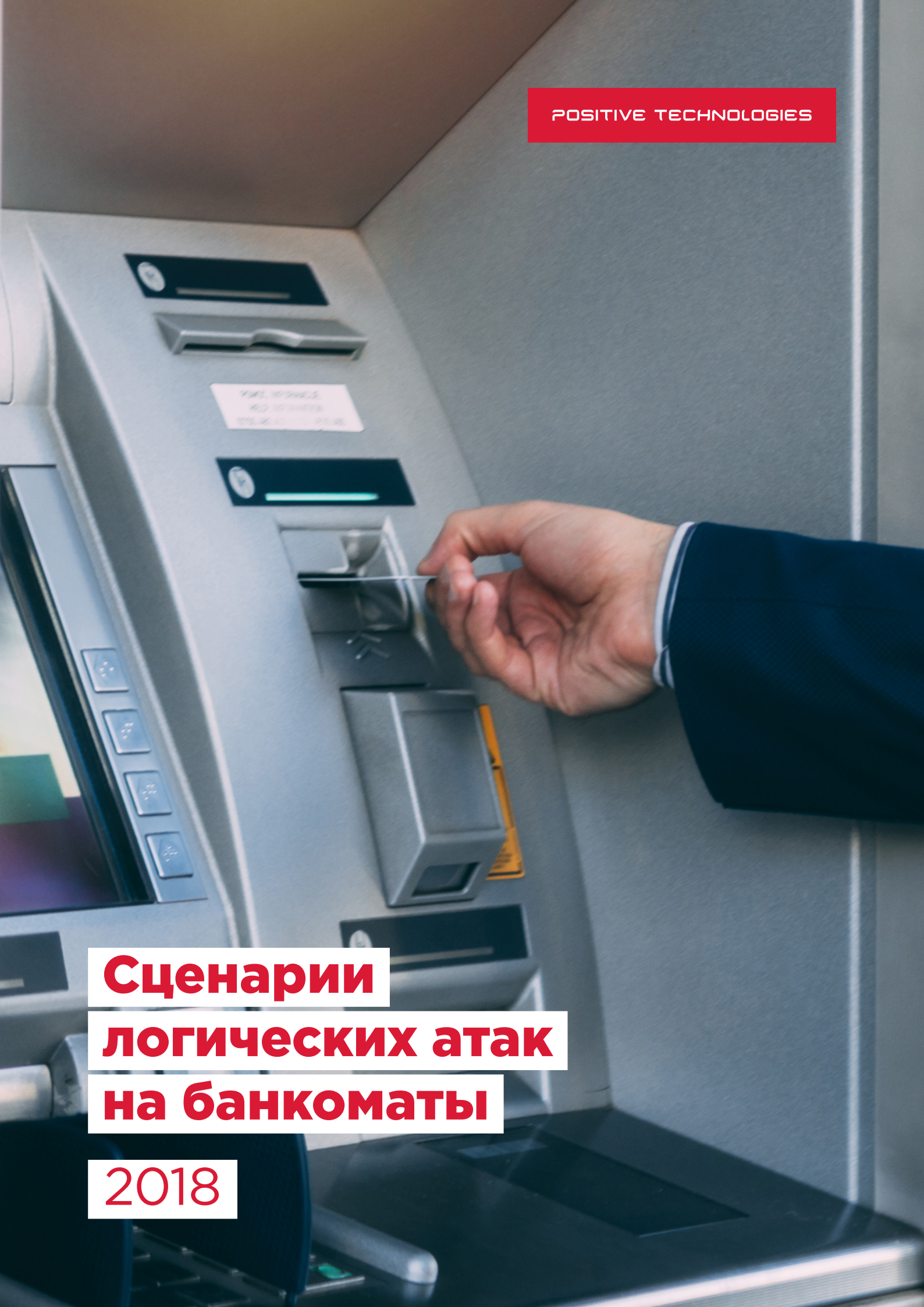


POSITIVE TECHNOLOGIES

A close-up photograph of an ATM interface. A person's hand, wearing a dark blue suit sleeve, is holding a thin, light-colored card and inserting it into a slot. The ATM is grey with a black screen on the left showing some colorful graphics. Below the screen are four buttons with icons. Above the card slot is a small white label with text. The background is a plain, light-colored wall.

# **Сценарии логических атак на банкоматы**

**2018**



## Содержание

Введение.....	2
Портрет участников.....	3
Как устроен банкомат.....	4
Сценарии атак.....	6
Хищение денег.....	6
Сетевые атаки.....	6
Black Box.....	11
Выход из режима киоска.....	13
Подключение к жесткому диску.....	17
Загрузка в нештатном режиме.....	19
Перехват карточных данных.....	20
Заключение.....	23



## Введение

В январе 2018 года Секретная служба США, а также крупнейшие производители банкоматов Diebold Nixdorf и NCR выпустили экстренные предупреждения, в которых сообщалось об угрозе атак на банкоматы. Особое внимание при этом уделялось способам атак: предполагалось, что преступники собираются заражать банкоматы вредоносным ПО или подключать специальные устройства, чтобы управлять выдачей денег.

За пару месяцев до этого, в октябре 2017 года, серия подобных атак прошла в Мексике. Злоумышленники заранее подготовили жесткий диск, на котором находилось вредоносное ПО, и подменяли оригинальный жесткий диск банкомата. Чтобы восстановить соединение с диспенсером купюр, требовалось эмулировать физическую аутентификацию, то есть подтвердить, что имеется легальный доступ к сейфу. Для этого преступники использовали медицинский эндоскоп: с его помощью они смогли управлять сенсорами диспенсера. По сообщениям NCR, в этот же период были зарегистрированы и так называемые атаки Black Box: вместо подмены жесткого диска преступники подключали к диспенсеру устройство, которое отправляло команды для выдачи купюр, и забирали деньги. В январе атаки распространились и на Соединенные Штаты.

Все атаки объединяло то, что преступники не применяли физических методов для взлома банкоматов: они опустошали банкоматы, используя вредоносные программы или устройства. Такие атаки называются логическими, и хотя они требуют тщательной технической подготовки, их проведение привлекает значительно меньше внимания, а значит, сопряжено с меньшим риском.

Если для США это был первый случай массового взлома банкоматов, то в остальном мире с такими инцидентами сталкиваются уже давно. Впервые информация об атаке с применением вредоносного ПО появилась в 2009 году, когда был обнаружен троян Skimer, позволяющий похитить деньги и данные платежных карт. С этого момента логические атаки начали набирать популярность среди киберпреступников. Европейская ассоциация безопасных транзакций (The European Association for Secure Transactions, EAST) опубликовала отчет об атаках на банкоматы за 2017 год. По сравнению с 2016 годом количество логических атак в Европе увеличилось в три раза, а общая сумма ущерба достигла 1,52 млн евро.

Использовавшееся в первых атаках ВПО Skimer продолжает активно развиваться и по сей день, а наряду с ним появляются все новые семейства вредоносных программ — GreenDispenser, Alice, Ripper, Radpin, Ploutus и др. Эти программы продаются на форумах дарквеба. Они отличаются высокой стоимостью: цены начинаются от 1500 долларов, однако потенциальная прибыль значительно превышает расходы. Приобретенное ВПО может окупиться уже после одного успешного ограбления, при этом разработчики стремятся адаптировать программы под как можно большее число моделей банкоматов. В 2017 году было обнаружено ПО CutletMaker, которое продавалось в свободном доступе вместе с подробной инструкцией по использованию за 5000 долларов.

Необходимо понимать, что главное — это не алгоритм работы программы, а то, каким образом она устанавливается на банкомат. Выявление потенциальных путей заражения и уязвимых компонентов — первый шаг к обеспечению защиты банка и его клиентов. В этом отчете мы поделимся результатами анализа защищенности банкоматов, который мы проводили в 2017–2018 годах, расскажем о возможных вариантах логических атак, выявленных в исследованных устройствах, и дадим рекомендации, как обезопасить банкомат.





