МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Национальный исследовательский ядерный университет
«МИФИ»

Материалы
VII Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ
«УГРОЗЫ И РИСКИ ФИНАНСОВОЙ БЕЗОПАСНОСТИ В КОНТЕКСТЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ»

24-26 ноября 2021 г., Москва

Москва 2021

УДК 005.934:004:336.7

Обеспечение безопасности банкоматов в условиях цифровизации

Т.И. Карабчук
студентка 1 курса магистратуры
ФГАОУ ВО «КФУ им. В. И. Вернадского», г. Симферополь
E-mail: tanya_karabchuk@mail.ua
научный руководитель: О.Г. Блажевич
к.э.н., доцент кафедры финансов и кредита
ФГАОУ ВО «КФУ им. В. И. Вернадского», г. Симферополь
E-mail: blolge@rambler.ru

Аннотация: *Преступность, связанная с банкоматами, продолжает расти и распространяться по всему миру, несмотря на региональные различия в частоте совершения преступлений. Поэтому в статье рассмотрены традиционные и новые преступления, связанные с банкоматами, а также разработаны рекомендации обеспечению безопасности банкоматов.*
Ключевые слова: *банкомат, мошенничество, безопасность, скимминг.*

Ensuring ATM security in the context of digitalization

Abstract: *ATM-related crime continues to grow and spread around the world, despite regional differences in the frequency of crimes. Therefore, the article discusses traditional and new crimes related to ATMs, as well as recommendations for ensuring the security of ATMs.*
Keywords: *ATM, fraud, security, skimming.*

Мошенничество с банкоматами стало глобальной проблемой, с которой сталкиваются не только клиенты, но и банковские операторы. Методы мошенничества, используемые киберпреступниками, стали более совершенными, и управление рисками, связанными с мошенничеством в банкоматах, является важной проблемой, с которой сталкиваются финансовые учреждения по всему миру. С появлением новых атак на банкоматы перед владельцами банкоматов стоит задача обеспечить их кибер-готовность к этим новым угрозам.

Угрозы/атаки банкоматов можно разделить на физические и логические атаки. Физические атаки включают в себя физическое нападение на банкомат, киберпреступники используют такие методы, как твердые и

газовые взрывчатые вещества. Другие физические атаки включают размещение гаджетов в банкомате киберпреступниками, которые копируют данные карты банкомата и воспроизводят их на другой карте, которую можно использовать для снятия денег со счета владельца карты. Логические атаки включают использование вредоносных программ для указания банкомату выдавать деньги. Такие атаки могут быть осуществлены путем получения физического доступа к банкомату для установки этой вредоносной программы на ядро ПК банкомата, либо вредоносная программа может быть внедрена через сеть [5]. Рассмотрим распространённые виды атак на банкоматы:

1. Скимминг банковских карт.

Атака на скимминг банковских карт — это физическая угроза, которая в прошлом была угрозой номер один для банкоматов во всем мире. Скимминг банкоматов относится к краже данных электронной карты, помогая преступнику подделать карту. Скиммер — это устройство, установленное на считывателе карт, заставляющее клиента поверить, что он вставляет свою карту в считыватель карт банкомата. Скиммер считывает данные с магнитной полосы карты или чипа EMV (Europay + MasterCard + VISA), когда клиент вставляет карту в банкомат. Некоторые скиммеры имеют возможность считывать данные с чипа карты на расстоянии. Однако атаки на скимминг банкоматов сокращаются благодаря внедрению решений для защиты от скимминга, стандарта безопасности данных индустрии платежных карт, технологии EMV и функциональности бесконтактных банкоматов [1].

2. Скимминг подслушивания.

Новый тип скимминг-атаки, называемый «скиммингом подслушивания», появился и распространился преимущественно в Соединенном Королевстве. Атака нацелена на моторизованные считыватели карт банкоматов на более старой модели банкоматов под названием personas. Злоумышленник проникает в банкомат, чтобы получить доступ к считывателю карт банкомата. Затем скиммер устанавливается непосредственно на электрический узел, который переносит данные карты на устройство считывания карт. В банкоматах Personas злоумышленник нацеливается на электронную панель управления считывателем карт, создавая отверстие за окном ориентации карты банкомата.

3. Блокировка карты банкомата.

Атака на блокировку карту банкомата — это атака, в ходе которой киберпреступник вставляет устройство в устройство считывания карт банкомата, которое перехватывает и записывает данные, передаваемые между чипом EMV и устройством считывания карт банкомата. Затем эти

данные могут быть повторно использованы для клонирования карты с магнитной полосой. Данные чипа EMV и данные магнитной полосы имеют разные контрольные значения (CVV), и поэтому данные, полученные с карты чипа EMV, нельзя использовать для клонирования магнитной полосы. Блокировка карты не является уязвимостью ни для чиповой карты, ни для банкомата. Поэтому нет необходимости добавлять в банкомат механизмы защиты от этой формы атаки. Если во время транзакции в банкомате соблюдается надлежащая процедура авторизации, поддельные карты могут быть немедленно обнаружены. Эта атака может быть успешной только в том случае, если эмитент пренебрегает проверкой CVV при авторизации транзакции. Поэтому все эмитенты должны проводить эти базовые проверки, чтобы предотвратить эту категорию мошенничества.

4. Перехват карт банкомата.

Перехват карты банкомата крадет саму физическую карту через устройство, подключенное к банкомату. Киберпреступники помещают устройство непосредственно над или в слот для считывания карт банкомата. Эти устройства предназначены для захвата карт после того, как клиенты вставляют их в банкомат. Возможность бесконтактной связи помогает в борьбе с этим мошенничеством.

5. Перехват наличных в банкоматах.

Перехват наличных — это когда киберпреступник использует устройство для физического захвата выдаваемых наличных и приходит за ними, как только клиент покинул место расположения банкомата. Это мошенничество включает в себя размещение денежных ловушек или фальшивых предъявителей перед банкоматом. При обработке транзакции банкомат выдает банкноты в ловушку, установленную киберпреступниками вместо того, чтобы передать деньги клиенту. Клиент предполагает, что банкомат неисправен, и уходит. Затем киберпреступник возвращается, удаляет денежную ловушку или фальшивого предъявителя и уходит с наличными, предназначенными для клиента.

6. Мошенничество с отменой транзакций.

Мошенничество с отменой транзакций включает в себя создание ошибки, из-за которой создается впечатление, что наличные деньги не были выданы. На счет повторно зачисляется сумма, (снятая), но эти деньги преступник забирает. Это может быть физический захват (аналогичный захвату наличных денег) или искажение сообщения о транзакции. Счет не будет списан, хотя преступник снимет наличные из банкомата [4].

7. Социальная инженерия/Фишинговые атаки.

Жертву обманом заставляют раскрыть свою идентификационную информацию (PIN-код). Это может быть физически или с помощью электронных средств. например, злоумышленники создают

мошеннические веб-сайты для сбора аутентификационной информации от ничего не подозревающих клиентов во имя необходимых обновлений или изменений, проводимых их "банкирами". Пользователь в конечном итоге разглашает конфиденциальные данные своей карты мошенническому сайту [2].

8. Операционное мошенничество.

При этом виде мошенничества банкоматом манипулируют. Банкомат сконфигурирован так, чтобы выдавать большие купюры как меньшие, вследствие чего выдает больше денег, чем следует выдавать. Это может быть достигнуто либо путем загрузки банкнот неправильного номинала в неправильные кассеты с деньгами, либо путем внесения неправильной конфигурации в программное обеспечение.

9. Атаки вредоносных программ.

Атаки вредоносного ПО обычно проще проводить при участии инсайдера, поскольку для развертывания вируса необходим физический доступ. Тем не менее, сегодня эта атака возможна онлайн. Вредоносный файл или устройство помещается в банкомат, затем его управляющее устройство запускается, чтобы предоставить злоумышленнику дистанционное управление через пользовательский интерфейс, который позволяет записывать номера карт и ПИН-коды через личное пространство памяти приложений для обработки транзакций, установленных на взломанном банкомате. Развертывание эффективного антивирусного программного обеспечения может помочь смягчить этот класс атак.

10. Атаки вымогателей.

Серьезная вредоносная программа под названием «WannaCry» затронула многие организации по всему миру. Она была запущена 12 мая 2017 года и предназначалась для компьютеров под управлением Windows 7 или более ранних версий в более чем 150 странах. «WannaCry» шифрует файлы на конечных точках, на которых запущено программное обеспечение операционной системы Microsoft, делая их недоступными. Файлы расшифровываются только после выплаты денежной суммы, известной как выкуп. Эта вредоносная программа пытается заразить другие конечные точки в той же сети. Вредоносная программа не нацелена специально на банковские и розничные системы или их функциональные возможности, но банкоматы, как и любая другая система на базе Windows, также подвержены риску этой атаки [3].

Многие организации по всему миру пострадали от другой вредоносной программы под названием «Petya». Эта вредоносная программа шифрует файлы на конечных точках, работающих под управлением программного обеспечения операционной системы Microsoft, делая их недоступными. Банкоматы подвержены риску этой атаки, поскольку они работают в

операционной системе Microsoft. Все банкоматы, работающие под управлением любой операционной системы Windows, которые не были исправлены с помощью обновления безопасности Microsoft MS17-010, подвергаются риску. Если какие-либо банкоматы заражены/заблокированы программой-вымогателем, то все остальные банкоматы и конечные точки в той же сети также должны быть проверены на наличие вирусов. Как только вредоносная программа заразит одну конечную точку в сети, она будет реплицироваться в другие уязвимые системы.

11. «Банкоматный джекпот».

