

Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК [004.056]:336.71

Паршукова
Регина Викторовна

Разработка системы комплексной безопасности кредитно-финансового учреждения

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01 «Методы и системы защиты информации,
информационная безопасность»

Научный руководитель
Прудник Александр Михайлович
кандидат технических наук, доцент

Минск 2016

ВВЕДЕНИЕ

Вопросы безопасности информации – важная часть процесса внедрения новых информационных технологий во все сферы жизни общества. Широкомасштабное использование вычислительной техники и телекоммуникационных систем в информационных системах, переход к электронной технологии, увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы предприятия, к их высокой уязвимости.

В последние годы в банковской деятельности обострилась проблема обеспечения безопасности данных. Ценность банковской информации предъявляет особые требования к защите данных от несанкционированного доступа, в том числе к контролю управления процессами, изменяющими состояние данных. Обеспечение безопасности информационных банковских систем представляет собой комплексную проблему, которая решается в направлениях совершенствования применения информационных технологий, совершенствования методов и средств их разработки, развития системы сертификации, обеспечения соответствующих организационно-технических условий эксплуатации. Ключевым аспектом решения проблемы безопасности является выработка системы требований, критериев и показателей для оценки уровня безопасности информационных технологий.

Высокая значимость проблемы обеспечения безопасности кредитно-финансового учреждения и недостаточный уровень её теоретической разработки, прежде всего, с точки зрения комплексного подхода обусловили выбор темы диссертационного исследования и его актуальность. В кредитно-финансовых учреждениях требования к системе безопасности предъявляются более серьезные, чем в большей части других организаций.

Актуальность темы диссертации определяется постоянным уровнем проблем связанных с информационной безопасностью. Возрастающая роль информационных технологий и возрастающая сложность информационных процессов и сетей связи требуют целостного взгляда на обеспечение информационной безопасности.

В диссертации соискателя представлены методики разработки комплексной системы безопасности кредитно-финансового учреждения. Комплексная система позволяет уменьшить риски денежной потери, потери производительности и репутационные потери.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Цель работы состоит в разработке методических основ комплексной системы обеспечения защиты информации кредитно-финансового учреждения, в том числе внедрение системы менеджмента информационной безопасности (СМИБ), методических рекомендаций по реализации основных мер по защите информации, разработки политики информационной безопасности. Важнейшая роль в создании комплексной системы безопасности отводится работе по выявлению, анализу и прогнозированию потенциальных угроз кредитной организации, учёту объективных существующих внешних и внутренних условий, влияющих на состояние безопасности.

В соответствии с поставленной целью, в работе сформулированы и решены следующие основные задачи:

- проведен анализ современного состояния систем информационной безопасности кредитно-финансовых учреждений;
- рассмотрены объекты и элементы защиты в кредитно-финансовом учреждении;
- определены подходы и методы оценки рисков информационной системе кредитно-финансового учреждения;
- разработана основные аспекты создания комплексной системы информационной;
- разработана политика информационной безопасности;
- предложена и теоретически обоснована концепция комплексной защиты информации и механизм ее реализации на примере кредитно-финансового учреждения;
- проведена оценка рисков;
- определены основные направления организации работы по защите информации в кредитно-финансовом учреждении.

Связь с приоритетными направлениями научных исследований и запросами реального сектора экономики

Тема диссертационной работы соответствует:

- п. 13. «Безопасность человека, общества и государства» Приоритетных направлений научных исследований Республики Беларусь на 2016–2020 годы утвержденных Постановлением Совета Министров Республики Беларусь № 190 от 12 марта 2015 г.

В диссертации поставлена и решена актуальная задача по разработке и обоснованию методологических положений, реализации практических

рекомендаций по защите информации на примере кредитно-финансового учреждения и выбору оптимальных средств защиты. Научную новизну содержит концепция комплексной системы защиты банковской информации, методика моделирования оптимальных средств защиты информации. Кроме того, новизну содержит предложенный системный подход к организации работ по защите информации в учреждении.

Теоретическая значимость диссертации заключается в том, что в ней предложен подход к построению эффективной комплексной системы обеспечения защиты информации.

Практическая ценность работы состоит в том, что сформулированные понятия, а также сделанные выводы и рекомендации могут быть непосредственно использованы кредитно-финансовыми учреждениями для формирования комплексной системы обеспечения информационной безопасности.

Положения, выносимые на защиту:

- основы построения системы защиты информации;
- этапы разработки системы менеджмента информационной безопасности;
- меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов;
- разработанные политики безопасности кредитно-финансового учреждения.

Личный вклад соискателя ученой степени

В совместно опубликованных работах соискателю принадлежат определение целей и постановка задач исследования, выбор методов разработки, участие в анализе современных методов и средств обеспечения комплексной безопасности объектов, а также обработке, анализе и интерпретации полученных результатов, формулировке выводов.

Основным соавтором опубликованных работ является научный руководитель, кандидат технических наук, доцент А.М. Прудник.

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты исследований докладывались на научных и научно-практических конференциях разного уровня: XIX Международная научно-техническая конференции «Современные средства связи» (Минск, 14–15 октября 2014), XIII Белорусско-российская научно-техническая конференция (Минск, 4–5 июня 2015 г).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении и общей характеристике работы обосновывается актуальность выбранной темы, даётся краткая характеристика её разработанности, определяются цель и задачи, указана теоретико-методологическая основа, отмечены элементы научной новизны, формулируются основные положения диссертации, выносимые на защиту.