## Портрет участников

Для исследования мы выбрали 26 банкоматов, в отношении которых проводились максимально полные проверки в рамках работ по анализу защищенности. Это были банкоматы производства NCR, Diebold Nixdorf и GRGBanking. Каждый банкомат имел уникальную конфигурацию: спектр атак на одну и ту же модель различался в зависимости от типа подключения к процессинговому центру, набора установленного ПО, используемых мер защиты и других специфических параметров. В таблице представлены основные характеристики исследованных банкоматов.

Таблица 1. Конфигурации исследованных банкоматов

Модель банкомата	Версия ОС	Решение класса Application Control	Защита от атак Black Box	Тип подключения к процессинговому центру
GRGBanking H68NL	Windows 10	KXSecurity	Аутентификация и шифрование данных между ОС и диспенсером	Прямое подключение
NCR Personas 6676	Windows XP	McAfee Solidcore	NCR USB Encryption Level 3	Прямое подключение или аппаратный VPN-клиент
NCR SelfServ 5877 (конфигурация 1)	Windows XP	Отсутствует	Отсутствует	Аппаратный VPN-клиент
NCR SelfServ 5877 (конфигурация 2)	Windows XP	McAfee Solidcore	NCR USB Encryption Level 3	Прямое подключение или аппаратный VPN-клиент
NCR SelfServ 6622 (конфигурация 1)	Windows 7	McAfee Solidcore	NCR USB Encryption Level 3	Прямое подключение
NCR SelfServ 6622 (конфигурация 2)	Windows 7	McAfee Solidcore	NCR USB Encryption Level 3	Программный VPN-клиент
NCR SelfServ 6622 (конфигурация 3)	Windows 7	Windows AppLocker	NCR USB Encryption Level 3	Программный VPN-клиент
NCR SelfServ 6622 (конфигурация 4)	Windows 7	Windows AppLocker	NCR USB Encryption Level 3	Программный VPN-клиент
NCR SelfServ 6622 (конфигурация 5)	Windows 7	McAfee Solidcore	NCR USB Encryption Level 3	Прямое подключение
NCR SelfServ 6622 (конфигурация 6)	Windows 7	McAfee Solidcore	NCR USB Encryption Level 3	Программный VPN-клиент
NCR SelfServ 6622 (конфигурация 7)	Windows XP	McAfee Solidcore	NCR USB Encryption Level 3	Программный VPN-клиент
NCR SelfServ 6622 (конфигурация 8)	Windows XP	McAfee Solidcore	NCR USB Encryption Level 3	Прямое подключение или аппаратный VPN-клиент
NCR SelfServ 6632	Windows XP	McAfee Solidcore	NCR USB Encryption Level 3	Аппаратный VPN-клиент
NCR SelfServ 6683	Windows 7	McAfee Solidcore	NCR USB Encryption Level 3	Прямое подключение или аппаратный VPN-клиент
NCR SelfServ 6822	Windows XP	GMV Checker ATM Security	NCR USB Encryption Level 3	Аппаратный VPN-клиент
WN 2000	Windows XP	M3.Defender	Отсутствует	Прямое подключение или аппаратный VPN-клиент
WN 2000XE (конфигурация 1)	Windows XP	M3.Defender	Отсутствует	Прямое подключение или аппаратный VPN-клиент
WN 2000XE (конфигурация 2)	Windows XP	M3.Defender	Cerber Lock	Прямое подключение или аппаратный VPN-клиент
WN 2000XE (конфигурация 3)	Windows XP	SafenSoft	Отсутствует	Прямое подключение или аппаратный VPN-клиент
WN 2000XE (конфигурация 4)	Windows XP	SafenSoft	Wincor USB Encryption	Прямое подключение или аппаратный VPN-клиент
WN 2100XE (конфигурация 1)	Windows XP	Отсутствует	Wincor USB Encryption	Прямое подключение или аппаратный VPN-клиент
WN 2100XE (конфигурация 2)	Windows XP	SafenSoft	Cerber Lock	Прямое подключение или аппаратный VPN-клиент
WN 2100XE (конфигурация 3)	Windows XP	Symantec PC/E Terminal Security	Отсутствует	Прямое подключение или аппаратный VPN-клиент
WN C4040 (конфигурация 1)	Windows 7	M3.Defender	Wincor USB Encryption	Прямое подключение или аппаратный VPN-клиент
WN C4040 (конфигурация 2)	Windows 10	Kaspersky KESS	Wincor USB Encryption	Аппаратный VPN-клиент
WN C4040 (конфигурация 3)	Windows 10	SafenSoft TP Secure	Wincor USB Encryption	Аппаратный VPN-клиент



## Как устроен банкомат

Перед тем как перейти непосредственно к сценариям атак, вкратце разберем, что представляет собой банкомат и какие его компоненты могут стать мишенью преступников.

Банкомат состоит из двух основных частей — сервисной зоны и сейфа. В сервисной зоне расположен системный блок — обычный компьютер, к которому присоединены все остальные устройства, в частности сетевое оборудование, картридер, клавиатура (пинпад) и диспенсер купюр (диспенсер находится в сейфовой части, но шлейф подключения к компьютеру вынесен за ее пределы). Сервисная зона практически никак не защищена от злоумышленников: пластиковая дверка закрыта на простой замок, причем производители обычно устанавливают одинаковые замки на все банкоматы одной серии. Ключ от такого замка легко приобрести в интернете, кроме того злоумышленник может воспользоваться отмычкой или просверлить тонкий пластик. В защищенном сейфе, сделанном уже из прочных материалов (стали и бетона), находятся только диспенсер купюр и модуль для приема наличных.

Компьютер обычно функционирует под управлением ОС Windows, при этом используется версия Embedded, разработанная специально для установки в банкоматах. Доступ к Windows должен быть только у администраторов, а остальные пользователи не должны иметь такого доступа, поэтому были созданы приложения, которые работают в режиме киоска. Такое приложение обеспечивает все необходимые пользователю функции при работе с банкоматом, и именно его интерфейс мы видим, когда пользуемся банкоматами.

Приложению необходимо взаимодействовать с разными периферийными устройствами: получать данные платежной карты от картридера, считывать информацию, введенную пользователем с клавиатуры, обращаться к диспенсеру купюр. Для этих целей был разработан стандарт XFS (eXtension For Financial Services), который упрощает и унифицирует управление оборудованием. Стандарт предполагает наличие менеджера оборудования, который предоставляет API любым Windows-приложениям и перенаправляет запросы устройствам. Обращение к каждому устройству, работающему по стандарту XFS, происходит через соответствующий сервисный провайдер (драйвер устройства). Менеджер оборудования переводит функции API в функции SPI и передает их сервисным провайдерам. Каждый производитель банкоматов имеет собственную реализацию стандарта XFS.

Банкомат никогда не принимает решение о выдаче средств: для обработки каждой транзакции он обращается к процессинговому центру, расположенному в банке. Подключение к центру осуществляется через проводные или беспроводные каналы связи (например, через сотовую связь). Важно, чтобы соединение было защищено от перехвата данных. В целях безопасности чаще всего используются программные и аппаратные VPN-клиенты.

Как правило, обмен данными с процессинговым центром происходит по протоколам NDC или DDC, но банк может использовать и собственные решения. Помимо процессингового центра банкомат также соединен с внутренней сетью банка, откуда осуществляются подключения для удаленного администрирования, и с сервером обновления ПО.

