ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Юридический адрес: набережная реки Мойки,
д. 61, Санкт-Петербург, 191186

Почтовый адрес: пр. Большевиков, д. 22, корп. 1,
Санкт-Петербург, 193232
Тел.(812) 3263156, Факс: (812) 3263159
E-mail: rector@sut.ru
ИНН 7808004760 КПП 784001001
ОГРН 1027809197635 ОКТМО 40909000

11.03.2020 № 505/54
на №_____ от_____

УТВЕРЖДАЮ
Проректор по научной работе
д-р техн. наук, с.н.с.

Шестаков
Александр Викторович

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

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 диссертационной работы

Развитие инфокоммуникационной системы достигло того уровня, когда корпоративные информационные системы (КИС) стали неотъемлемой частью, практически, любого предприятия или организации. Они имеют различные масштабы, цели и задачи. Их общей чертой и тенденцией развития является то, что все большая часть деятельности соответствующих предприятий и организаций становится в высшей степени, зависимой от функционирования КИС. В связи с этим предпринимаются меры по обеспечению их надежности и устойчивости функционирования. Фактически, устойчивость функционирования КИС значительно отражается на устойчивости функционирования соответствующей

организации, а в условиях множественной разветвленной кооперации и на функционировании целых отраслей экономики.

Актуальность работы соискателя определяется ее целью, которая состоит в повышении эффективности защиты КИС от комплексных деструктивных информационных воздействий, а также решаемыми в работе задачами, обеспечивающими ее достижение.

Новизна представленных в диссертационной работе результатов

Новизна полученных автором результатов определяется в развитии научного аппарата оценивания эффективности методов защиты КИС от деструктивных информационных воздействий.

Новыми научными результатами являются:

1. Разработана новая 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. Разработан 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. Разработан 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. Предложена 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. Разработаны новые запатентованные способы и средства, отличающиеся новыми последовательностями действий по обоснованию и реализации мероприятий защиты, позволяющие повысить эффективность корпоративных информационных систем.

Степень обоснованности и достоверности научных положений, выводов и результатов, полученных в диссертационной работе

Обеспечивается корректностью исходных предпосылок, соответствием результатов моделирования общим закономерностям, апробацией основных результатов работы на конференциях и в научной печати, реализацией результатов работы.

Оценка представленных диссертационной работе результатов

1. В работе автор приводит результаты анализа процесса обеспечения информационной безопасности корпоративных интеллектуальных систем от информационных угроз, и результаты разработки на его основе математических моделей корпоративной информационной системы, рассматриваемой как объект защиты в условиях информационных угроз.

2. Приведены результаты разработки метода оценивания эффективности функционирования корпоративной информационной системы в условиях воздействия информационных угроз.

3. Выполнена разработка метода адаптивной защиты корпоративной информационной системы от информационных угроз.

4. Выполнена разработка архитектуры программной системы адаптивной защиты корпоративной информационной системы от информационных угроз.

5. Выполнена разработка рекомендаций по повышению эффективности защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий.

Значимость полученных результатов для развития науки состоит в развитии научного аппарата, позволяющего оценить эффективность и обоснованность принимаемых мер по защите КИС от деструктивных информационных воздействий.

Это развитие обеспечивают разработанные автором:

1. метод оценивания эффективности защиты КИС от комплексных деструктивных воздействий, основанный на новой марковской модели анализируемого процесса и алгоритме расчета нового показателя такой эффективности;

2. метод адаптивной защиты КИС от комплексных деструктивных воздействий, ориентированный на новую архитектуру системы такой защиты с оптимизацией ее конфигурации;

3. способы и средства защиты КИС от комплексных деструктивных информационных воздействий, повышающие ее эффективность.

Полученные автором результаты могут быть использованы как для исследовательских задач, так и для задач проектирования и эксплуатации КИС.

Рекомендации по использованию результатов, полученных в диссертационной работе

1. Разработанный автором метод оценивания эффективности защиты КИС от комплексных деструктивных воздействий, основанный на новой марковской модели анализируемого процесса и алгоритме расчета нового показателя позволяет производит сравнительную оценку и выбор различных мер, направленных на обеспечение защиты.

Данный метод рекомендуется для применения как в исследовательских задачах, при разработке новых средств защиты, так и при выборе стандартных решений для конкретных КИС, при решении задач управления их защищенностью, в таких организациях как АО "НИИ "РУБИН" и ООО "Код Безопасности"

2. Разработанный автором метод адаптивной защиты КИС от комплексных деструктивных воздействий, ориентированный на новую архитектуру системы такой защиты с оптимизацией ее конфигурации позволяет повысить защищенность КИС. Причем эффективность данного метода обеспечивается, оптимизацией конфигурации системы защиты путем автоматической адаптации под конкретные условия.

Достоинства данного метода позволяют найти ему применение при разработке новых и модернизации существующих систем защиты КИС в производственных предприятиях, в учебных заведениях (ИТМО, СПбГЭТУ "ЛЭТИ") и учреждениях науки.

