Экз. № 1

ОТЗЫВ

официального оппонента, доктора технических наук, доцента
Душкина Александра Викторовича
на диссертационную работу Левоневского Дмитрия Константиновича
на тему «Методы и модели защиты корпоративных информационных систем
от комплексных деструктивных воздействий», представленную на соискание ученой
степени кандидата технических наук по специальности
05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Актуальность темы диссертации

Актуальность темы настоящей диссертационной работы определяется широким распространением корпоративных информационных систем (КИС), высокими требованиями к их защите, широким и динамичным множеством угроз безопасности систем этого класса. От успешного функционирования корпоративных информационных систем во многом зависит эффективность многих современных предприятий и организаций.

Масштабные сетевые атаки на информационную инфраструктуру предприятий в настоящее время происходят часто, мощность атак имеет тенденцию к росту, а растущая зависимость процессов от информационных технологий приводит к тому, что сетевая атака может парализовать работу предприятия и нанести существенный ущерб как предприятию, так и, при определённых условиях, всей отрасли, государству. Для эффективного противодействия таким угрозам необходимо учитывать исследуемые в диссертационной работе свойства как самих угроз, так и объекта защиты. К этим свойствам относятся комплексность, изменчивость, распределённость и др.

С учётом изложенного, тема диссертации представляется актуальной в научном и практическом плане.

Обоснованность и достоверность полученных научных результатов

Обоснованность и достоверность полученных результатов подтверждается корректностью исходных предпосылок; использованием методов системного и математического анализа, положения теории вероятности и математической статистики, теории информационной безопасности; соответствием результатов моделирования общим закономерностям; апробацией основных результатов работы на российских и международных конференциях и в научной печати; регистрацией результатов работы в качестве объектов интеллектуальной собственности (3 программ для ЭВМ и 1 патента на изобретение); реализацией результатов работы в научных, образовательных учреждениях и коммерческих предприятиях.

Значимость результатов для науки и практики

Теоретическая значимость полученных результатов состоит в развитии научного аппарата оценивания эффективности и обоснования мероприятий защиты КИС от деструктивных информационных воздействий, а именно в разработке новой модели корпоративной информационной системы,

функционирующей в условиях комплексных деструктивных информационных воздействий, методов оценивания эффективности функционирования корпоративной информационной системы.

Практическая значимость результатов заключается в том, что предложенные решения позволяют количественно и качественно оценивать процессы, протекающие в защищаемых системах, функционирующих в условиях комплексных деструктивных воздействий. Они позволяют обосновывать целесообразные мероприятия в области управления данными при защите прикладных систем от комплексных информационных угроз. Данные решения могут быть использованы как для планирования и осуществления противодействия вредоносным воздействиям, так и для оперативного управления информационной безопасностью систем. В частности, разработанные модели и методы могут быть применены для высокоуровневой формализации процессов функционирования корпоративных информационных систем на производственных предприятиях, в социальных учреждениях, транспортных объектах, и т.д. Подобные модели и методы могут также успешно применяться в задачах планирования и выбора соответствующего программного обеспечения для противодействия угрозам в этих организациях.

Научная новизна исследования

В ходе проведения исследования автором получен ряд новых научных результатов, в частности:

1. Математическая модель корпоративной информационной системы, функционирующей в условиях комплексных деструктивных информационных воздействий, отличающаяся новым пространством состояний и множеством переходов между ними, что позволяет шире исследовать и точнее прогнозировать поведение системы при наличии этих угроз.
2. Метод оценивания эффективности функционирования корпоративной информационной системы с использованием предложенной математической модели, отличающийся новым показателем эффективности КИС и правилами его расчета, позволяющий расширить возможности оценивания влияния информационных угроз на работу систем.
3. Метод адаптивной защиты корпоративной информационной системы от информационных угроз, отличающийся новой математической формулировкой задачи поиска оптимальной программы защиты и алгоритмом ее решения, позволяющий адаптировать эту защиту от комплексных деструктивных воздействий.
4. Архитектура системы адаптивной защиты КИС от комплексных деструктивных информационных воздействий, которая отличается новой совокупностью связанных блоков сбора, предобработки и анализа данных и выбора контрмер для защиты от сетевых атак и иных деструктивных воздействий, позволяющая расширить функциональные возможности такой защиты.
5. Способы и средства, отличающиеся новыми последовательностями действий по обоснованию и реализации мероприятий защиты, позволяющие повысить эффективность корпоративных информационных систем.

Общая оценка диссертационной работы

В диссертационной работе Левоневского Д.К. решена научная задача разработки новых методов и моделей адаптивной защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий. Работа написана грамотным литературным языком. Диссертация состоит из введения, 4 глав, заключения, библиографического списка и 3 приложений.

Во введении обосновывается актуальность темы исследования и описывается степень разработанности проблемы, формулируется цель работы и содержание поставленных задач, обозначается научная новизна положений, выносимых на защиту, определяются теоретическая и практическая значимость полученных результатов, сообщается о степени достоверности и апробации результатов.