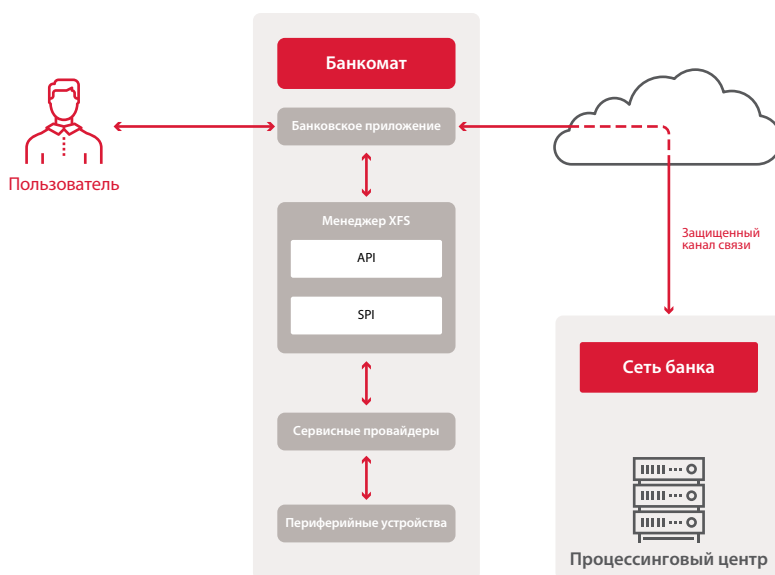


Рисунок 1. Взаимодействие компонентов банкомата

Для преступника интерес представляют встроенный компьютер, сетевое оборудование, а также основные периферийные устройства — картридер и диспенсер. Атаки на эти компоненты позволяют перехватить карточные данные, вмешаться в процесс обработки транзакции процессинговым центром или отправить команду на выдачу купюр диспенсеру. Для проведения атак злоумышленнику нужно получить физический доступ в сервисную зону банкомата либо подключиться к сети, в которой находится банкомат.

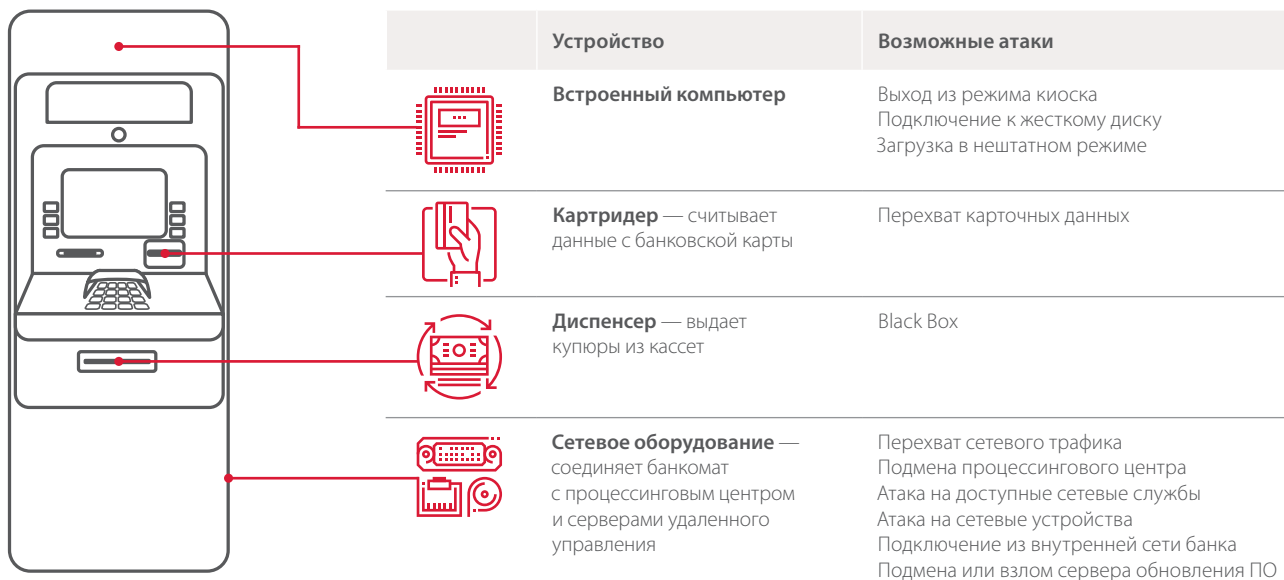


Рисунок 2. Возможные атаки на устройства банкомата

### Типы уязвимостей

Все уязвимости, которые встречаются при анализе защищенности банкоматов, можно разделить на четыре группы:

- недостатки сетевой безопасности,
- недостатки защиты периферийных устройств,
- недостатки конфигурации систем и устройств,
- уязвимости и недостатки конфигурации приложений класса Application Control.



Недостатки сетевой безопасности позволяют злоумышленнику, получившему доступ к сети банкомата, проводить атаки на доступные сетевые службы, перехватывать и подменять трафик, проводить атаки на сетевое оборудование. Такие атаки могут позволить подменить ответы процессингового центра или получить контроль над банкоматом. В исследуемых системах часто выявлялись недостатки межсетевого экранирования и недостаточная защита данных, передаваемых между банкоматом и процессинговым центром.

Недостаточная защита периферийных устройств, например отсутствие аутентификации между периферийным оборудованием и ОС банкомата, позволяет преступнику обращаться к этим устройствам после заражения банкомата вредоносным ПО или напрямую подключать свое оборудование к диспенсеру или картридеру. Это может привести к краже денег или перехвату данных платежных карт.

Под недостатками конфигурации будем понимать те пробелы в защите, которыми злоумышленник может воспользоваться при наличии доступа в сервисную зону, например отсутствие шифрования жесткого диска, ошибки аутентификации, недостаточную защиту от выхода из режима киоска, возможность подключения произвольных устройств.

В отдельную группу вынесены уязвимости, возникшие вследствие установки средств защиты класса Application Control. Такие решения направлены на предотвращение выполнения постороннего кода в системе, однако на проверку зачастую оказываются недостаточно эффективными. Уязвимости могут изначально содержаться в их коде или появиться как результат неправильной конфигурации.

В следующем разделе мы более подробно рассмотрим уязвимости, выявляемые при анализе защищенности, и связанные с ними потенциальные сценарии атак, которые были успешно продемонстрированы в рамках тестирования.

## Сценарии атак

Мы разделили все сценарии на две группы: в первую очередь рассмотрим атаки, которые позволяют похитить деньги из сейфа банкомата, а затем отдельно разберем способы копирования информации с банковских карт пользователей.

### Хищение денег

#### Сетевые атаки

Уязвимы для атаки	Что необходимо	Время на атаку
<b>85%</b> банкоматов	Доступ к сети банкомата	<b>15</b> минут

Для проведения атак на сетевом уровне злоумышленнику прежде всего необходим доступ к сети, к которой подключен банкомат. Если злоумышленник — сотрудник банка или провайдера, то у него есть возможность получить доступ удаленно. В других случаях требуется физическое присутствие, чтобы открыть сервисную зону, отключить Ethernet-кабель от банкомата и подсоединить свое устройство до модема или вместо него. Затем злоумышленник сможет подключиться к этому устройству и проводить атаки на доступные сетевые службы или атаки типа «человек посередине». Иногда модем расположен снаружи банкомата, и для того, чтобы подключиться к сетевому кабелю, не нужно даже иметь доступ к сервисной зоне.

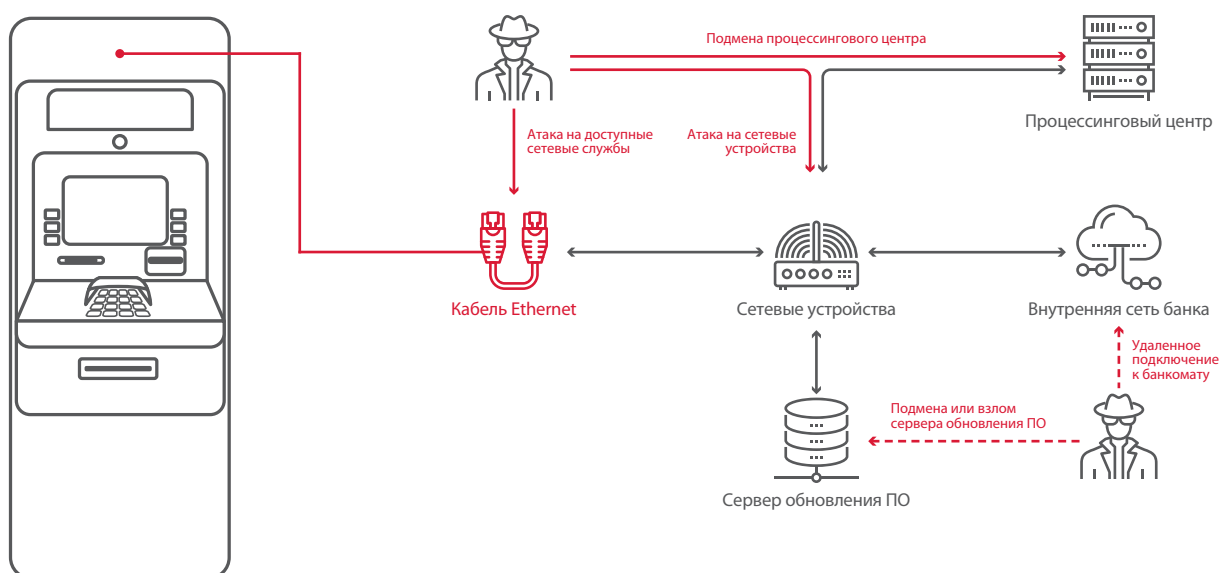


Рисунок 3. Сетевые атаки на банкоматы

Мы не будем рассматривать возможность проведения атак путем взлома банковской инфраструктуры, но если злоумышленник проникнет во внутреннюю сеть банка, он также сможет получить доступ к управлению банкоматами и загрузить на них вредоносное ПО. Так, например, действовала группировка Cobalt. В начале 2018 года мы проводили исследование защищенности банковских информационных систем и выяснили, что несанкционированный доступ к управлению банкоматами возможно получить в каждом четвертом из протестированных банков.

