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

УДК 004.056.53:336.77

Филенков
Максим Петрович

Управление системой защиты информации в кредитно-финансовых организациях

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-98 80 01 – Методы и системы защиты информации, информационная безопасность

Научный руководитель:
Маликов Владимир Викторович
кандидат технических наук, доцент

Минск 2016

ВВЕДЕНИЕ

Информация в наше время является наиболее ценным ресурсом и поэтому сегодня достаточно сложно встретить компании, которые не уделяют должного внимания вопросам защиты информации. Во многих компаниях созданы и функционируют подразделения информационной безопасности, разработаны политики информационной безопасности, внедрено большое количество разнообразных средств защиты, но, важно помнить о том, что даже при наличии надежной защиты от взлома информационных систем внешними злоумышленниками, остается возможной утечка конфиденциальной информации по обычным каналам передачи данных (электронная почта, Интернет, съемные носители информации и т.п.) за счет умышленных или ошибочных действий работников. Именно такие утечки присущи подавляющему большинству предприятий, не использующих специализированные системы защиты от утечки информации.

По оценкам экспертов в области информационной безопасности, утечки корпоративных данных, происходящие по злому умыслу или недосмотру персонала, выдвигаются на первое место в современных рейтингах ИБ-угроз. Внешние нарушители (мошенники, конкуренты, хакеры, и т.д.), стремящиеся получить доступ к защищаемой информации и собственные непорядочные работники, имеющие легальный доступ к ней, в том числе к сведениям о клиентах, персональным данным работников, документам стратегического развития, внутренним аналитическим отчетам и многому другому могут использовать такую информацию в собственных корыстных целях.

В связи с этим, актуальным на сегодняшний день является вопрос защиты конфиденциальной информации в организациях, так как нарушение свойств информации, таких как конфиденциальность, целостность или доступность, может повлечь за собой не только многомиллионные финансовые потери, но и нанести трудно оцениваемые в деньгах репутационные потери.

В настоящий момент вопросам информационной безопасности наибольшее внимание уделяется в банковской сфере, так как деятельность любого банка напрямую связана с большими объемами конфиденциальной информации. Поэтому информация, используемая в деятельности кредитно-финансовых организаций, требует соответствующих методов защиты.

Эффективным способом защиты является создание системы управления информационной безопасностью (СУИБ), которая является современным процессом обеспечения безопасности информационных ресурсов организации, построенная на лучших мировых практиках.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью работы является исследование методов управления системой защиты информации кредитно-финансовых организаций.

Основными задачами являются:

- изучение и классификация угроз системам защиты информации кредитно-финансовых организаций;
- исследование моделей управления системой зашиты информации;
- выбор и обоснование методов, средств для проведения оперативного аудита и оценки эффективности систем защиты информации;
- повышение эффективности управления системой защиты информации.

Объектом исследования являются системы защиты информации кредитно-финансовых организаций.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 1 статья в сборниках материалов конференций.

Положения, выносимые на защиту

1. Модель управления системой зашиты информации КФО, основанная на анализе модели угроз системе менеджмента информационной безопасности с учетом требований по нормативно-правовому, организационно-техническому и техническому обеспечению для управления безопасностью КФО, позволяющая проводить оперативное управление системой защиты с прогнозированием потенциальных угроз такой системе и ликвидации их последствий.
2. Методический подход по оценке эффективности систем защиты информации КФО, основанный на анализе результатов оперативного аудита систем защиты информации КФО с учетом разработанных показателей и критериев оценки эффективности защиты, позволяющий сотрудникам служб безопасности проводить оперативный аудит таких систем.

Личный вклад соискателя ученой степени

Содержание диссертации отражает личный вклад автора. Заключается в анализе существующих угроз безопасности и методах их предотвращения.

Определения целей и задач исследований, интерпретация и обобщение научных результатов проводились совместно с научным руководителем диссертации.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении и общей характеристике работы обосновывается актуальность выбранной темы, даётся краткая характеристика её разработанности, определяются объект и предмет исследования, цель и задачи, формулируются основные положения диссертации, выносимые на защиту.

