МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный технологический институт (технический университет)» (СПбГТИ(ТУ))

Московский пр., д.26, г.Санкт-Петербург, 190013,
телеграф: Санкт-Петербург, Л-13, Технолог,
факс: ректор (812) 710-6285, общий отдел (812) 712-7791,
телефон: (812) 710-1356,
E-mail: office@technolog.edu.ru

_____ № _____

«УТВЕРЖДАЮ»

Ректор федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный технологический институт (технический университет)»
доктор тех ент

_____ чик

ОТЗЫВ

ведущей организации

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»

Актуальность темы диссертации

В последнее время всё большее внимание уделяется вопросу защиты информационных систем, отличающихся по назначению, масштабу, архитектуре и прочим характеристикам.

В диссертации Нурдинова Руслана Артуровича рассмотрена проблема выбора защитных мер для корпоративных информационных систем (КИС), под которыми понимаются открытые интегрированные системы, автоматизирующие бизнес-процессы всех уровней и направлений деятельности предприятия.

Одним из подходов к формированию системы защиты информации является риск-ориентированный подход, позволяющий экономически обосновать затраты на обеспечение информационной безопасности (ИБ).

Вместе с тем, существует ряд проблем, связанных с низкой точностью, необъективностью и трудоемкостью выполнения детализированной количественной оценки рисков безопасности КИС. Стоит отметить, что правила и процедуры оценки рисков сложно формализуются, поэтому оценка рисков чаще всего осуществляется с привлечением экспертов.

В диссертационной работе Нурдинова Р.А. проведен анализ существующих моделей и методик оценки рисков ИБ, результаты которого свидетельствуют о необходимости разработки формализованной модели количественной оценки рисков, учитывающей причинно-следственные связи между событиями риска и способной к обучению с применением интеллектуальных технологий, позволяющей, таким образом, избежать необходимости постоянного привлечения экспертов для оценки рисков безопасности КИС.

Таким образом, тема диссертационной работы Нурдинова Руслана Артуровича, посвященная разработке модели количественной оценки рисков безопасности корпоративной информационной системы на основе метрик, является актуальной научно-технической проблемой, решение которой имеет существенное значение для науки и практики.

Анализ содержания диссертационной работы

Текст диссертации состоит из введения, четырех глав, заключения, списка сокращений и условных обозначений, списка литературы и четырех приложений. Материал диссертационного исследования представлен на 186 страницах машинописного текста. Список литературы включает 180 наименований.

Во ***введении*** обоснована актуальность выбранной темы исследования; сформулированы цель, предмет и объект, научная задача и частные задачи исследования, а также положения, выносимые на защиту.

В ***первой главе*** проведен анализ предметной области оценки рисков безопасности информационных систем, определены основные объекты предметной области и связи между ними.

Выполнено сравнение существующих стандартов и методик в части реализации идентификации, анализа и сравнительной оценки рисков ИБ, в ходе которого было определено, что чаще всего оценка параметров риска осуществляется по некоторым

качественным шкалам экспертом или группой экспертов, что затрудняет формализацию процесса оценки рисков

Также упоминаются различные математические модели и методы оценки рисков ИБ, предложенные российскими и зарубежными авторами, основанные на применении нечеткой логики, линейного программирования, статистического анализа, байесовских сетей, нейронных сетей, логико-вероятностного моделирования, моделирования с использованием когнитивных карт и имитационного моделирования.

Определены основные недостатки и проблемы, характерные для экспертных методов оценки рисков, а также ограничения применения статистических методов оценки. Приведены основные способы решения выявленных проблем, которые послужили предпосылками для разработки формализованной модели количественной оценки рисков безопасности КИС.

Во ***второй главе*** приведены два основные научных результата диссертации: модель количественной оценки рисков безопасности КИС и методика формирования рационального комплекса защитных мер.

Приведены характерные особенности и отличительные признаки, присущие КИС, рассмотрены стадии жизненного цикла КИС. Проведён структурный анализ КИС, определены типы элементов и связи между ними. Также представлена классификация защитных мер для КИС, основанная на положениях нормативных документов ФСТЭК России.

Предложена научно-обоснованная модель количественной оценки рисков, представляющая собой взвешенный ориентированный граф и формируемая на основе двух частных моделей: инфраструктурной модели КИС и модели сценариев реализации угроз КИС.

Предложен подход к определению совокупности взвешенных метрик для оценки показателей степени опасности нарушителя и степени реализации защитных мер. Достаточно подробно описана процедура начальной оценки весовых коэффициентов метрик с использованием метода анализа иерархий.

Также в главе приводится характеристика разработанной методики формирования рационального комплекса защитных мер для КИС на основе разработанной модели оценки рисков. Выбор рационального комплекса защитных

мер из множества альтернативных вариантов предлагается осуществлять за счёт минимизации значения показателя затратоёмкости активов, предложенного в диссертации.

В ***третьей главе*** рассмотрен вопрос настройки весовых коэффициентов метрик с использованием методов обучения нейронной сети для повышения точности прогнозирования вероятности реализации угроз нарушителем.

В качестве объектов обучающей выборки рассматриваются структурированные сведения о произошедших и предотвращенных инцидентах ИБ. Представлено теоретическое и экспериментальное обоснование выбора специального варианта метода обратного распространения ошибки, позволяющего в несколько сократить требуемое число объектов обучающей выборки.

Приводятся результаты экспериментального исследования, в ходе которого определены наиболее подходящие значения параметров обучения, а также устойчивость выбранного метода к влиянию различных факторов, например, возможность обучения на объектах, данные о которых неполны.

В ***четвёртой главе*** представлены основные результаты использования предложенных в работе моделей и методик при решении практических задач.