### Подмена процессинга

Если не обеспечивается защита данных, передаваемых между банкоматом и процессинговым центром, злоумышленник может вмешаться в процесс подтверждения транзакции. Для этого используется эмулятор процессингового центра, который одобрит любой запрос, поступивший от банкомата, и в ответ отправит команду на выдачу денег. Эмулятор подключается к кабелю Ethernet в сервисной зоне банкомата или вместо сетевого оборудования.

Атака возможна  
в **27%** банкоматов

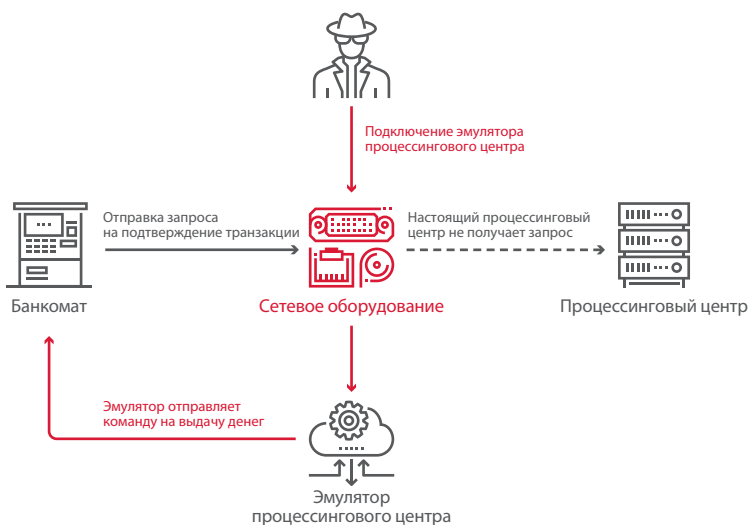


Рисунок 4. Подмена процессингового центра



Подмена процессингового центра возможна, если одновременно выполняются три условия:

- **Отсутствует дополнительное шифрование данных, передаваемых между банкоматом и процессинговым центром.** Поскольку сами по себе протоколы NDC и DDC не предусматривают шифрования данных, злоумышленник может перехватывать и модифицировать информацию.
- **Используются недостаточно эффективные VPN-решения.** Как программные, так и аппаратные VPN-решения в исследованных нами системах можно было отключить. Например, при установке VPN-клиента за пределами сервисной зоны либо при наличии доступа в сервисную зону злоумышленник может подключить собственное оборудование между банкоматом и аппаратной частью VPN-комплекса.
- **Отсутствуют значения Message Authentication Code в транзакционных запросах и ответах,** что позволяет изменять трафик без обнаружения подмены.

В ходе исследований эксперты выявляли и другой сценарий атаки, позволяющий подменить ответы процессингового центра. Атака типа «человек посередине» ARP Spoofing — внесение изменений в ARP-таблицы путем отправки ложных сообщений ARP Response — используется для перенаправления трафика через оборудование злоумышленника. Если трафик не шифруется, то злоумышленник может изменить содержание ответа, например увеличить количество выдаваемых купюр.

```
Scanning for merged targets (2 hosts)...
* |=====| 100.00 %
2 hosts added to the hosts list...
ARP poisoning victims:
GROUP 1 : 192.168.13.1 E0:CB:4E:48:E6:B1
GROUP 2 : 192.168.13.105 00:1A:D4:21:45:4A
```

Рисунок 5. Демонстрация атаки ARP Poisoning



Рисунок 6. Подмена ответа от процессингового центра (выдача одной купюры)

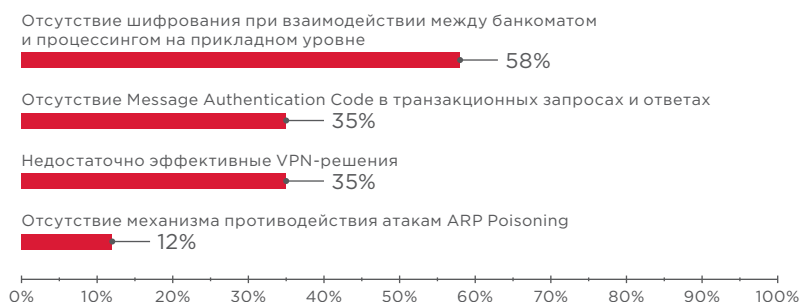


Рисунок 7. Выявленные уязвимости (доля уязвимых банкоматов)



Атака возможна  
в **58%** банкоматов

### Эксплуатация уязвимостей в доступных сетевых службах

Злоумышленник может воспользоваться уязвимостями в доступных сетевых службах, в том числе в службах удаленного управления, и получить возможность выполнять произвольные команды. В результате он сможет отключить защитные механизмы и управлять выдачей денег из диспенсера.

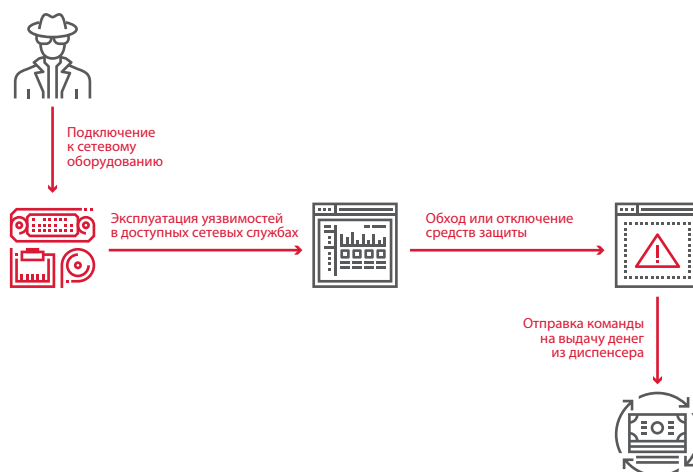


Рисунок 8. Эксплуатация уязвимостей в доступных сетевых службах

Уязвимости, позволяющие осуществить такой вектор атаки, связаны с недостатками межсетевого экранирования, использованием уязвимых или устаревших версий ПО (например, были обнаружены уязвимости [CVE-2017-8464](#) и [CVE-2018-1038](#), которые позволяют удаленно выполнить произвольный код, а затем повысить привилегии в системе), а также с некорректной конфигурацией средств защиты (как правило, использовался ошибочный подход к построению списка доверенных приложений).

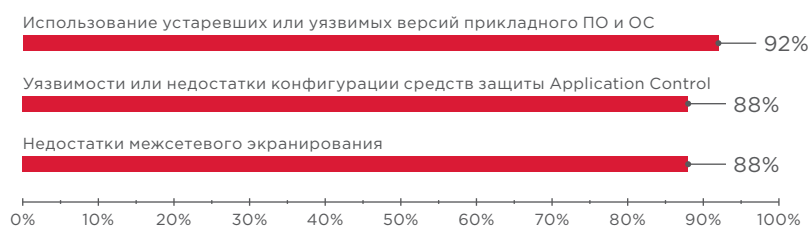


Рисунок 9. Выявленные уязвимости (доля уязвимых банкоматов)

### Атаки на сетевые устройства

Атака возможна  
в **23%** банкоматов

Существует еще один способ получения доступа к сети — атака непосредственно на сетевые устройства, к которым подключен банкомат. Преступники, получившие контроль над оборудованием, могут распространить атаку на другие банкоматы, входящие в данную сеть, и даже более того — проникнуть в инфраструктуру банка.