В первой главе автор анализирует процесс защиты КИС от комплексных деструктивных информационных воздействий, уточняет цели, задачи и возможности защиты, раскрывает особенности информационных угроз для данного класса систем, даёт анализ известных систем и методов их защиты, формулирует решаемую научную задачу разработки новых методов и моделей адаптивной защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий.

Во второй главе предлагается новый метод оценивания эффективности защиты КИС от деструктивных информационных воздействий. Для этого автор описывает формальную постановку задачи и обосновывает показатели эффективности защиты. Далее строится новая марковская модель защищаемой системы, предлагается алгоритм оценивания эффективности защиты по новому интегральному показателю с использованием построенной модели.

В третьей главе описывается разработка метода адаптивной защиты корпоративной информационной системы от комплексных деструктивных воздействий и предлагается модель системы адаптивной защиты.

В четвертой главе проводится экспериментальное исследование эффективности предложенных методов и моделей. Для этого было проведено математическое моделирование поведения корпоративной информационной системы на примере сервиса интерактивного корпоративного телевидения.

Каждая глава завершается краткими выводами о полученных результатах.

В заключении представляются полученные результаты, обозначаются перспективы их дальнейшего использования и сообщается о соответствии полученных результатов следующим пунктам паспорта специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»: «3. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса» (результаты 3-5), «6. Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования» (результаты 4-5), «7. Анализ рисков нарушения информационной безопасности и уязвимости процессов

переработки информации в информационных системах любого вида и области применения» (результат 1), «8. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем» (результат 1), «9. Модели и методы оценки защищенности информации и информационной безопасности объекта» (результаты 1–2), «10. Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты» (результат 2), «14. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности» (результат 2). Библиографический список содержит 101 наименование. В приложениях представлены свидетельства о государственной регистрации интеллектуальной собственности, акты реализации полученных результатов, список публикаций соискателя.

Основные этапы работы, выводы и результаты представлены в автореферате. Содержание автореферата соответствует основному содержанию диссертационной работы. По теме диссертации опубликовано 18 научных работ, из них 7 – в печатных изданиях, входящих в перечень ВАК. Основные результаты работы апробированы на различных международных и всероссийских научных конференциях.

Замечания по работе

Представленная диссертация имеет ряд недостатков, к числу которых следует отнести:

1. В главе 2 рассматривается классификация угроз, в том числе, по аспектам информационной безопасности (целостность, доступность, конфиденциальность), однако в экспериментальном исследовании рассматриваются только угрозы доступности.
2. В таблице 2 не определён ряд характеристик исследуемых систем обеспечения безопасности ИБ КИС.
3. В главе 2 две величины $E(t)$ и $V(t)$, имеющие разный физический смысл, называются эффектом функционирования системы, что может порождать путаницу.
4. Некоторые показатели, рассмотренные в таблице 4 (время загрузки и инициализации приложения, время актуализации данных в приложении), не учитываются при моделировании системы в главе 4.
5. На рис. 10 не используются формальные нотации (UML, DFD) для описания архитектуры системы адаптивной защиты, в результате чего не вполне ясно, как именно выполняется обработка данных в подобной системе.
6. Имеются неточности редакционного характера при оформлении диссертации и автореферата (например, список литературы и т.д.).

Однако, указанные недостатки не снижают значимости работы и носят преимущественно уточняющий и рекомендательный характер.

Заключение

Диссертация Левоневского Дмитрия Константиновича представляет собой завершённую научно-квалификационную работу, выполненную самостоятельно и

затрагивающую актуальную тему. Научные результаты, полученные диссертантом, являются новыми и имеют существенное значение для науки и практики. Рекомендации и выводы достаточно обоснованы.

Представленная диссертация удовлетворяет требованиям п. 9-14 Положения о присуждении учёных степеней, утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 года, предъявляемым к кандидатским диссертациям, а её автор Левоневский Д.К. достоин присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

ОФИЦИАЛЬНЫЙ ОППОНЕНТ:
профессор кафедры «Информационная безопасность»
федерального государственного автономного образовательного учреждения
высшего образования «Национальный исследовательский университет
«Московский институт электронной техники»
доктор технических наук, доцент,

Александр Викторович Душкин

Сведения о составителе отзыва:
ФИО: Душкин Александр Викторович.
Учёная степень: доктор технических наук.
Учёное звание: доцент.
Место работы: федеральное государственное автономное образовательное учреждение высшего образования «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МОСКОВСКИЙ ИНСТИТУТ ЭЛЕКТРОННОЙ ТЕХНИКИ».
Должность: профессор, кафедра «Информационная безопасность».
Почтовый адрес: 124498, Россия, г. Москва, г. Зеленоград, площадь Шокина, дом 1.
Телефон рабочий: +7 (499) 740-92-13
Электронная почта: a_dushkin@mail.ru

Подпись Душкина А.В. заверяю.
Начальник отдела кадров НИУ МИЭТ С.В. Заболотный

11.03.2020 г.