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

УДК 004.056.336.717

Райко
Владислав Владимирович

Методика аудита информационной безопасности банковских технических средств самообслуживания

АВТОРЕФЕРАТ

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

_____

Научный руководитель
Охрименко Алексей Александрович
кандидат технических наук, доцент

_____

Минск 2018

ВВЕДЕНИЕ

Устройства самообслуживания – это наиболее общее определение всех автоматов, позволяющих клиенту совершать различные банковские и иные операции без участия сотрудника. Банковские устройства самообслуживания подразделяются на два типа в зависимости от того, поддерживают ли они функцию выдачи наличных денег или нет. При положительном ответе речь идет об ATM (automated teller mashi-nes), или банкоматах, при отрицательном – о NCS (non-cash systems), или терминалах для безналичных операций.

Жизнь современного общества немыслима без этих устройств. Они облегчают нам жизнь и экономят столь драгоценное в современных реалиях время. Однако рост популярности этих устройств наблюдается не только среди клиентов, все чаще устройства самообслуживания становятся объектами нападения вандалов и грабителей, а также средством, с помощью которого мошенники уводят деньги с карточных счетов держателей банковских карт.

Аудит информационной безопасности банковских технических средств самообслуживания - это мероприятие, призванное проверить насколько эти устройства надежно защищены от посягательств злоумышленников на текущий момент и позволяющее выработать решения по повышению уровня защищенности в случае их недостаточности.

Стандарты информационной безопасности для банковских организаций устанавливаются Национальным Банком Республики Беларусь, однако возникает вопрос, достаточно ли просто соответствовать предъявляемым стандартам для надежной и эффективной защиты банковских технических средств самообслуживания. Очевидно, что нет. Для обеспечения высокого уровня защиты необходимо применение дополнительных средств и мер и мероприятий.

Экспертный аудит информационной безопасности является эффективным мероприятием для повышения уровня защищенности банковских технических средств самообслуживания.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований.

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016-2020 гг., утвержденных Постановлением Совета Министров Республики Беларусь 12 марта 2015 г., № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники»

Цель и задачи исследования

Цель диссертационной работы заключается в разработке методики аудита информационной безопасности банковских технических средств самообслуживания

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Проанализировать ряд нормативных правовых актов и международных стандартов, а также рекомендаций Национального Банка Республики Беларусь в области обеспечения безопасности банковских технических средств самообслуживания и методов проведения аудита безопасности;
2. Проанализировать основные модели нарушителей, угроз и уязвимостей банковских технических средств самообслуживания.
3. Определить требования безопасности, предъявляемые к банковским техническим средствам самообслуживания;
4. Разработать методику проведения аудита информационной безопасности, применимую к банковским техническим средствам самообслуживания.

Результаты работы опубликованы в работах:

Райко, В. В. О защите информации в банкоматах / В. В. Райко // Программирование и защита информации. Сборник трудов постоянно действующего семинара «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп. заседание 15.09.2016. Под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорус. гос. ун-та информатики и радиоэлектроники: рукопись деп. в БелИ-СА 01.11.2016, № 201630. – 155 с. – С. 124–128.

Райко, В. В. Устройство защиты банкоматов, с внешним излучателем электромагнитного поля устройства / В. В. Райко // 53-я науч. конф. аспирантов, магистрантов и студентов учреждения образования «Белорусский госу-

дарственный университет информатики и радиоэлектроники»: материалы конференции по направлению 8: Информационные системы и технологии (Минск, 6 мая 2017 года). – Минск: БГУИР, 2017. – 88 с. – С. 73.

Результаты работы апробированы на

Постоянно действующем семинаре «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп. заседание 15.09.2016. Под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорус. гос. ун-та информатики и радиоэлектроники

53-я науч. конференции. аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» по направлению 8: Информационные системы и технологии (Минск, 6 мая 2017 года)

КРАТКОЕ СОДЕРЖАНИЕ

Работа состоит из введения, общей характеристики работы, шести глав, заключения и двух приложений.

В первой главе был проведен анализ существующих нормативно правовых актов, регулирующих деятельность в области информационной безопасности банковских технических средств самообслуживания. Были рассмотрены рекомендации регулирующих органов в вопросах информационной безопасности банковских устройств самообслуживания. Регулирующим органом является Национальный Банк Республики Беларусь, он устанавливает для банков обязательные требования к безопасному функционированию объектов и безопасности оказания банковских услуг, защите информационных ресурсов и информации, распространение или предоставление которых ограничено. Национальный банк также осуществляет контроль за обеспечением безопасности и защиты информационных ресурсов в банках.

Национальным банком установлено, что при проведении проверки информационной безопасности следует проанализировать основные процессы обеспечения информационной безопасности банка, руководствуясь положениями стандартов РБ:

СТБ 34.101.41-2013 Обеспечение информационной безопасности банков Республики Беларусь. Общие положения;

СТБ 34.101.42-2013 Аудит информационной безопасности;

СТБ 34.101.61-2013 Методика оценки рисков нарушения информационной безопасности;

СТБ 34.101.62-2013 Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с СТБ 34.101.41.