Приведено описание архитектуры и функциональных возможностей разработанного на базе интеграционной платформы RSA Archer GRC модуля управления рисками ИБ, а также коннекторов к смежным системам.

Также представлены результаты применения методики формирования рационального комплекса защитных мер при проектировании системы защиты информации промышленного предприятия.

В ***заключении*** приведены основные научные результаты, полученные в ходе диссертационного исследования.

Список литературы включает в себя большое число отечественных и зарубежных стандартов, а также научных работ по данной тематике.

Новизна полученных результатов

Научную новизну диссертационной работы составляют разработанные оригинальные модели и методики. В частности, научную новизну составляют следующие положения.

Формализованная модель количественной оценки рисков безопасности КИС, отличающаяся набором связанных переходов ее элементов в деструктивные состояния, рассматриваемых в качестве событий риска, обеспечивает переоценку рисков при изменении исходных данных без повторного привлечения экспертов.

Методика формирования рационального комплекса защитных мер, отличающаяся применением предложенного в работе показателя затратоемкости активов, позволяет повысить качество выбора защитных мер.

Оригинальная методика количественной оценки вероятности реализации угроз на основе определения метрик нарушителя и защитных мер, отличающаяся использованием комбинации экспертных и нейросетевых методов, позволяет повысить точность прогнозирования вероятности событий риска. При этом для повышения точности прогнозирования вероятности реализации угроз нарушителем диссертантом впервые применен специальный вариант алгоритма обратного распространения ошибки на основе диагонального метода Левенберга-Марквардта, позволяющий значительно сократить требуемое число объектов обучающей выборки. Это преимущество является существенным, поскольку объем обучающей выборки, выраженный числом инцидентов ИБ, как правило, ограничен

Достоверность и обоснованность результатов исследования

Достоверность основных выводов и результатов диссертационной работы обеспечивается глубоким анализом предметной области и использованием современного и апробированного математического аппарата.

Корректность предложенных моделей и методик подтверждается совпадением полученных в ходе экспериментального исследования результатов теоретическим положениям, практической апробацией на научно-технических конференциях и публикациями в достаточном количестве рецензируемых научных изданий.

Практическая значимость результатов исследования

Практическая ценность результатов диссертационной работы состоит в том, что предложенные модели и методики успешно применяются при решении практических задач.

Предложенные в диссертационной работе модели и методики использованы при разработке модуля управления рисками ИБ в составе системы автоматизации процессов управления ИБ.

Использование методики формирования рационального комплекса защитных мер при проектировании и внедрении систем защиты информации позволяет определить наиболее подходящий комплекс защитных мер с учетом установленных технических, финансовых и нормативных и ограничений.

В диссертационной работе приводятся акты о внедрении результатов исследования в следующих организациях:

- ООО «Газинформсервис»;
- ООО «Газпром трансгаз Санкт-Петербург»;
- ЧОУ ДПО «Центр предпринимательских рисков»;
- кафедра безопасных информационных технологий Университета ИТМО.

Рекомендации по использованию результатов и выводов диссертации

Разработанные в ходе диссертационного исследования модели и методики могут найти практическое применение при решении широкого круга практических задач.

Предложенная формализованная модель оценки рисков безопасности КИС может быть использована при автоматизации процесса управления рисками ИБ. Разработанный на её основе программный модуль управления рисками позволяет осуществлять динамическую переоценку рисков без привлечения экспертов, тем самым, реагировать на различные изменения структуры КИС, конфигурации системы защиты, появление новых угроз и нарушителей.

Методика формирования рационального комплекса защитных мер может использоваться в составе системы поддержки принятия решений для создания и совершенствования систем защиты информации.

Предложенная методика количественной оценки вероятности реализации угроз нарушителем на основе экспертно-нейросетевого определения метрик может использоваться для:

- прогнозирования вероятности реализации угроз нарушителем на основе централизованной базы данных инцидентов ИБ;
- непрерывной актуализации перечня требований к защите различных видов информационных систем и определения степени важности требований.

Замечания по диссертационной работе

1. В первой главе недостаточное внимание уделено анализу научных трудов по схожей проблематике, выполненных российскими авторами, и существующих программных комплексов оценки рисков.
2. Содержание второй главы диссертационной работы перегружено. Следовало бы перенести в главу 3 подраздел 2.3, в котором рассмотрены вопросы определения метрик и начальной оценки их весовых коэффициентов.
3. На 128 странице диссертации встречается фраза «Предложенные в диссертационной работе модели и методы использованы при разработке модуля управления рисками». Вероятно, имелось в виду слово «методики», поскольку в числе научных результатов, полученных в ходе диссертационного исследования, отсутствуют какие-либо методы.
4. В приложении к диссертации следовало бы привести разработанный программный код, который использовался при проведении вычислительных экспериментов.

Перечисленные недостатки и замечания не снижают общей ценности полученных научных результатов и не влияют на общее положительное впечатление о качестве представленной к защите диссертации. Данные замечания носят рекомендательный характер и могут быть учтены автором при подготовке доклада, представляемого к защите.

Заключение

В целом диссертационная работа Нурдинова Руслана Артуровича представляет собой завершенную научно-исследовательскую работу, выполненную на актуальную тему, 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, который достаточно полно отражает содержание 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 СПбГТИ(ТУ), протокол № 3 от «28» октября 2016 г.

Профессор кафедры системного
анализа и информационных
технологий, д.т.н., профессор _____ А.В. Холоднов

Сведения о составителе отзыва

Холоднов Владислав Алексеевич, доктор технических наук, профессор, профессор кафедры системного анализа и информационных технологий.

Тел.: +7 (911) 180-58-14. E-mail: holodnow@yandex.ru.