



АКЦИОНЕРНОЕ ОБЩЕСТВО

“НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
“РУБИН”

194100, Санкт-Петербург, ул. Кантемировская, д. 5, тел. (812) 670-89-89, факс: (812) 596-35-81, e-mail: inforubin@rubin-spb.ru
ИНН/КПП 7802776390/780201001, ОГРН 1127847043720, ОКПО 07542394

УТВЕРЖДАЮ

Заместитель генерального директора, к.т.н.

В. Б. Чуйков

 «03» марта 2020 г.

С

на автореферат диссертационной работы левоневского Дмитрия Константиновича на тему: «Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

АКТУАЛЬНОСТЬ ТЕМЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

На современном этапе развития информационных технологий широкое распространение получили корпоративные информационные системы (КИС). От их успешного функционирования во многом зависит эффективность многих современных предприятий и организаций. Это масштабируемые системы, предназначенные для комплексной автоматизации всех видов деятельности компаний, требующих единого управления. Такие системы часто основаны на углубленном анализе данных, широком использовании систем информационной поддержки принятия решений, электронном документообороте. КИС организуются на основе компьютерных сетей и подвержены деструктивным информационным воздействиям, в том числе сетевым атакам, которые постоянно совершенствуются.

Не являются редкостью масштабные сетевые атаки на облачную информационную инфраструктуру предприятий и государств. Несанкционированный доступ злоумышленника к облачным хранилищам позволяет ему получить не только данные о пользователях (включая такую информацию, как реквизиты платёжных карт, пароли от аккаунтов, копии удостоверений личности), но и данные, составляющие коммерческую тайну.

Несмотря на предпринимаемые попытки защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий,

они не имеют тенденций к снижению. К причинам этого относится появление новых видов угроз, невысокая адаптивность методов и систем защиты к изменяющимся условиям функционирования корпоративных информационных систем.

Таким образом, диссертационная работа посвященная повышению эффективности защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий, представляется актуальной.

НАУЧНАЯ НОВИЗНА, ТЕОРЕТИЧЕСКАЯ И ПРАКТИЧЕСКАЯ ЦЕННОСТЬ

Исходя из содержания автореферата, диссертационная работа имеет новые научные результаты (положения), выносимые на защиту.

Научная новизна первого результата заключается в том, что автор разработал метод оценивания эффективности защиты корпоративных информационных систем от комплексных деструктивных воздействий, основанный на новой Марковской модели анализируемого процесса, отличающийся новым пространством состояний и множеством переходов между ними, что позволяет шире исследовать и точнее прогнозировать поведение системы при наличии угроз и алгоритме расчета нового показателя эффективности.

Научная новизна второго результата заключается в том, что разработанный метод адаптивной защиты корпоративной информационной системы от информационных угроз, отличающийся новой математической формулировкой задачи поиска оптимальной программы защиты и алгоритмом ее решения, позволяющий адаптировать защиту к комплексным деструктивным воздействиям.

Научная новизна третьего результата заключается в разработке научно обоснованных способов и средств защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий, отличающиеся новыми последовательностями действий по обоснованию и реализации мероприятий защиты, позволяющие повысить эффективность корпоративных информационных систем.

Теоретическая значимость полученных результатов состоит в развитии научного аппарата оценивания эффективности и обоснования мероприятий защиты КИС от деструктивных информационных воздействий.

Практическая значимость результатов диссертационной работы заключается в усовершенствовании системы информационной защиты КИС и повышении их эффективности.

ДОСТОВЕРНОСТЬ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

Автореферат корректно и достаточно полно описывает основные результаты диссертационной работы. В качестве методической и теоретической основы в данном диссертационном исследовании использовались методы системного и математического анализа, положения теории вероятности и математической статистики, теории информационной безопасности.

Полученные автором в диссертации результаты основываются на непротиворечивом использовании апробированного математического аппарата.

Достоверность полученных результатов обеспечивается корректностью исходных предпосылок, соответствием результатов моделирования общим закономерностям, апробацией основных результатов работы на конференциях и в научной печати, реализацией результатов работы в различных проектах.

Список трудов по теме диссертации, представленный в автореферате, позволяет сделать вывод о том, что научные результаты, выносимые на защиту, в достаточной мере апробированы на научно-практических конференциях различного уровня.

Полученные в работе результаты прошли апробацию на 9 научных и практических конференциях. По результатам исследования опубликовано 18 печатных работ, в том числе 6 статей в рецензируемых научных изданиях, включенных в перечень ВАК.

Автор показал научную квалификацию, умение самостоятельно вести научные исследования с доведением их до конструктивных практических результатов. Предложенные методы и научно обоснованные решения по адаптивной защите корпоративных информационных систем от деструктивных и информационных угроз запатентованы, а алгоритмы – программно реализованы (1 патент на изобретение, 3 зарегистрированных программы для ЭВМ).

НЕДОСТАТКИ

Вместе с тем необходимо отметить следующие недостатки:

1. Из содержания автореферата не совсем понятно какой именно показатель эффективности защиты КИС предлагает автор.

2. В автореферате указывается использование модуля анализа эффектов системы защиты, однако не определено какие именно эффекты анализируются.

3. Предложенный автором метод адаптивной защиты КИС от деструктивных информационных воздействий ограничивается поиском оптимальной конфигурации системы защиты и недостаточно учитывает возможные изменения их реализаций.

4. В качестве апробации полученных результатов диссертации автор использует систему сервиса интерактивного корпоративного телевиденья, которая не в полной мере отражает все особенности функционирования современных КИС.

Однако отмеченные недостатки имеют частный характер, принципиально не влияя на полученные в диссертационной работе научные результаты.

ВЫВОДЫ

Содержание автореферата свидетельствует, что диссертационная работа Левоневского Дмитрия Константиновича на тему: «Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий» представляет собой законченную научно-квалификационную работу на актуальную тему, которая заслуживает **положительного отзыва** и позволяет констатировать получение нового решения актуальной научной задачи, имеющей значение для развития технической отрасли знаний. Представленные в

ней результаты достоверны и обладают научной новизной, теоретической и практической значимостью.

Диссертация полностью удовлетворяет критериям, представленным в п.п. 9, 10, 11 и 14 «Положения о присуждении ученых степеней, предъявляемым к кандидатским диссертациям» (утвержденного постановлением Правительства РФ от 24.09.2013г. № 842), а ее автор Левоневского Дмитрия Константиновича, заслуживает присуждения ученой степени кандидата технических наук.

Отзыв составил

Старший научный сотрудник
доктор технических наук
доцент

В. В. Бухарин

«12» марта 2020 г.

Отзыв обсужден и одобрен на заседании научно-исследовательского отдела АО «НИИ «Рубин», протокол №3 от «10» марта 2020 года.

С отзывом на автореферат СОГЛАСЕН

Начальник научно-исследовательского отдела
кандидат технических наук

К. А. Смирнов

«12» марта 2020 г.

Сведения о составителе отзыва:

Бухарин Владимир Владимирович
доктор технических наук, доцент
старший научный сотрудник научно-исследовательского отдела
АО «НИИ «Рубин»
194100, Санкт-Петербург, ул. Кантемировская, д. 5,
тел. (812) 670-89-89, e-mail: inforubin@rubin-spb.ru