Приведем пример, который встретился в одном из проектов по анализу защищенности. Эксперты анализировали прошивку GSM-модема, используемого для создания сети передачи данных. Сеть служит для работы с процессингом, передачи видеоматериалов, оповещения о событиях, а также для подключения к банкоматам удаленно. Узлы, входящие в сеть, могут обращаться друг к другу при помощи особого протокола, в котором предусмотрены разные служебные сообщения: например, для получения информации об узлах, чтения конфигурационных файлов, а также для выполнения команд ОС.

Обмен сообщениями шифруется с использованием сеансового ключа, который формируется на основе ключа узла. Ключ узла, в свою очередь, зашифрован на основе другого ключа, который хранится в прошивке модема. Если у злоумышленника есть физический доступ к модему, он может считать прошивку, используя специальное аппаратное и программное обеспечение. В ходе исследования эксперты извлекли ключ из прошивки и подключились к сети.

В конфигурационных файлах узлов, находящихся в сети передачи данных, были обнаружены адреса серверов во внутренней сети банка. Эти серверы были доступны из рассматриваемой сети и поддерживали упомянутый протокол обмена сообщениями, в том числе и выполнение команд ОС. Таким образом, обладая ключом из прошивки модема, злоумышленник смог бы получить контроль над внутренней инфраструктурой банка. В рамках тестирования атаку удалось развить до получения доступа к платежным шлюзам, базам данных и серверам с видеоматериалами.

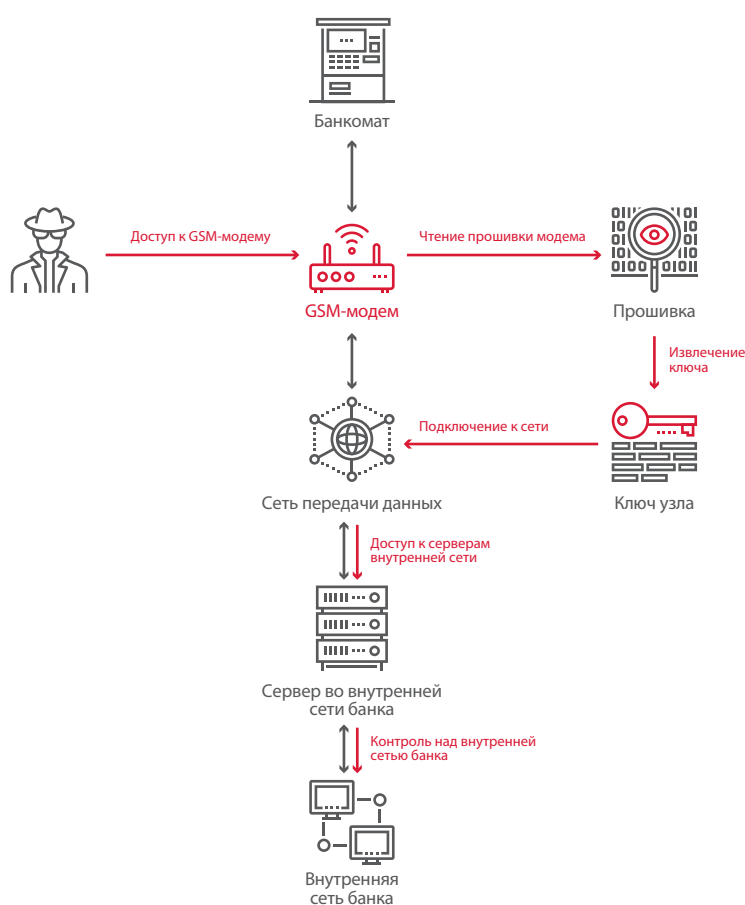


Рисунок 10. Сценарий атаки на GSM-модем

В другом проекте потенциальный вектор атаки был связан с тем, что после установки GSM-модема остались открытыми сетевые интерфейсы удаленного управления, и при этом использовались стандартные учетные записи.

Экспертам удалось подключить GSM-модем к собственной поддельной базовой станции. После этого были обнаружены два открытых сетевых интерфейса: Telnet и веб-интерфейс администрирования. На устройстве использовалась словарная учетная запись администратора root:root, благодаря чему был получен доступ к модему с максимальными привилегиями по протоколу Telnet. Словарные учетные данные были подобраны и для авторизации в веб-интерфейсе. Злоумышленник мог бы перенаправить сетевой трафик на свое устройство, перехватывать любые запросы и подменять ответы процессингового центра.

## Рекомендации

1. Размещать сетевое оборудование в пределах сервисной зоны банкомата.
2. Использовать программный или аппаратный VPN-клиент, размещаемый в сервисной зоне банкомата.
3. Обеспечить надежное шифрование данных, передаваемых между банкоматом и процессинговым центром.
4. Включить добавление Message Authentication Code ко всем транзакционным запросам и ответам.
5. Обеспечить защиту или отключить неиспользуемые протоколы канального и сетевого уровней.
6. Настроить межсетевой экран, разрешив удаленное подключение только к необходимым для работы банкомата сервисам. Не оставлять открытыми сетевые интерфейсы, необходимость доступа к которым отсутствует. Удаленное подключение должно быть разрешено только с определенных адресов администраторов.
7. Использовать стойкие пароли для подключения к интерфейсам удаленного управления.
8. Регулярно обновлять используемые ОС и прикладное ПО до актуальных версий.
9. Вести регистрацию и мониторинг событий безопасности.

## Black Box

Уязвимы для атаки	Что необходимо	Время на атаку
<b>69%</b> банкоматов	Физический доступ в сервисную зону	<b>10</b> минут

Как мы уже знаем, диспенсер купюр находится в хорошо защищенном сейфе. Однако ко встроенному компьютеру он подключен в сервисной зоне, открыть которую не составляет труда. Также были зафиксированы случаи, когда злоумышленники просверливали отверстия в лицевой панели банкомата, чтобы добраться до кабеля диспенсера. Получив доступ к кабелю, злоумышленник может напрямую подключить диспенсер к своему устройству, запрограммированному для отправки команд на выдачу купюр. Такое устройство, как правило, представляет собой одноплатный микрокомпьютер, например на базе Raspberry Pi, а в качестве ПО используются модифицированные утилиты для диагностики работы банкомата. Обычно в диагностических утилитах заложены проверки для подтверждения легитимности доступа, но злоумышленники могут взломать их и отключить любые механизмы безопасности. Атаки такого типа получили название Black Box.