В первой главе «Современные системы защиты информации кредитно-финансовых организаций» приводятся статистические данные по угрозам безопасности, определяются угрозы безопасности кредитно-финансовых организаций, приводятся данные по методам управления информационной безопасностью, приведена схема управления безопасностью информационных технологий как управление рисками, определено перспективное направление управления информационной безопасностью кредитной организации.

В теории и практике управления есть развивающееся и емкое направление – создание стандартов управления организациями, имеющее своей целью оптимизацию внутренней структуры организации для получения максимального результата от их деятельности. Появились «Стандарты управления деятельностью организаций», которые рассматривают общие вопросы управления сложно организованными коллективами людей.

Со стороны безопасности, последняя подверглась анализу и глубоким разносторонним исследованиям, что послужило толчком для последних разработок на базе риск-ориентированных подходов.

Во второй главе «Управление системой защиты информации кредитно-финансовых организаций» приводятся нормативно-правовое, организационно-техническое и техническое обеспечение для управления системой зашиты информации, модели угроз системе менеджмента информационной безопасности КФО, модели управления системой зашиты информации КФО.

В третьей главе «Оперативный аудит и оценка эффективности систем защиты информации кредитно-финансовых организаций» приводятся нормативно-правовое, организационно-техническое и техническое обеспечение проведения аудитов, психологические особенности проведения аудитов, оценка эффективности систем защиты информации, типовые показатели и критерии эффективности систем защиты информации, методы оценки эффективности систем защиты информации.

Для того чтобы оценить эффективность системы защиты информации или сравнить системы по их эффективности, необходимо задать некоторое правило предпочтения. Такое правило или соотношение, основанное на

использовании показателей эффективности, называют критерием эффективности.

Поставленная проблема может быть решена при развитии «базовой» модели СМИБ за счет метода анализа иерархий (МАИ), предложенного Т. Саати в 70-х года XX века и дающей возможность применять совместно иерархическую систему критериев ИБ и средств обеспечения ИБ.

В четвертой главе даны рекомендации по повышение эффективности управления системой защиты информации КФО.

План мероприятий по совершенствованию СУИБ банка должен состоять:

- подготовка к совершенствованию СУИБ;
- создание СМИБ головного офиса (проектирование, внедрение, опытная эксплуатация);
- совершенствование СИБ головного офиса (проектирование, внедрение, опытная эксплуатация);
- внешний аудит СУИБ головного офиса на соответствие СТБ;
- создание интегрированной СУИБ головного офиса и филиалов банка;
- внешний аудит интегрированной СУИБ на соответствие СТБ.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Проведен анализ статистических данных по угрозам информационной безопасности и современных методов защиты банков на основе которого показано, что основным каналом утечек информации является персонал организации, а также нерациональный выбор способов хранения, передачи и обработки информации. Обозначено, что, являясь широко исследуемым и постоянно совершенствуемым, риск-ориентированных подход является приоритетным для управления информационной безопасностью кредитно-финансовых организаций.

2. Исследованы основные технические нормативно-правовые документы по информационной безопасности кредитно-финансовых организаций. На примере ISO/IEC 27001:2005, COBIT и ITSM проведен сравнительный анализ подходов к обеспечению защиты кредитно-финансовых организаций.

3. Показаны преимущества и недостатки основных походов по определению оценки эффективности СЗИ.

4. Определены этапы совершенствования СУИБ: подготовка к совершенствованию СУИБ, совершенствование СУИБ (проектирование, внедрение, опытная эксплуатация), внешний аудит СУИБ.

Рекомендации по практическому использованию результатов

1. Практические рекомендации по совершенствованию системы управления информационной безопасности КФО могут быть применены при построении систем защиты информации банков.

2. Предложенный подход по оценке эффективности систем защиты информации КФО позволяет сотрудникам служб безопасности проводить оперативный аудит таких систем, оценку реальных и прогнозирования потенциальных угроз, а также обеспечение их оперативной локализации и ликвидации.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1-А. Филенков, М.П. Исследование структуры APT-атак на кредитно-финансовые учреждения / Кушнеров А.Д., Филенков М.П. // Технические средства защиты информации: Тезисы докладов 13–ой Белорусско-российской НТК, 4-5 июня 2015 г., Минск. – Мн.: БГУИР, 2015. – С. 36.