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

УДК [336.71]:657.6

Зубко
Александр Александрович

Методика аудита уязвимостей системы дистанционного банковского обслуживания

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 2017

ВВЕДЕНИЕ

Обоснование актуальности темы магистерской диссертации. Использование автоматизированных систем во всех сферах деятельности человека, основанных на применении современных информационно-коммуникационных технологий, выдвинуло целый ряд проблем перед разработчиками и пользователями этих систем. Одна из наиболее острых проблем – проблема информационной безопасности, которую необходимо обеспечивать, контролировать, а также создавать условия для ее управления.

Главной целью любой системы обеспечения информационной безопасности является создание условий функционирования предприятия, предотвращение угроз его безопасности, защита законных интересов предприятия от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение в рамках производственной деятельности всех подразделений предприятия. Для эффективной защиты от атак компаниям необходима объективная оценка уровня безопасности ИС - именно для этих целей и применяется аудит безопасности. В этих условиях **актуальность** исследования наиболее опасные уязвимостей систем ДБО и создания методики аудита систем ДБО в области ИБ **не вызывает сомнений.**

Оценка современного состояния решаемой задачи. Дистанционное банковское обслуживание – общий термин для технологий предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленным образом (то есть без визита в банк), чаще всего с использованием компьютерных и телефонных сетей.

Этот вид сервиса имеет ряд преимуществ перед другими видами обслуживания, но, несмотря на все многочисленные достоинства, серьезной проблемой для него является обеспечение информационной безопасности обслуживания: высок риск хищения средств клиентов с помощью компьютерных технологий.

Наиболее интересный объект для атаки со стороны электронных кибервзломщиков представляют юридические лица. В подавляющем большинстве случаев хищение денег организуется с несанкционированным использованием даже неизвлекаемых секретных ключей при онлайновых атаках (когда USB-токен установлен в рабочем компьютере). Наибольшее число проблем возникает, если бухгалтерский компьютер не только постоянно оснащен однажды установленным USB-токеном, но и системный блок не выключается на ночь, а только переводится в «спящий» режим, оставаясь подключенным к каналу доступа в Интернет.

Специалисты по информационной безопасности отмечают низкий уровень защищенности ДБО и большое количество уязвимостей в программном обеспечении, используемом в ДБО-системах, несмотря на увеличение доли профессиональных разработок.

Поэтому требуется найти уязвимости систем ДБО с целью минимизировать риски хищения средств клиентов банка.

Задачи и назначение работы. В соответствии с вышесказанным назначение этой работы – разработка методики аудита систем ДБО.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи проводимых исследований. С ростом числа пользователей банковского дистанционного обслуживания, растет и количество угроз для этих систем. Злоумышленники могут использовать уязвимости не только клиента банка, но и самого банка, а вернее системы ДБО. Используя эти уязвимости, злоумышленник может получить большие возможности по манипуляции данными в системе ДБО, в том числе может управлять счетами клиентов. Поэтому есть необходимость в проведении аудита уязвимостей системы ДБО по определенному методу.

Поэтому **целью настоящей работы** стало исследование создание методики аудита безопасности на возможные уязвимости, слабые места и потенциально опасные участки в области информационной безопасности в дистанционном банковском обслуживании. Для достижения поставленной цели в этой диссертации **решены следующие задачи**:

- проведен обзор накопленного опыта в области аудита информационной безопасности;
- проведены исследования в области информационной безопасности в дистанционном банковском обслуживании;
- разработана методика аудита дистанционного банковского обслуживании для программного обеспечения QUALYS.

Теоретическая и практическая значимость. Теоретическая значимость работы заключается в исследовании методик аудита информационной безопасности. Практическая ценность работы заключается в возможности использования разработанной методики аудита уязвимостей на практике.

Личный вклад магистранта в выполненную работу. Работа полностью выполнена лично магистрантом на базе его исследований, проводимых на работе и на кафедре ЗИ БГУИР.

Результаты работы опубликованы в:

- Материалах XIV Белорусско-российской научно-технической конференции «Технические средства защиты информации» – Методика аудита уязвимостей системы дистанционного банковского обслуживания, 25 — 26 мая 2016 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО БГУИР, 2016.
- Материалах XIIIМеждународной научно-практической конференции «Управление информационными ресурсами» - Аудит уязвимостей системы дистанционного банковского обслуживания системой сканирования QUALYSGUARD, 9 декабря 2016 года, Минск, Респ. Беларусь / редкол.: А. В. Ивановский [и др.]. – Минск: АУ при Президенте, 2016.

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.

Первая глава «Обзор научной литературы» носит теоретический характер, состоит из 3 разделов. В ней определяется следующее:

– предметная область исследования;

– выбор направления исследования;

– выводы.

Вторая глава «Теоретические аспекты дистанционного банковского обслуживания» носит теоретический характер, состоит из 4 разделов. В 1-м разделе 2-й главы дается определение системы ДБО и характеристика.

Во 2-м разделе 2-й главы дается сравнительный анализ дистанционного банковского обслуживания физических лиц предоставляемымуслуги различных банков Республики Беларусь.

В 3-ем разделе 2-й главы рассматривается новшества в дистанционного банковского обслуживания со стороны безопасности, предоставляемых услуг клиенту банка.

В четвёртом разделе 2-й главы описываютсясостояние белорусского банковского обслуживания, каких результаты применения дистанционного банковского обслуживания в Республике Беларусь.

В главе 3 «Методы аудита информационной безопасности информационных систем» носит практико-ориентированный характер, и состоит из 2 разделов. В которых рассматривается следующее:

– Уязвимости ДБО;

– Аудит уязвимостей информационных систем.

Раздел 2 делится на следующие подразделы:

– Инициирование процедуры аудита;

– Анализ данных;

– Анализ рисков;

– Использование методов анализа рисков.

В главе 4 описывается подробная методика аудита уязвимостей с программного обеспечения Qualys, где показывается преимущества данного программного обеспечения.

ЗАКЛЮЧЕНИЕ

Рассмотрена предметная область, выбранная для исследования в диссертации – Методика аудита уязвимостей систем дистанционного банковского обслуживания. Показано, что дистанционное банковское обслуживаниепользуется большим спросом в нашей стране. Но как и другие информационные систем, дистанционное банковское обслуживание нуждаются в защите информации своих клиентов. Рассмотрены опыт по обеспечению безопасности информационных систем. Выбрано направление исследования методика аудита уязвимостей системы дистанционного банковского обслуживания.

Рассмотреныуязвимости информационных систем ДБО. Проведен анализ уязвимостейдистанционного банковского обслуживания.в Главе 3Выделены наиболее опасные участки в ДБО в рамках исследований за предыдущие годы.Также рассмотрена методика аудита исходя из ISO 27001.

Исходя из исследований, разработана методика аудита уязвимостей систем ДБО с помощью программного обеспечения QUALYS. Уязвимости неотделимы от объекта и обуславливаются недостатками процесса его функционирования, свойствами архитектуры, протоколами обмена и интерфейсами, применяемым программным обеспечением и аппаратурой, условиями эксплуатации и расположения. Источники угроз могут использовать уязвимости для нарушения безопасности информации.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1–А]Зубко А.А., Прудник А.М. Методика аудита уязвимостей системы дистанционного банковского обслуживания // Технические средства защиты информации. Тезисы докладов XIV Белорусско-российской научно-технической конференции. / ред. коллегия Л.М. Лыньков [и др.]. 28–29 мая 2016 г., Минск. Минск: БГУИР, 2016. С. 9.

[2–А]Зубко, А. А., Прудник, А. М., Аудит уязвимостейсистемы дистанционногобанковскогообслуживания системой сканирования QUALYSGUARD //Управление информационными ресурсами : материалы XIIIМеждунар. науч.-техн. конф., 9 дек. 2016 года, Минск, Респ. Беларусь / редкол.: А.В. Ивановский[и др.]. – Минск: УО АУ при Президенте, 2016. – С. 192.