты голосования: «за» - 36 чел., «против» - 0 чел., «воздержалось» - 0 чел., протокол №6 от «17» июня 2016 г.

Зикратов И.А., доктор технических наук,
профессор, заведующий кафедрой БИТ

Коваль Е.Н., заведующая лабораторией
кафедры БИТ

Зикратов Игорь Алексеевич

Место работы: ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

Должность: декан факультета информационной безопасности и компьютерных технологий

Телефон: +7 (931) 306-01-95

Адрес электронной почты: zikratov@cit.ifmo.ru

Коваль Елена Николаевна

Место работы: ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

Должность: заведующая лабораторией кафедры безопасных информационных технологий

Телефон: +7 (921) 309-62-04

Адрес электронной почты: lena@cit.ifmo.ru