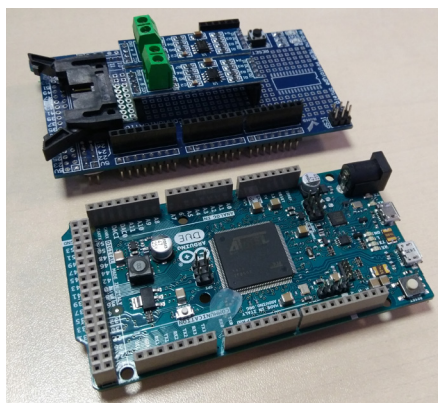


Рисунок 11. Компоненты устройства Black Box

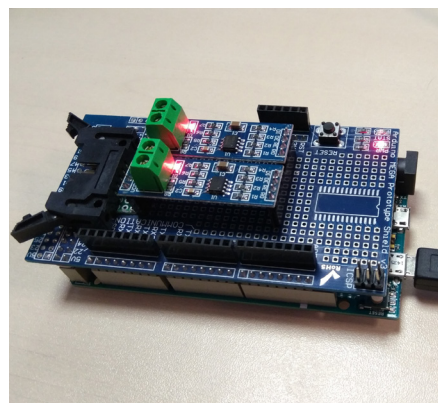


Рисунок 12. Устройство Black Box

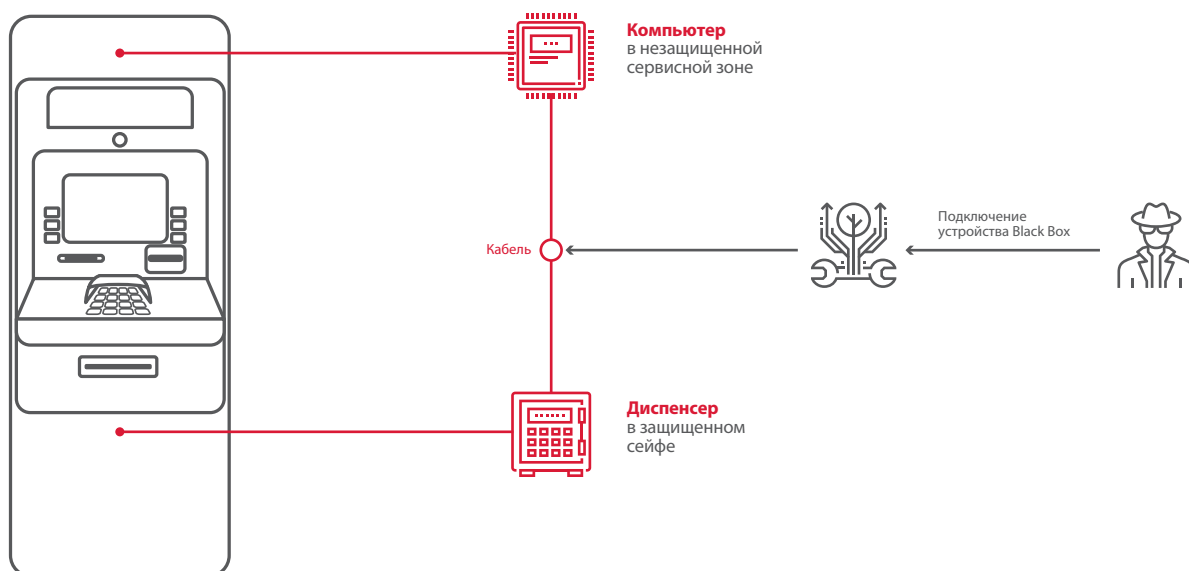


Рисунок 13. Атака Black Box

Чтобы предотвратить атаки Black Box, производители банкоматов рекомендуют использовать актуальные версии платформ XFS, обеспечивающие надежное шифрование и поддерживающие физическую аутентификацию между ОС и диспенсером. Физическая аутентификация предполагает, что ключи шифрования будут передаваться только в том случае, если будет подтвержден легальный доступ к сейфу. Однако преступники учатся обходить сложные меры защиты — так, во время недавних атак в Мексике им удалось эмулировать физическую аутентификацию при помощи эндоскопа.

Шифрование не всегда реализовано эффективно, даже если на банкомате установлено актуальное ПО. Например, в 2018 году в платформе APTRA XFS компании NCR эксперты Positive Technologies обнаружили уязвимости, позволяющие установить на контроллер диспенсера модифицированную версию прошивки и обойти физическую аутентификацию.

Недостаточно надежная система защиты NCR использовалась в половине исследованных банкоматов. Еще в 19% банкоматов вовсе отсутствовали какие-либо меры защиты от атак Black Box.

### Рекомендации

1. Использовать физическую аутентификацию между ОС и диспенсером для подтверждения легального доступа к сейфу.
2. Обеспечить шифрование данных между ОС банкомата и диспенсером.
3. Использовать актуальные версии ПО и своевременно устанавливать обновления.
4. Вести регистрацию и мониторинг событий безопасности.
5. В качестве компенсационного механизма использовать внешние устройства (например, Cerber Lock, ATM Keeper), обеспечивающие защиту от несанкционированного подключения к диспенсеру.





## Выход из режима киоска

Уязвимы для атаки

Что необходимо

Время на атаку

**76%**  
банкоматов

Физический доступ  
в сервисную зону

**15**  
минут

Предполагается, что пользователь взаимодействует лишь с одним приложением, которое отображает информацию на экране банкомата и обрабатывает полученные от пользователя данные. Это приложение работает в режиме киоска, то есть возможности пользователя ограничены: он не может запускать посторонние программы и вообще каким-либо образом работать с ОС. Выход из режима киоска — это атака, целью которой является обход установленных ограничений и выполнение команд в ОС банкомата.



Рисунок 14. Подключение устройства злоумышленника

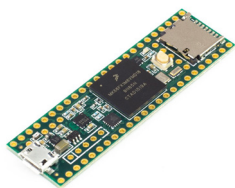


Рисунок 15. Платформа Teensy

Потенциальный сценарий атаки выглядит следующим образом:

1. Злоумышленник подключает к USB- или PS/2-интерфейсу банкомата устройство для эмуляции клавиатуры и ввода информации пользователем, например на базе Raspberry Pi, Teensy или BeagleBone. На следующей стадии атаку можно полностью автоматизировать или подключиться к этому устройству удаленно.
2. Далее злоумышленник получает доступ к ОС. Во всех случаях сделать это удалось с помощью горячих клавиш, поскольку ограничения на ввод информации либо отсутствовали, либо предусматривали не все возможные сочетания.
3. Заключительный шаг — обход средств защиты, направленных на предотвращение выполнения постороннего кода, и получение возможности отправить команду диспенсеру.

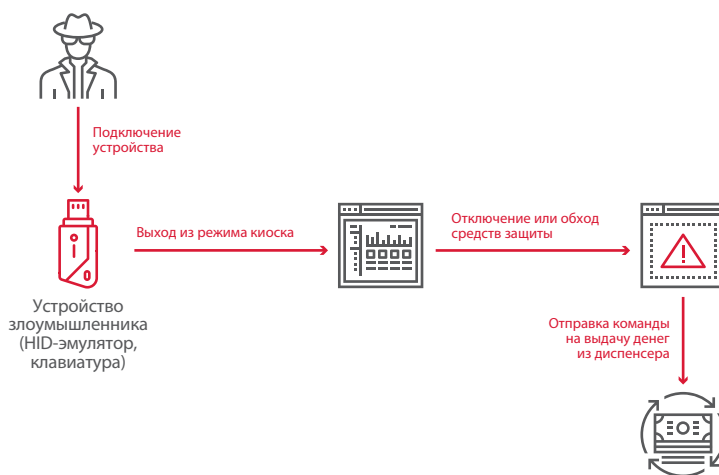


Рисунок 16. Сценарий атаки «Выход из режима киоска»

## Выявленные уязвимости

В исследуемых системах были выявлены ошибки конфигурации, связанные главным образом с недостаточным ограничением прав пользовательской учетной записи, а также уязвимости в средствах защиты Application Control.



Рисунок 17. Выявленные уязвимости (доля уязвимых банкоматов)

В большинстве банкоматов можно было свободно подключать посторонние устройства к интерфейсам USB и PS/2. Это позволяет злоумышленнику подключить клавиатуру или другое устройство, имитирующее пользовательский ввод.

Необходимо исключить возможность ввода произвольной информации, в частности предусмотреть запрет некоторых сочетаний клавиш, которые могут быть использованы для обхода режима киоска и получения доступа к функциям ОС. В этих целях в большинстве банкоматов применялось специальное ПО для выборочного отключения клавиш. Тем не менее в 85% случаев были доступны стандартные сочетания, например Alt+F4 для закрытия активного окна или Win+Ctrl, Alt+Tab, Alt+Shift+Tab для переключения задач. Это позволяло не только закрыть окно основного банковского приложения, но и отключить сами приложения, блокирующие ввод произвольных символов с клавиатуры.