Термин «Банкоматный джекпот» происходит от термина «Джекпот». При таком типе атаки киберпреступники сразу получают огромные суммы денег из банкомата. Киберпреступники используют два метода для выполнения этой атаки:

- Атака черного ящика: Киберпреступнику необходим физический доступ к верхнему шкафу банкомата, в котором размещается ядро ПК банкомата, а затем он переводит банкомат в режим супервизора. Злоумышленник удаляет сетевой кабель банкомата, чтобы банкомат не мог контролироваться службой мониторинга банкоматов. Затем злоумышленник устанавливает черный ящик, который представляет собой специальное устройство, запрограммированное для управления банкоматом. Банкомат переходит в режим супервизора для клиента банкомата, но банкомат все еще работает. Черным ящиком можно управлять по беспроводной сети с помощью обычного смартфона. Злоумышленник использует смартфон для выдачи команд банкомату для выдачи наличных. Команда может выдаваться непрерывно до тех пор, пока в банкомате не закончатся деньги. Затем злоумышленники удаляют устройство черного ящика и не оставляют никаких следов его установки на банкомате.

- Вредоносная атака: Вредоносное ПО может быть доставлено физически с помощью USB-портов банкомата или удаленно через взломанную банковскую сеть. Используя клавиатуру и командную строку, злоумышленник запускает вредоносную программу. Эти действия можно даже автоматизировать, чтобы вредоносная программа работала автономно. Атака может быть проведена через сеть без физического доступа к банкомату и возможна, когда отсутствуют система защиты банкомата от вредоносных программ, белый список программного обеспечения для банкомата, аутентификация для обмена данными между аппаратными блоками банкомата и его основным приложением.

Владельцы банкоматов должны внедрять решения для предотвращения несанкционированного развертывания вредоносных программ на

банкоматах [4]. В целом, все владельцы банкоматов должны выполнять следующие действия для обеспечения безопасности своих банкоматов:

– следовать всем рекомендациям в стандарт безопасности индустрии платёжных карт;

– система обнаружения вторжений должна быть настроена так, чтобы отслеживать весь трафик и предупреждать о любых подозрительных действиях;

– брандмауэр должен быть настроен так, чтобы обновлять и пропускать только известный трафик приложений внутрь и наружу;

– программа управления исправлениями для операционной системы и приложений должна быть на месте, чтобы гарантировать, что программное обеспечение банкоматов хорошо исправлено;

– должно быть разработано программное решение для внесения банкоматов в белый список, а также должен быть установлен и постоянно обновляться антивирус;

– необходимо внедрить систему управления рисками и подготовить план реагирования на эти риски, чтобы сообщения о мошенничестве с банкоматами поступали в режиме реального времени;

– программное обеспечение банкомата должно регулярно обновляться;

– всем операторам банкоматов следует перейти на чип EMV и PIN-карту и исключить откат магнитной полосы, это снизит риск скимминга карт;

– отделить сеть банкоматов от остальной сети банка с помощью брандмауэра и виртуальных локальных сетей;

– должна быть разработана политика паролей, чтобы гарантировать, что в банкоматах используются только надежные пароли, и у каждого пользователя есть свой собственный уникальный пароль;

– все коммуникации в банкомате должны быть зашифрованы, включая связь между ядром ПК и банкоматом;

– неиспользуемые сервисы и приложения должны быть удалены из банкомата, чтобы уменьшить поверхность атаки;

– необходимо развернуть эффективное программное обеспечение для защиты от вредоносных программ;

– операционная система ядра ПК должна быть закалена;

– тестирование на проникновение должно проводиться на банкомате ежегодно;

– обеспечить физическую безопасность банкомата, такую как видеонаблюдение и сигнализация, при его установке;

– установить инструмент, который обеспечит конфиденциальность, целостность и доступность банкомата.

Таким образом, для предотвращения рассмотренных рисков владельцы банкоматов должны убедиться, что они применяют рекомендуемые меры противодействия для обеспечения безопасности среды банкомата для пользователя. Предлагаемые средства управления должны быть проверены путем их внедрения в банкомате, а затем выполнение теста на проникновение. Это должно быть сделано в разных географических регионах, чтобы обеспечить работу средств контроля во всех регионах мира. На основе предлагаемых средств контроля будет разработана структура, способствующая повышению безопасности банкоматов.

Список использованных источников:

1. Антонов А. Как злоумышленники используют уязвимости АТМ // Расчеты и операционная работа в коммерческом банке. М.: Регламент, – 2018. – № 2 (144). – С. 47–59.
2. Архипов А. Проблемы определения места совершения мошенничества в отношении безналичных денежных средств // Уголовное право. – 2016. – № 3. – С. 4–10
3. Блажевич О. Г. Особенности развития финансового рынка в условиях цифровизации / О. Г Блажевич, Н.С. Сафонова // Научный вестник: финансы, банки, инвестиции – 2021. – №1 (54). – С. 106-124.
4. Буркальцева Д. Д., Управление финансово-экономической безопасностью: институциональные основы в условиях цифровизации / Д. Д. Буркальцева Р.А. Овчинников // Методологические основы и научно-практические положения институционального прогнозирования и планирования в системе государственного регулирования экономики: Материалы Международного научно-практического круглого стола. – 2018. – С. 21-24.
5. Норец Н.К. Цифровая безопасность банковской сферы / Н.К. Норец // Развитие Российской экономики и ее финансовая безопасность в условиях современных вызовов и угроз: международная научно-практическая онлайн конференция, г. Ростов, 22-23 октября 2020 г. – С. 183-186.