В ходе анализа были приведены основные отличия выше перечисленных стандартов по отношению к стандартам серии СТБ ISO/IEC 27000.

Особо было отмечено что банковские технические средства самообслуживания использующие банковские карты международных платежных систем, в обязательном порядке должны проходить сертификацию по стандарту PCI DSS.

Во второй главе были рассмотрены виды аудита информационной безопасности такие как:

активный аудит. - исследование состояния защищенности информационной системы с точки зрения злоумышленника, обладающего высокой квалификацией в области информационных технологий.

аудит на соответствие стандартам - проверка на предмет соответствия рекомендациям международных и локальных стандартов и требованиям руководящих документов.

экспертный аудит - можно условно представить, как сравнение состояния информационной безопасности с «идеальным» описанием, которое базируется на следующем:

- требования, которые были предъявлены руководством в процессе проведения аудита;
- описание «идеальной» системы безопасности, основанное на аккумулированном в компании-аудиторе мировом и частном опыте.

При анализе представленных видов аудита информационной безопасности были рассмотрены их достоинства и недостатки, а также особенности их проведения.

Для определения, наиболее подходящего под цели и задачи разрабатываемой методики аудита информационной безопасности банковских технических средств самообслуживания, был применен SWOT анализ для оценки сильных и слабых сторон каждого из представленных видов аудита. На основании полученных данных был выбран «экспертный» аудит, как наиболее удовлетворяющий поставленной цели.

В третьей главе рассматриваются базовые принципы построения методика аудита информационной безопасности. Методика основывается на моделях угроз, нарушителей и уязвимостях. В главе приводится описание моделей угроз, нарушителей и уязвимостей, дается их классификация. Схема взаимодействия основных элементов методики приведена в приложении А.

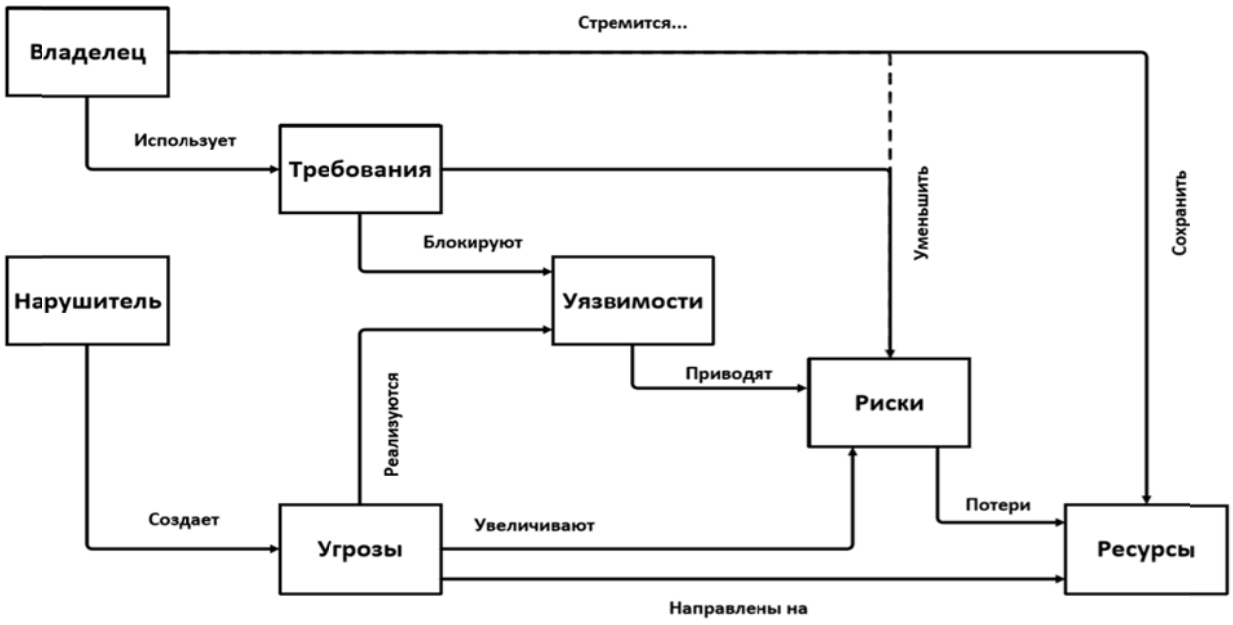

Рисунок 1 – Схема взаимодействия элементов методики.

В четвертой главе представлена рабочая модель методики, рассмотрено применение средств автоматизации призванных систематизировать знания экспертов в области обеспечения информационной безопасности банковских технических средств самообслуживания. Приводится описание преимуществ применения реляционных баз данных для упрощения процедуры проведения аудита. Рассматриваются вопросы наполнения базы данными об известных уязвимостях и угрозах. Схема элементов базы данных рабочей модели методики аудита информационной безопасности приведена на рисунке 2.

