ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

Беззатеева Сергея Валентиновича

на диссертацию 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 исследования

Актуальность темы диссертационной работы обусловлена необходимостью и сложностью создания и постоянного совершенствования систем защиты информации для корпоративных информационных систем (КИС) организаций, обладающих сложной информационно-технологической инфраструктурой.

Поскольку основное предназначение КИС заключается в повышении эффективности деятельности предприятия, формируемый комплекс защитных мер для КИС должен быть рациональным с точки зрения соотношения ценности информации и затрат на ее защиту.

Перспективным представляется риск-ориентированный подход к формированию систем защиты информации, в соответствии с которым для снижения неприемлемых рисков осуществляется выбор защитных мер, наилучшим образом соответствующих потребностям организации.

Отмечается, что только объективная количественная оценка рисков позволяет обосновать затраты на защиту информации. Вместе с тем, отмечается ряд проблем, связанных с субъективностью, неточностью и трудоемкостью получения результатов количественной оценки рисков безопасности КИС.

Таким образом, диссертационная работа Нурдинова Руслана Артуровича посвящена решению актуальной научной проблемы разработки методического аппарата, позволяющего повысить качество выбора защитных мер за счет применения научно-обоснованной формализованной модели количественной оценки рисков.

II. Обоснованность научных положений, выводов и рекомендаций

В диссертационной работе представлено три основных научных положения:

1. Модель оценки рисков безопасности корпоративной информационной системы на основе определения деструктивных состояний ее элементов обеспечивает переоценку рисков при изменении исходных данных без повторного привлечения экспертов.
2. Методика формирования рационального комплекса защитных мер для корпоративной информационной системы на основе минимизации значения показателя затратоемкости активов позволяет повысить качество выбора защитных мер.
3. Методика количественной оценки вероятности реализации угроз нарушителем на основе экспертно-нейросетевого определения метрик позволяет повысить точность прогнозирования вероятности событий риска.

Обоснованность научных положений, выводов и рекомендаций обеспечивается тщательным анализом предметной области, применением системного подхода к решению поставленных задач, корректным использованием выбранного математического аппарата, а также их согласованностью с современными практиками в области оценки рисков информационной безопасности.

III. Новизна и достоверность результатов исследования

Новизну диссертационной работы составляет предложенный в ней методический аппарат, позволяющий повысить качество выбора защитных мер за счет применения научно-обоснованной формализованной модели количественной оценки рисков. Новизна научных положений, предложенных в диссертационной работе, заключается, главным образом, в следующем:

- оригинальность модели количественной оценки рисков безопасности КИС состоит в том, что в качестве событий риска в ней

рассматриваются связанные переходы элементов КИС в деструктивные состояния, предложенные автором;

- в методике формирования рационального комплекса защитных мер задача выбора рационального комплекса формализована как экстремальная задача теории принятия решений, при этом используется показатель затратоемкости активов КИС, предложенный в работе;
- в методике количественной оценки вероятности реализации угроз нарушителем предложен новый подход к определению совокупности согласованных метрик нарушителя и защитных мер с использованием метода анализа иерархий и диагонального метода Левенберга-Марквардта для настройки значений весовых коэффициентов метрик.

Достоверность представленных моделей и методик подтверждается результатами вычислительных экспериментов, а также внедрением в практику работы научных и производственных организаций.

Основные результаты диссертационной работы прошли апробацию и были одобрены на 12 научных и практических конференциях, в том числе международных.

По результатам диссертационного исследования опубликовано 17 работ, в том числе пять статей в журналах, рекомендованных Высшей аттестационной комиссией.

IV. Значимость результатов исследования для науки и практики и рекомендации по их дальнейшему использованию

Значимость полученных в диссертационной работе результатов для науки заключается в разработке оригинальных методик и моделей оценки рисков информационной безопасности, позволяющих повысить качество выбора защитных мер для корпоративных информационных систем.

Значимость полученных результатов для практики заключается в том, что они обладают достаточной степенью универсальности и обеспечивают методические основы автоматизации процессов оценки рисков и выбора защитных мер для КИС.

Предложенные модели и методики внедрены в практику деятельности следующих научных и коммерческих организаций:

- ФГБОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»;
- ЧОУ ДПО «Центр предпринимательских рисков»;
- ООО «Газинформсервис»;
- ООО «Газпром трансгаз Санкт-Петербург».

Перспективной представляется адаптация предложенных моделей и методик для различных классов информационных и автоматизированных систем.

V. Оценка содержания диссертации

Диссертационная работа изложена на 186 страницах машинописного текста и состоит из введения, четырех глав, заключения, списка сокращений и условных обозначений, списка литературы и четырех приложений.

Первая глава посвящена сравнительному анализу существующих подходов к оценке рисков безопасности информационных систем, их преимуществ и недостатков. Во второй и третьей главах приводятся подробная характеристика полученных результатов. Четвертая глава посвящена практическому применению результатов исследования. Приведены выводы и рекомендации по каждой главе. Основные научные и практические результаты, полученные в диссертационной работе, приведены в заключении.

В целом, диссертационная работа хорошо структурирована и представляет собой законченное научное исследование.

VI. Замечания по диссертационной работе

1. Излишняя избыточность при описании классификаций элементов, активов и мероприятий, выраженная в приведении ее как в текстовой, так и в табличной форме.(стр. 25 и 27, стр. 29 и 30, стр. 31 и 33) Очевидна большая эффективность и наглядность табличной формы.
2. Предложена логистическая функция для оценки функции реализации угроз нарушителем. К сожалению, автором не проведено сравнение адекватности приведенной варианта оценки с известными ранее. Кроме того, на графике этой функции на стр. 61 не указан аргумент по оси абсцисс.
3. Для понимания существа приведенной на стр. 63 кусочно-линейной функции было бы очень желательно привести графическую иллюстрацию используемых интервалов для аргумента функции.
4. Не ясен смысл и цель рассуждений автора об экономической составляющей угроз, приведенных на стр.83, 84-86. Очевидно, что диссертация не посвящена экономике информационной безопасности и в целом такого анализа в работе не проводится.
5. К сожалению, автор диссертационной работы не всегда соблюдает единую терминологию. Так, например, функция реализации угроз нарушителем называется им в различных местах текста диссертационной работы как:
    - весовая функция перехода (стр. 60);
    - логистическая функция активации (стр.107).
6. Неудачно выбранная терминология также существенно затрудняет понимание формул и выводов. Так, например, на стр. 99 и далее автор рассматривает разницу между вероятностью и результатом инцидента.

Отмеченные замечания не снижают общей ценности диссертационной работы и не влияют на главные теоретические и практические результаты.

VII. Заключение

Диссертационная работа Нурдинова Руслана Артуровича представляет собой законченную научно-исследовательскую работу, выполненную на актуальную тему. Представленные в ней результаты достоверны, обладают научной новизной и практической значимостью.

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

Таким образом, диссертационная работа соответствует требованиям п. 9 «Положения 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 Нурдинов Руслан Артурович заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент