УДК 004.56

УГРОЗЫ БЕЗОПАСНОСТИ СИСТЕМ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Топалов Р.В.,
студент колледжа информатики и программирования, Финансовый университет
root@topalov.pro

Чачуа Т.Г.,
студент колледжа информатики и программирования, Финансовый университет
tamriko17@bk.ru

Аннотация. *В статье рассмотрено понятие электронного банкинга, его место и перспективы в системе современных банковских услуг. Определены виды и состав системы дистанционного банковского обслуживания как технологии предоставления финансовых услуг, при которой поставщик услуг и клиент взаимодействуют посредством информационно-телекоммуникационных систем. Представлена и проанализирована статистика угроз безопасности взаимодействия в системах дистанционного банковского обслуживания. Сделан вывод о существовании рисков, связанных с атаками злоумышленников на банкоматы и другие виды дистанционного банковского обслуживания. Выделены способы и средства несанкционированного воздействия, влекущие за собой получение злоумышленником денежных средств. Рассмотрен алгоритм поведения современного вредоносного программного обеспечения «Тюпкин», воздействующего на банкоматы, которое способно нанести значительный ущерб финансовой организации. По результатам проведенного исследования сделан вывод, что большая часть действующих систем дистанционного банковского обслуживания имеет проблемы, связанные с обеспечением необходимого уровня защищенности, что указывает на необходимость внедрения процессов обеспечения безопасности на всех стадиях жизненного цикла приложений элементов системы.*

Ключевые слова: *защита информации; угроза; банкомат; вредоносное программное обеспечение; риск.*

SECURITY THREATS OF REMOTE BANKING SERVICES

Topalov R.V.,
student at College of Computer Science and Programming, Financial University
root@topalov.pro

Chachua T.G.,
student at College of Computer Science and Programming, Financial University
tamriko17@bk.ru

Abstract. *The subject of this article is electronic banking, its place and prospects in modern system of banking services. Definitions are given to the different kinds and the structure itself of the system of remote*

Научный руководитель: ***Оладько В.С.,*** *кандидат технических наук, председатель ПЦК «Информационная безопасность» колледжа информатики и программирования.*

banking as a type of processing of financial services, in which the provider and client interact by means of information and telecommunication networks. The information regarding statistics of security risks interaction in remote banking systems is provided and analyzed. The conclusion regarding the existence of risks linked with intruder attacks on ATMs and other means of remote banking is drawn. The ways and means of unauthorized impact which brings about the intruder receipting money are provided. The behavioral algorithm of modern malicious software "Tyupkin" which affects ATM and could potentially cause considerable damage on financial organization is examined. By results of the conducted research the following conclusion is drawn: the majority of functioning now systems of remote banking have issues, connected with providing them with necessary level of security, which points to necessity of implanting processes of safety on all stages of lifecycle of applications connected with all elements of the system.

Keywords: *data protection; threat; ATM; malicious software; risk.*

В настоящее время системы дистанционного банковского обслуживания (ДБО) становятся неотъемлемой частью повседневной жизни, обеспечивающей удобную и выгодную форму взаимодействия банка с клиентами. Целью систем ДБО является применение средств автоматизации и информационно-телекоммуникационных технологий для обеспечения удаленного или дистанционного обслуживания клиентов. В соответствии с [1, 2] система ДБО включает в себя следующие элементы:

- ПС-банкинг (PC-banking) — системы типа клиент-банк.
- Интернет-банкинг (Internet-banking).
- Мобильный банкинг (Mobile-banking).
- Телебанкинг (phone-banking).
- Обслуживание с использованием банкоматов и устройств банковского самообслуживания (ATM-banking).

Связи между элементами систем ДБО являются физическими и функциональными, каждый элемент в отдельности выполняет свои функции, при этом все элементы системы взаимодействуют между собой, выполняя общую системную функцию, связанную с реализацией банковских бизнес-процессов и обеспечением высокого качества банковских услуг. Поэтому быстрая, безопасная и бесперебойная обработка значительных информационных потоков, циркулирующих между элементами системы ДБО и автоматизированной банковской системой, является одной из главных задач любой банковской организации.

Анализ исследований [3, 4], проводимых компаниями-аналитиками в области информационной безопасности, показывает, что основными причинами нарушения безопасности данных и бесперебойности обработки информационных потоков в ДБО являются целенаправленные кибератаки злоумышленников. По данным [5], в январе — сентябре 2016 г. в шесть раз участились случаи кибератак на ведущие финансовые организации России. Причиной таких атак, в подавляющем большинстве случаев, является коммерческий интерес, для маскировки которого злоумышленниками часто используется политический контекст. Основным способом реализации кибератак являются уязвимости в системах ДБО: 40% всех уязвимостей систем ДБО, уже находящихся в эксплуатации, — критически опасные; 27,8% имеют средний уровень опасности и 32,0% — низкий уровень опасности. Основными последствиями реализации кибератак являются (*рис. 1*):

- кража денежных средств — 30%;
- несанкционированный доступ к банковской тайне — 15%;
- доступ к файловой системе или СУБД банка — 30%;
- несанкционированный доступ к сведениям, составляющим банковскую тайну на уровне отдельных клиентов — 25% [4].

Наибольший риск несут последствия угроз, связанные с кражей денежных средств. При реализации подобных угроз злоумышленники часто в качестве объекта проведения атаки используют публичные узлы инфраструктуры ДБО банков — банкоматы. С точки зрения архитектуры сети банка они являются обычными узлами, за исключением того, что банкоматы не должны иметь прямого доступа к глобальной сети Интернет и часто находятся за пределами контролируемой зоны банка.

Иногда банки прибегают к виртуализации сетевых адаптеров, которые обращаются

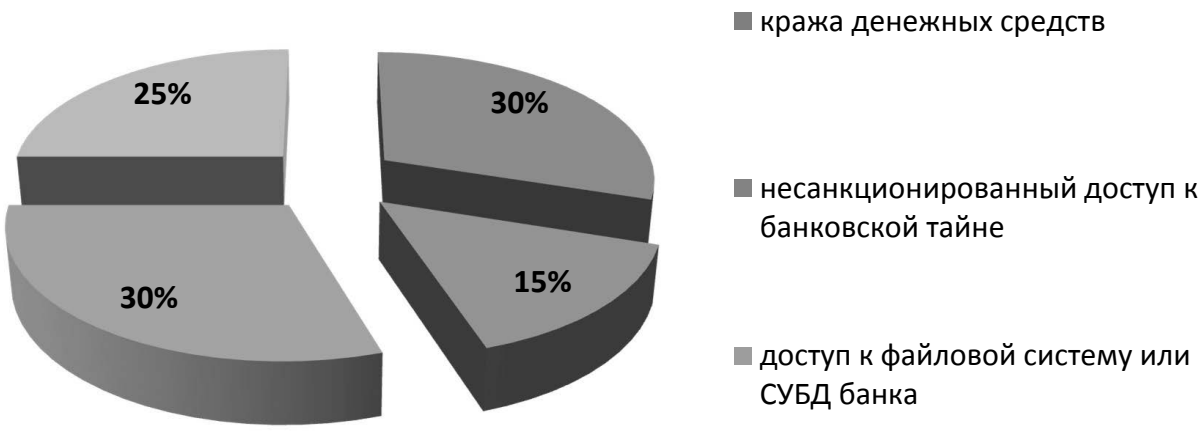

Рис. 1. **Последствия реализации кибератак на системы ДБО в 2015 г., данные Positive Technologies**

к сети только через VPN (виртуальную частную сеть). Однако в случае, если происходит сбой VPN-сервера или нарушение соединения с ним, туннелирование прекращается, и данные автоматически начинают передаваться через открытые каналы. Банкоматы всегда работают с деньгами двух типов: реальные банкноты, которые лежат в кассетах и выдаются через диспенсер, и данные банковских карт, которые являются, по своей сути, ключами к счетам клиентов банка. Основной задачей злоумышленников всегда является получение этих денег. В качестве основных несанкционированных способов получения денежных средств выделяют:

- физическое воздействие и повреждение банкомата;
- заражение программного обеспечения банкомата вредоносным программным обеспечением;
- мошенничество с банковскими картами.

Рассмотрим процесс получения наличных на примере вредоносной программы «Тюпкин». Этот вирус распространился в 2014 г. по всему миру и нанес огромный ущерб большому числу банков. Существует как минимум три версии данного вируса:

1. Первая версия, которая появилась в феврале-марте 2014 г. в Санкт-Петербурге, отчасти была написана на языке программирования C#. Однако позднее создатели вируса поняли, что далеко не на всех банкоматах установлена программная платформа NET Framework компании Microsoft, необходимая для выполнения программ, написанных на этом языке.

2. Во второй версии была учтена ошибка с выбором языка программирования, и все модули были переписаны на более универсальный язык C++.

Большая часть действующих систем ДБО имеют проблемы, связанные с обеспечением необходимого уровня защищенности, что указывает на необходимость внедрения процессов обеспечения безопасности на всех стадиях жизненного цикла приложений элементов системы ДБО.

3. До выхода третьей версии вируса использовались одноразовые пароли для доступа к банкоматам. Теперь же создатели вредоносного ПО научились работать с картами и для авторизации вируса требовались данные карты. Стоит заметить, что переход от одноразовых паролей характерен для большинства вредоносных программ такого типа.

Заражение банкомата происходит в несколько этапов (*рис. 2*).

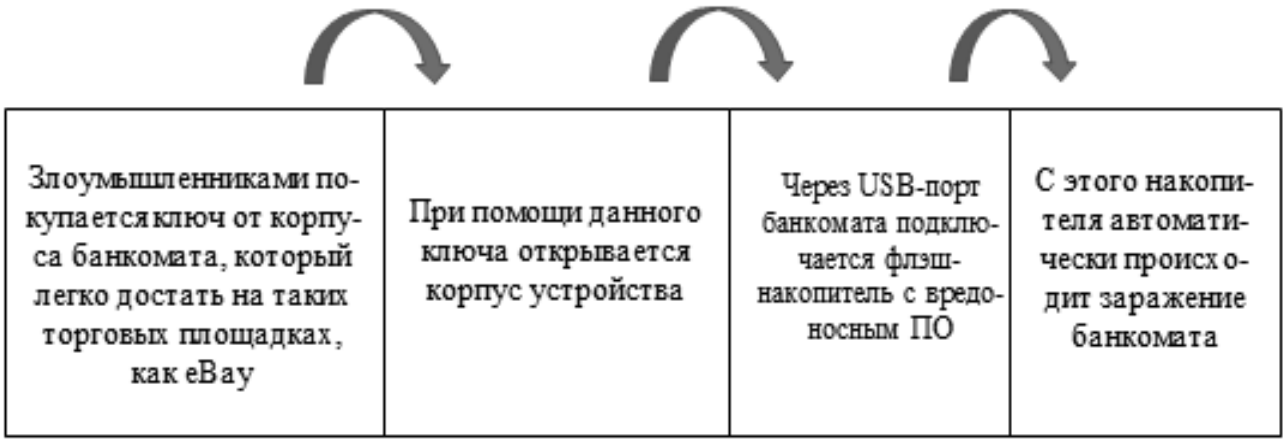

Рис. 2. **Этапы заражения банкомата вирусом «Тюпкин»**

Существует окно времени, в течение которого троян находится в ожидании команд от злоумышленника. Происходит генерация сессионного ключа, т.е. псевдослучайной последовательности символов, которая действительна один раз и только для данной сессии. Злоумышленник сообщает по телефону оператору трояна этот сессионный ключ, получая в ответ временный пароль, который вводится через клавиатуру (пинпад). Далее при помощи кнопок на пинпаде атакующий выбирает, содержимое какой кассеты необходимо извлечь.

«Тюпкин» временно блокирует все сетевые интерфейсы банкомата, таким образом отключая устройство от Интранета (внутренней сети) банка. В случае если системы видеонаблюдения, сигнализации и подобные привязаны к сетевому интерфейсу, то они также становятся временно недоступны банку. Обнаружение пропажи наличных происходит лишь в момент передачи кассет от инкассации к кассиру банка. В первую очередь рассматривается возможность нахождения злоумышленника среди сотрудников банка, который, пользуясь своим служебным положением, мог провести подобную атаку. Только после исследования содержимого накопителей банкомата (жестких дисков) и просмотра записей с камер видеонаблюдения становится ясно, что произошло заражение банкомата.

Таким образом, можно сделать вывод, что большая часть действующих систем ДБО имеют проблемы, связанные с обеспечением необходимого уровня защищенности, что указывает на необходимость внедрения процессов обеспечения безопасности на всех стадиях жизненного цикла приложений элементов системы ДБО. Для контроля состояния защищенности необходимо проводить ее оценку как на этапах разработки и перед вводом системы в эксплуатацию, так и во время ее активного использования клиентами банка. Такую оценку необходимо осуществлять на регулярной основе с контролем устранения выявленных недостатков.

Литература

1. *Дьякова О.*Н. Содержание системы дистанционного банковского обслуживания // Современные проблемы науки и образования. 2015. № 1–1. С. 60–72.
2. *Самсонова Л.А.* Дистанционное банковское обслуживание // Философские проблемы информационных технологий и киберпространства. 2012. № 2 (4). С. 81–91.
3. Уязвимости онлайн-банков 2016: лидируют проблемы авторизации // ХабраХабр. URL: https://habrahabr.ru/company/pt/blog/307450/ (дата обращения: 11.12.2016).
4. *Акимов Е.* Угрозы и тренды 2016 // Информационная безопасность. URL: http://www.itsec.ru/articles2/Oborandteh/ugrozy-i-trendy-2016 (дата обращения: 11.12.2016).
5. Отчет Центрального банка РФ «Обзор финансовой стабильности за второй-третий кварталы 2016 года». URL: https://www.cbr.ru/publ/Stability/fin-stab-2016_2–3r.pdf.