О Т З Ы В

официального оппонента на диссертационную работу Левоневского Дмитрия Константиновича “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. Корпоративные информационные системы (КИС) в настоящее время являются необходимой составляющей деятельности любой организационно-экономической системы. Нарушение безопасности передачи, хранения и обработки информации приводит к ущербу, степень и масштабы которого определяются целевым назначением этой информации и могут привести к непоправим последствиям в деятельности организации и ее окружении. В направлении обеспечения безопасности КИС ведутся многочисленные исследования и разработки. Действует международный стандарт ISO 15408 “Общие критерии оценки безопасности информационных технологий”.

Для нейтрализации угроз применяется типовой комплекс контрмер, остающийся неизменным на протяжении длительного времени. Подобный подход приемлем, если ценность защищаемых ресурсов в данной организации не слишком высока и имеются значительный запас вычислительных мощностей. В целом анализ текущего состояния защиты КИС от этих угроз показывает, что возможности существующих систем и методов защиты во многом не удовлетворяют требованиям практики. Одним из недостатков выступает слабая приспособленность к изменениям условий функционирования и видов угроз.

Диссертационная работа посвящена разработке моделей оценки эффективности инструментов защиты корпоративных информационных систем и адаптивным методам управления защитой от комплексных деструктивных информационных воздействий (КДВ). Центральное место в исследовании занимают задачи выбора программ обнаружения и программ мероприятий защиты от комплексных деструктивных воздействий (КДВ), при которых достигается максимум эффективности защиты при ограничении на используемые вычислительные ресурсы.

Это дает основание утверждать, что научная проблема, сформулированная в диссертации, является важной и актуальной, положительно влияющей в итоге на безопасность функционирования корпоративных информационных систем в различных областях деятельности.

Степень обоснованности научных положений, выводов и рекомендаций. Диссертантом изучены и критически анализируются известные достижения

и теоретические положения, существующие в области управления защитой от комплексных деструктивных информационных воздействий. Список использованной литературы содержит 101 наименование. Автор достаточно корректно использует известные научные методы обоснования полученных результатов, выводов и рекомендаций. Результаты и выводы диссертанта обоснованы и достоверны, они опираются на существующую теоретико-методологическую и нормативную базу.

Оценка новизны и достоверности. Достоинством диссертационной работы является полнота проведенного исследования, охватывающего большинство проблем управления защитой КИС от комплексных деструктивных информационных воздействий.

Автор предлагает оригинальную модель состояний средств защиты КИС, использующую марковские цепи для оценки вероятностно-временных характеристик пары «класс деструктивного информационного воздействия» - «программа мероприятий по защите КИС». Особенностью предложенной модели является возможность учесть состояния потока информационных угроз, состояния средств обнаружения, состояния средств информирования об угрозах и состояния программы устранения угроз. Рассмотрена возможность как агрегировать состояния, так и детализировать отдельные состояния для целей более точной оценки характеристик системы защиты.

В работе предложен оригинальный алгоритм расчета показателя эффективности защиты корпоративных информационных систем от комплексных деструктивных воздействий, основанный на предложенной автором марковской модели анализируемого процесса. Алгоритм позволяет учесть эффекты защиты в каждом из состояний системы защиты с учетом времени пребывания в каждом из состояний.

Для управления средствами защиты в работе предложен оригинальный алгоритм адаптивной защиты корпоративной информационной системы от комплексных деструктивных воздействий, позволяющий обеспечить конфигурирование системы защиты на двух уровнях:

1) путем выбора состава программ защиты на основе оценки показателя их эффективности;
2) путем оперативной настройки параметров средств обнаружения и защиты и управления их активностью в процессе функционирования КИС, обеспечивающий оптимизацию по предложенному показателю эффективности защиты.