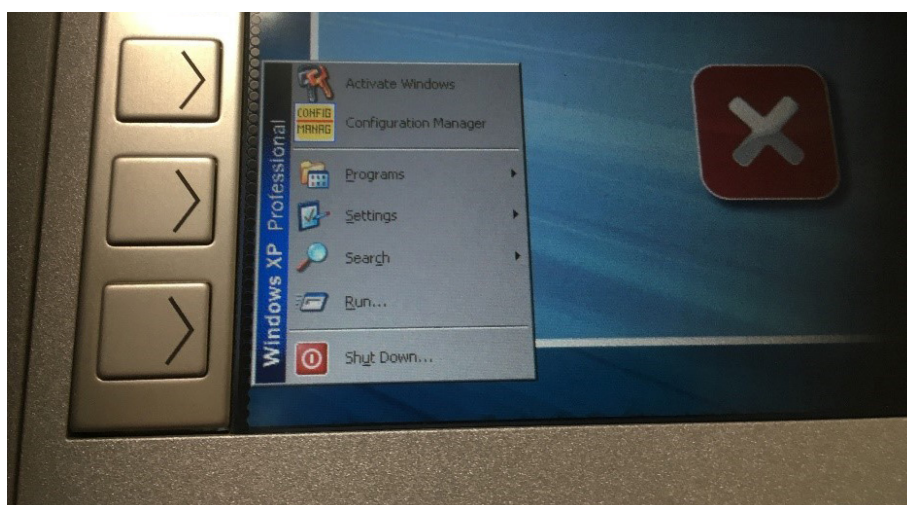


Рисунок 18. Выход из режима киоска при помощи «горячих клавиш»

Уязвимости, позволяющие обойти режим киоска, могут содержаться и в ПО, установленном для дополнительной защиты. Так, в двух банкоматах использовалось ПО для видеозаписи и мониторинга событий безопасности. Окно приложения было скрыто, однако во время исследования выяснилось, что оно открывается при наведении курсора мыши на угол экрана монитора. В приложении присутствовала функция редактирования файлов, через которую можно было получить доступ к приложению «Проводник» ОС Windows, а затем — к любому ПО на компьютере, например Internet Explorer, FAR Manager.

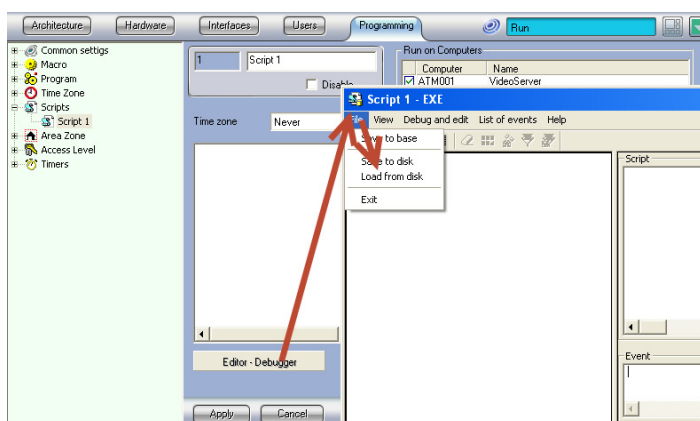


Рисунок 19. Выход из режима киоска в ПО «Интеллект»

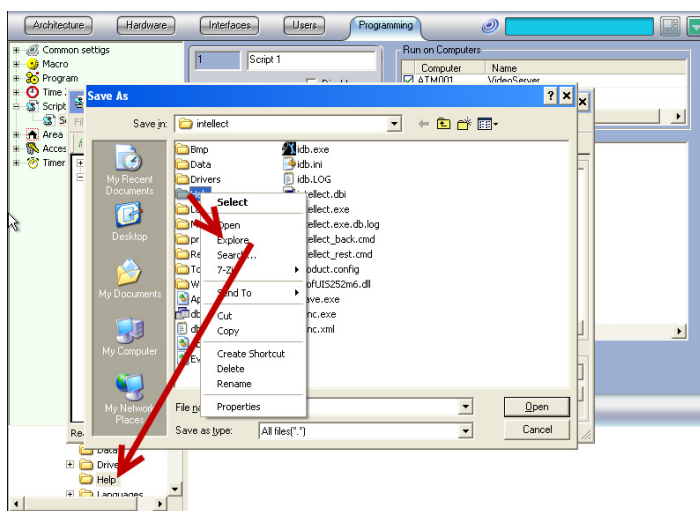


Рисунок 20. Выход из режима киоска в ПО «Интеллект»

Локальные политики безопасности должны быть настроены таким образом, чтобы пользователь не имел возможности читать или записывать файлы и запускать произвольные программы. В большинстве исследуемых систем локальные политики безопасности были настроены некорректно или вовсе отсутствовали.

В 92% исследованных банкоматов применялись решения класса Application Control, которые предотвращают выполнение постороннего кода, разрешая запуск только определенных приложений. Основной недостаток конфигурации таких решений заключался в принципе построения белого списка: доверенным считалось любое ПО, которое присутствовало в системе на момент установки средства защиты, включая и те приложения, которые не были необходимы для работы банкомата. Следовательно, появлялась возможность воспользоваться уязвимостями в доверенном ПО и выполнить произвольный код, а также отключить защиту. Помимо этого, были обнаружены уязвимости и в самих средствах защиты, в том числе уязвимости нулевого дня.



### Уязвимости нулевого дня

В ходе исследований наши эксперты выявляют уязвимости нулевого дня в решениях класса Application Control, например в [GMV Checker ATM Security](#), [Kaspersky Embedded Systems Security](#), [McAfee Application Control \(Solidcore\)](#). В 2018 году эксперты Positive Technologies выявили три уязвимости в решении [SafenSoft SoftControl](#): CVE-2018-13014, CVE-2018-13013 и CVE-2018-13012.

Уязвимость CVE-2018-13014 дает возможность получить пароль для доступа к параметрам конфигурации. Пароль хранился в открытом виде в базе данных, которая находилась в каталоге, доступном обычному пользователю. В результате злоумышленник мог изменять параметры SafenSoft, например полностью отключить защиту на компьютере.

Имея пароль для доступа к параметрам, злоумышленник может эксплуатировать вторую уязвимость, CVE-2018-13013. Она связана с неправильной проверкой запуска файла msixexec.exe, который используется для установки ПО. Злоумышленник может создать конфигурацию, в которой не осуществляется проверка сигнатур установочных файлов с расширением .msi и запустить произвольный MSI-файл.

Третья уязвимость, CVE-2018-13012, связана с процессом обновления ПО. SafenSoft загружает конфигурационный файл и файлы обновлений по незащищенному протоколу HTTP. Поскольку проверка целостности не осуществляется, злоумышленник может провести атаку «человек посередине» и подменить файлы обновлений на вредоносные приложения.

### Рекомендации

1. Ограничивать возможность подключения посторонних устройств с помощью локальных политик ОС или средств защиты класса Device Control.
2. Отключить стандартные сочетания клавиш, позволяющие получить доступ к функциям ОС.
3. Использовать принцип наименьших привилегий при настройке прав учетной записи пользователя. Ограничить возможность редактирования файлов, значений реестра и запуска произвольных программ.
4. Удалить ПО, которое не является необходимым для работы банкомата. Если удалить ПО невозможно, следует использовать средства защиты, ограничивающие его работу.
5. При построении белого списка доверенных приложений не включать в него встроенные сервисы ОС, необязательные для ее функционирования, а также иные приложения, не предназначенные для работы банкомата.
6. Обеспечить эксклюзивное открытие логических устройств. Взаимодействовать с производителем для изменения API и поддержки авторизации доступа к устройствам.
7. Использовать актуальные версии ПО и своевременно устанавливать обновления.
8. Вести регистрацию и мониторинг событий безопасности.



## Подключение к жесткому диску

Уязвимы для атаки

Что необходимо

Время на атаку

**92%**  
банкоматов

Физический доступ  
в сервисную зону

**20**  
минут

Обойти установленные средства защиты и получить контроль над диспенсером возможно при подключении к жесткому диску банкомата. Рассмотрим потенциальные сценарии атак.



Рисунок 21. Подключение к жесткому диску

### Прямой доступ к жесткому диску

Атака возможна  
в **92%** банкоматов

Самый простой способ — напрямую подключиться к жесткому диску. Если содержимое диска не зашифровано, злоумышленник может записать на него вредоносную программу, содержащую команды для взаимодействия с диспенсером. Затем эту программу необходимо добавить в белый список приложения Application Control — для этого достаточно внести изменения в конфигурационные файлы. Далее при загрузке банкомата в рабочем («защищенном») режиме защитное ПО запустится и будет функционировать, но нарушитель сможет выполнить произвольный код с использованием вредоносного ПО. Злоумышленник может и вовсе отключить средства защиты, например удалить файлы с диска.