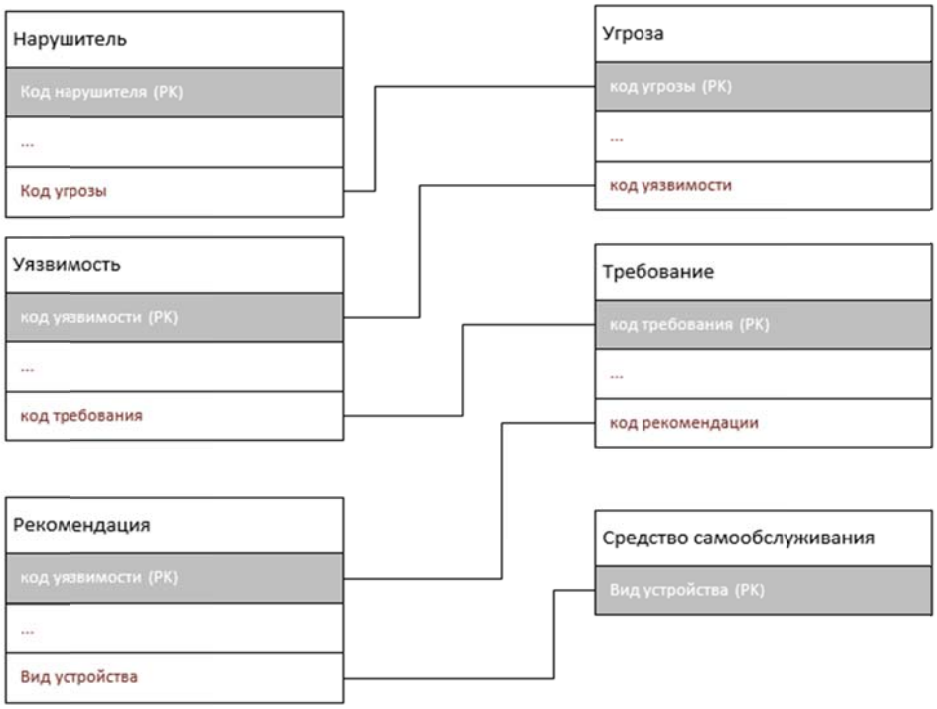

Рисунок 2 – Модель базы данных

Также в четвертой главе рассматривается условный перечень требований информационной безопасности, предъявляемый к банковским техническим средствам самообслуживания.

В пятой главе рассматривается подготовка и предоставление отчетности по результатам проведения аудита информационной безопасности банковских технических средств самообслуживания. В главе также был определен порядок действия аудитора по подготовке отчетной документации и процедуры закрытия аудита. Определен порядок взаимодействия с заказчиком по последующим корректирующим действиям.

Шестая глава посвящена внедрению методики в организации являвшейся исполнителем аудиту

ЗАКЛЮЧЕНИЕ

В ходе проведенной работы, посредством анализа существующих подходов к построению системы защиты информации банковских технических средств самообслуживания, анализа правовых и нормативных документов в области информационной безопасности, анализа видов и методов аудита информационной безопасности была разработана методика аудита применимая к банковским техническим средствам самообслуживания.

В работе был проведен сравнительный анализ различных методик аудита информационной безопасности, определены ключевые различия, достоинства и недостатки. Определен наиболее удовлетворяющий поставленным целям и задачам вид аудита информационной безопасности. Разработаны модели угроз и нарушителей информационной безопасности, характерных для банковских устройств самообслуживания. Рассмотрены вопросы, касающиеся порядка действий при проведении аудита. В работе были определены ключевые требования, предъявляемые к банковским техническим средствам самообслуживания. Был разработан четкий и последовательный алгоритм проведения аудита.

Для обеспечения автоматизации процедуры аудита информационной безопасности банковских технических средств самообслуживания было предложено использование реляционных баз данных, поскольку методика аудита предполагает работу с большим количеством исходных данных, полученных путем сбора через опросные листы, данные полученные по результатам предыдущих аудитов безопасности и дополнительные данные.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1 Райко, В. В. О защите информации в банкоматах / В. В. Райко // Программирование и защита информации. Сборник трудов постоянно действующего семинара «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп. заседание 15.09.2016. Под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорус. гос. ун-та информатики и радиоэлектроники: рукопись деп. в БелИСА 01.11.2016, № 201630. – 155 с. – С. 124–128.

Райко, В. В. Устройство защиты банкоматов, с внешним излучателем электромагнитного поля устройства / В. В. Райко // 53-я науч. конф. аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»: материалы конференции по направлению 8: Информационные системы и технологии (Минск, 6 мая 2017 года). – Минск: БГУИР, 2017. – 88 с. – С. 73.