3. Разработанные автором способы и средства защиты КИС от комплексных деструктивных информационных воздействий позволяют повысить эффективность системы защиты и КИС в целом.

Приведенные в работе способы защиты могут быть использованы в КИС различного назначения, в зависимости от требований к степени защищенности. Это дает возможность выбрать именно те способы и средства защиты, которые обеспечат необходимый уровень безопасности при наибольшей эффективности использования ресурсов.

Разработанные автором способы и средства защиты рекомендуются к реализации в виде типовых программно-аппаратных решений для КИС различного назначения.

Результаты диссертационной работы Левоневского Дмитрия Константиновича также рекомендуется использовать в учебном процессе при подготовке бакалавров, магистров и аспирантов в области систем защиты информации в вузах.

Работа выполнена достаточно грамотно, материал изложен последовательно и логично, однако в ходе ознакомления с диссертацией был сделан ряд замечаний, которые приведены ниже.

Замечания

1. В ряде случаев автор оперирует понятиями, значение которых не очевидно и не поясняется в тексте работы, например, (страница 18), «… множество распределенных каналов доступа» – не ясно что имеется ввиду. В ряде случаев имеют место неудачные формулировки, например, «… система интегрирована в её окружение …» – непонятно как же тогда выделить систему и ее окружение.

На странице 49 приводится утверждение «При наличии возможности распознавания актуального состояния системы и известных …, появление угроз может быть предсказано», однако, не дается пояснений каким образом, какой возможно использовать метод прогнозирования и какова достоверность такого прогноза.

На странице 52, вероятно, было бы целесообразно вместо фразы «Эти особенности включают в себя следующие шаги:» написать «Алгоритм включает в себя следующие шаги:»

2. Не вполне удачное распределение материала по подразделам, в частности, в подразделе 2.1 «Формальная постановка задачи» содержимое страниц 37, 38 частично повторяется на страницах 67, 68 подраздела 3.3. «Метод оптимизации конфигурации системы защиты». Было бы целесообразно привести необходимые ссылки на формулы другого подраздела.

3. В подразделе 2.5 «Алгоритм оценивания эффективности защиты корпоративных» на странице 52 вводится понятие «…величина эффекта V_z, связанная с показателями качества обслуживания, доставляемого пользователю в единицу времени.», на странице 53 говорится «Для оценки эффекта $V_z(t)$ эти показатели необходимо свернуть в единый показатель.», далее для этой цели приводится ряд выкладок, однако конечного выражения для $V_z(t)$ так и не приведено.

4. В решении задачи оптимизации в подразделе 3.3 используется поиск полным перебором, но упоминается возможность применения метода ветвей и границ и других методов. Автор не приводит оценок сложности решения задачи

оптимизации. Имело бы смысл подробнее рассмотреть данную возможность и оценить эффективность ряда методов в данном случае.

5. В подразделе 4.4 приводится перечень параметров, вычисляемых в целях обнаружения атак (отношение объема входящего трафика к исходящему, количества пакетов UDP к количеству пакетов TCP и др.), однако не приводится метода выбора временного интервала, на котором производится подсчет этих показателей в зависимости от свойств трафика, которые могут быть различны для различных услуг. Вероятно, что оперативность реагирования на угрозу и точность ее диагностирования имеют противоположные зависимости от величины этого интервала. Поэтому, его величина представляет интерес и существенно влияет на эффективность системы в целом.

6. На странице 108 утверждается, что для получения результатов годится метод скользящего среднего, однако это утверждение никак не доказано, отсутствуют сравнения с другими методами.

7. Имеют место недочеты редактирования и оформления. В работе имеют место отдельные опечатки, неудачные фразеологические обороты и неоднозначности. На графиках, рисунки 19–28, 34–36 не подписаны единицы измерения, на ряде графиков отсутствую наименования осей. В тексте встречается различный шрифт (страница 38). При описании алгоритма решения задачи поиска оптимальной программы, приведенном на страницах 68, 69 следовало бы обозначить конечный шаг (например, как «Останов» или иным образом).

Приведенные замечания не снижают общей положительной оценки работы.

Выводы

Диссертационная работа Левоневского Дмитрия Константиновича «Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий» является законченной научно-квалификационной работой, в которой решена научная задача моделирования и разработки моделей и методов защиты корпоративных информационных систем от комплексных

деструктивных воздействий. Автореферат адекватно отражает основное содержание диссертационной работы.

Диссертационная работа Левоневского Дмитрия Константиновича «Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий» соответствует пунктам 9, 10, 13 паспорта специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность и отвечает всем критериям пп. 9–14 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842, а её автор – Левоневский Дмитрий Константинович – заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Диссертация и автореферат заслушаны и обсуждены на заседании кафедры сетей связи и передачи данных 7 февраля 2020 г., протокол № 9.

Отзыв подготовили:

Профессор кафедры сетей связи и передачи данных,
доктор технических наук

Парамонов Александр Иванович

Доцент кафедры сетей связи и передачи данных,
кандидат технических наук

Маколкина Мария Александровна