Первая глава «Обзор современных методов и средств обеспечения комплексной безопасности объектов» носит теоретический характер, состоит из 5 разделов. В ней определяется следующее:

- основы построения системы защиты информации;
- ресурсы и объекты информационной системы кредитно-финансового учреждения, подлежащих защите;
- угрозы информационной безопасности кредитно-финансового учреждения;
- оценка рисков;
- требований к системе защиты информации.

Вторая глава носит практико-ориентированный характер, состоит из 2 разделов с подразделами. В 1-м разделе 2-й главы определяются этапы разработки система менеджмента информационной безопасности (СМИБ).

Этапы разработки СМИБ:

- получение одобрения руководства для запуска проекта по разработке СМИБ;
- определение области применения, границ и политики СМИБ;
- проведение анализа требований информационной безопасности;
- проведение оценки рисков и планирование обработки рисков;
- разработка СМИБ.

Во 2-м разделе 2-й главы рассмотрены меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. К ним относятся:

- формирование политики безопасности;
- регламентация доступа в помещения;
- обеспечение и контроль физической целостности аппаратных ресурсов;
- подбор и подготовка персонала, обучение пользователей;
- ответственность за нарушения установленного порядка пользования ресурсами информационной системы.

Третья глава имеет практический характер, состоит из 11 разделов. В ней описывается кредитно-финансового учреждения, проводится оценка рисков кредитно-финансового учреждения и выбираются технических средств защиты.

В четвёртой главе описываются правила эксплуатации системы комплексной безопасности кредитно-финансового учреждения.

В ней содержится следующее:

- основные направления технической концепции в области обеспечения безопасности информации;
- распределение полномочий в службе безопасности кредитно-финансового учреждения;
- политики безопасности кредитно-финансового учреждения;
- оценка рисков по результатам внедрения СМИБ в кредитно-финансовое учреждение.

Библиотека БГУИР

ЗАКЛЮЧЕНИЕ

В диссертационной работе выполнено исследование проблем и подходов к обеспечению информационной безопасности кредитно-финансового учреждения.

В процессе исследования разработана классификация угроз безопасности, исследованы объекты, подлежащие защите от потенциальных угроз, сформулированы и раскрыты главные цели и принципы построения комплексной системы обеспечения информационной безопасности учреждения и управления этой системой, сформулированы основные принципы организации работы подразделения безопасности и основные направления его деятельности, а также разработаны методические рекомендации по реализации основных мер, обеспечивающих защиту информации и политика безопасности.

В диссертационной работе произведена оценка рисков до внедрения системы менеджмента информационной безопасности и политики безопасности и после осуществления мероприятий и применения средств защиты.

Показано, что разработанная система комплексной безопасности позволила снизить риски потерь производительности на физическом уровне, риски денежных потерь на сетевом уровне при неавторизованном раскрытии защищаемой информации, риски потерь производительности и репутационных потерь на уровне ОС, риски денежной потери на уровне приложений, необходимых для реализации основных функций ИС, при неавторизованном раскрытии защищаемой информации и риски потери производительности и репутационных потерь на уровне бизнес-процессов организации.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1–А. Белоус Т.В., Паршукова Р.В., Прудник А.М. Документирование на этапах разработки системы менеджмента информационной безопасности // Материалы Международной научно-технической конференции, приуроченной к 50-летию МРТИ-БГУИР. в 2 ч. Ч. 1. / ред. коллегия: А.А. Кураев [и др.]. Минск, 18–19 марта 2014 г. – Минск, БГУИР, 2014. С. 348–349.

2–А. Паршукова Р.В., Белоус Т.В., Прудник А.М. Практические аспекты внедрения систем менеджмента информационной безопасности // Технические средства защиты информации. Тезисы докладов XII Белорусско-российской научно-технической конференции. / ред. коллегия Л.М. Лыньков [и др.]. 28–29 мая 2014 г., Минск. Минск: БГУИР, 2012. С. 6–7.

3–А. Паршукова Р.В., Прудник А.М. Политики безопасности как составная часть комплексной защиты информации предприятия // Технические средства защиты информации. Тезисы докладов XIII Белорусско-российской научно-технической конференции / ред. коллегия Л.М. Лыньков [и др.]. 4–5 июня 2015г., Минск. Минск: БГУИР, 2015. С. 11–12.

4–А. Паршукова Р.В., Прудник А.М. Применение систем менеджмента информационной безопасности для обеспечения комплексной безопасности объекта // Материалы XIX Международной научно-технической конференции "Современные средства связи". / ред. коллегия А.О. Зеневич [и др.]. 14–15 октября 2014. Минск. Минск, ВГКС. С. 207–208. ISBN 978-985-7061-37-2.

5–А. Прудник А.М., Белоус Т.В., Паршукова Р.В. Разработка систем менеджмента информационной безопасности для государственных учреждений // Материалы X Международной научно-практической конференции "Управление информационными ресурсами". / ред. коллегия А.В. Ивановский, А.И. Шемаров, Б.В. Новыш [и др.]. 13 декабря 2013 г., Минск, Академия управления при Президенте Республики Беларусь. С. 151–153.