Для обнаружения комплексных деструктивных воздействий в работе предложен оригинальный способ обнаружения атак на компьютерные системы. Особенность способа состоит в выбранном наборе параметров,

предложенном наборе правил определения наличия компьютерной атаки и методике расчета и параметрической настройки этих правил.

Проведенные автором исследования позволили реализовать комплексный подход к формированию механизмов управления защитой КИС от деструктивных информационных воздействий.

Основные положения диссертации нашли отражение в публикациях автора, а также были доложены на научно-практических конференциях.

Результаты работы использованы при разработке с участием автора программных продуктов, на которые получено три свидетельства о государственной регистрации программ для ЭВМ. Также диссертант является одним из авторов полученного патента на способ обнаружения компьютерных атак на сетевую компьютерную систему.

Замечания по диссертационной работе в целом.

1. В исследовании вопрос оперативного перераспределения вычислительных ресурсов между сервисами КИС и средствами защиты отражен не достаточно полно.
2. Не нашел отражение вопрос анализа чувствительности оценок эффективности защиты к изменениям параметров предложенной модели состояний системы защиты.
3. Нуждается в дальнейшей проработке вопрос асинхронного взаимодействия активных компонентов системы защиты. Принятая модель несовместных состояний несколько сужает область применения и становится слишком сложной при учете большого числа объектов классов деструктивных воздействий, средств обнаружения и сервисов КИС.
4. Диссертация была бы более полной при рассмотрении вопросов учета особенностей служб бизнес-процессов КИС. Для большинства сервисов КИС наиболее адекватной является замкнутая модель массового обслуживания с конечным числом источников.
5. Представленные на рис. 30, 31 диаграммы классов компонентов реализации без атрибутов, операций и пояснений практически не несут полезной информации.
6. Описание построенной автором имитационной модели (п. 4.2) не содержит достаточных пояснений по ограничениям и правилам функционирования блоков F – фильтр, Q – контроллер очереди и P – обработчик запросов. Границы применения модели не приведены. Не ясно, насколько выбор конкретной модели сервиса влияет на общие выводы по результатам моделирования.

7. Предложения по составу, структуре, математическому и программному обеспечению системы адаптивной защиты КИС (п. 4.3) представлены после описания имитационной модели и результатов моделирования. Автор не показал, какие оценки эффективности получены путем расчетов с использованием аналитических моделей, а какие по результатам моделирования.

Отмеченные недостатки несколько снижают качество исследования, но они не влияют на главные теоретические и практические результаты диссертации.

Заключение. Диссертация является законченным научно-исследовательским трудом на актуальную тему. выполненным автором самостоятельно на высоком научном уровне.

В работе приведены научные результаты, позволяющие квалифицировать ее как разработку научно обоснованных моделей, способов и технических решений, внедрение которых вносит значительный вклад в решение важнейших задач управления защитой корпоративных информационных систем.

Новые научные результаты, полученные диссертантом, имеют существенное значение для науки и практики в области управления безопасностью КИС. Работа базируется на достаточном числе исходных данных, примеров и расчетов. Она написана доходчиво, грамотно и аккуратно оформлена. В заключении каждой главы сделаны четкие выводы. Выводы и рекомендации обоснованы.

Автореферат соответствует основному содержанию диссертации.

Диссертационная работа отвечает требованиям ВАК, предъявляемым к кандидатским диссертациям, а ее автор, Левоневский Дмитрий Константинович, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент

Доцент СПбГЭТУ, кандидат
технических наук /В.А. Дубенецкий/

05.03.2020г.

Подпись официального оппонента
заверяю

Сведения о составителе отзыва:

ФИО: Дубенецкий Владислав Алексеевич
Учёная степень: кандидат технических наук
Учёное звание: доцент
Место работы: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)».
Должность: доцент кафедры информационных систем.
Почтовый адрес: 197022, Россия, Санкт-Петербург, ул. Профессора Попова, д. 5.
Телефон: +7 812 346-44-87.
Эл. почта: dubvl@list.ru