Кроме того, злоумышленник может похитить чувствительную информацию с диска, например скопировать отдельное приложение или полный образ диска, а затем использовать модифицированные версии для дальнейших атак.

### Загрузка с внешнего носителя

Атака возможна  
в **27%** банкоматов

Злоумышленник может произвести загрузку с внешнего носителя и получить доступ к файловой системе. Порядок загрузки установлен в параметрах BIOS, которые должны быть защищены паролем. Однако в 23% банкоматов пароль для доступа к BIOS был предсказуемым, а в 8% не требовался вовсе. В одном случае не удавалось подобрать пароль администратора, но для доступа с пользовательскими привилегиями пароль не требовался, при этом пользователь мог изменять порядок загрузки. Еще в одном банкомате была доступна загрузка ОС по сети с использованием Intel Boot Agent в обход приоритетов загрузки BIOS.

Загрузившись со своего носителя, злоумышленник получает возможность подключить оригинальный жесткий диск и продолжить атаку теми же способами, как и в случае прямого подключения к диску. На рисунке ниже продемонстрировано переименование драйвера McAfee Solidcore for APTRA, содержащегося на жестком диске банкомата, после загрузки ОС с внешнего носителя. В результате ПО McAfee Solidcore не будет запущено при загрузке банкомата в рабочем режиме.



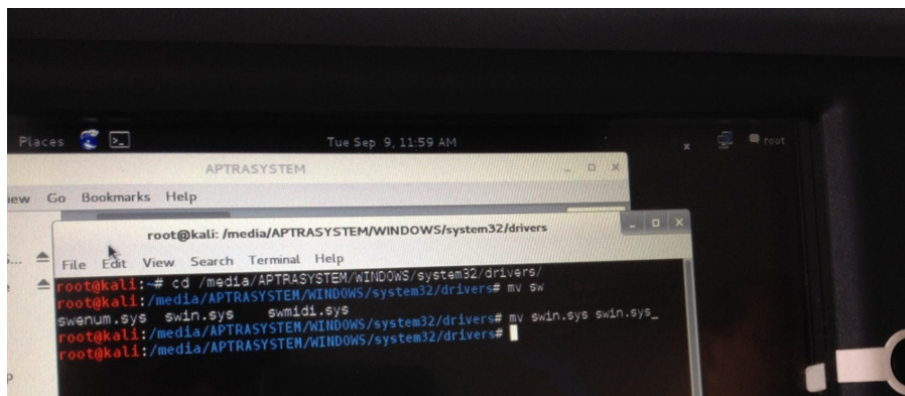


Рисунок 22. Переименование драйвера McAfee Solidcore for APTRA

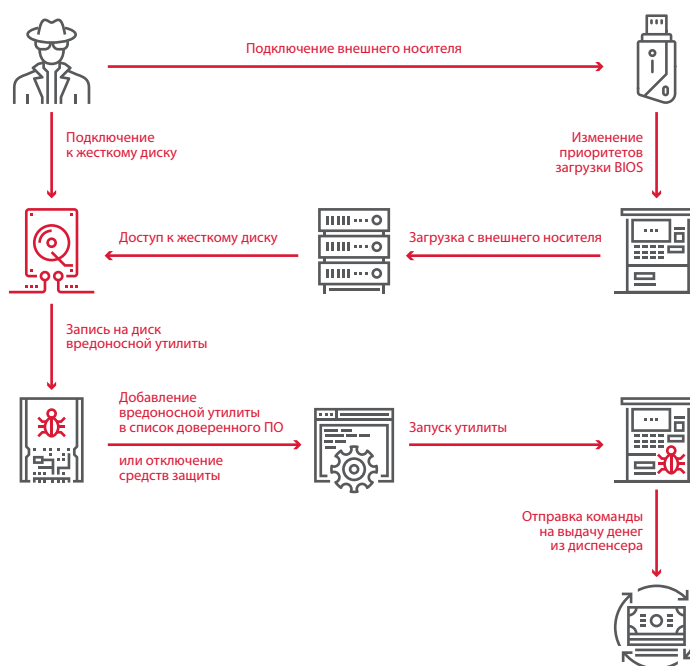


Рисунок 23. Подключение к жесткому диску для записи вредоносного ПО

### Выявленные уязвимости

Уязвимости, которые позволяют получить доступ к файловой системе жесткого диска, связаны с недостатками аутентификации при доступе к BIOS и отсутствием шифрования диска. Взаимодействие вредоносной программы с диспенсером купюр возможно из-за недостаточной защиты периферийных устройств — отсутствия аутентификации и шифрования между ОС и устройствами.

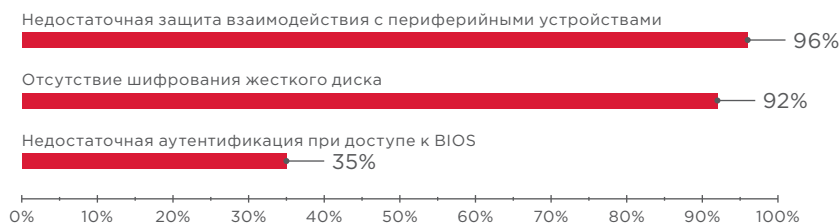


Рисунок 24. Выявленные уязвимости (доля уязвимых банкоматов)



Семейство вредоносных программ Ploutus известно с 2013 года. Первые атаки с использованием Ploutus были зарегистрированы в Латинской Америке, но на текущий момент различные вариации программы обнаруживаются по всему миру. Общий ущерб от этих атак превышает 450 млн долларов.

Для заражения банкоматов преступники прибегают к различным методам, в том числе и к непосредственной записи на жесткий диск. Злоумышленники вытаскивают жесткий диск из банкомата, подключают его к своему компьютеру и записывают вредоносную программу, после чего возвращают диск на место.

### Рекомендации

1. Использовать шифрование жесткого диска. Один из основных производителей банкоматов компания NCR имеет свой набор рекомендаций по организации эффективной схемы шифрования. В частности, производитель указывает на необходимость передавать ключи по сети, а не хранить их локально.
2. Обеспечить строгую аутентификацию при доступе к BIOS.
3. Использовать UEFI вместо BIOS для обеспечения контроля целостности загружаемой области памяти.
4. Разрешить загрузку только с жесткого диска банкомата. Запретить загрузку с внешних носителей или по сети.

### Загрузка в штатном режиме

Уязвимы для атаки	Что необходимо	Время на атаку
<b>42%</b> банкоматов	Физический доступ в сервисную зону	<b>15</b> минут

При загрузке ОС банкомата в одном из специальных режимов появляется возможность обойти установленные средства защиты. В исследуемых банкоматах были доступны следующие варианты загрузки:

- режим отладки ядра;
- режим восстановления Directory Service Restore Mode;
- безопасные режимы («Безопасный режим», «Безопасный режим с загрузкой сетевых драйверов», «Безопасный режим с поддержкой командной строки»).

В этих режимах отключаются некоторые сервисы и средства защиты, а значит — появляется возможность выйти из режима киоска. При загрузке в режиме отладки и подключении к COM-портам злоумышленник может получить полный контроль над банкоматом, используя утилиту WinDbg.

Возможность выбора вариантов загрузки была обнаружена в 88% банкоматов, при этом в рамках тестирования удалось развить атаку вплоть до вывода денег в 42% случаев.



Рисунок 25. Развитие атаки после загрузки в нештатном режиме

### Рекомендации

1. Отключить возможность выбора режима загрузки из загрузчика ОС Windows.
2. Отключить доступ к режиму отладки по COM/USB-интерфейсам, а также по сети.

## Перехват карточных данных

Уязвимы для атаки	Что необходимо	Время на атаку
<b>100%</b> банкоматов	Физический доступ в сервисную зону или доступ к сети банкомата	<b>15</b> минут

На банковской карте присутствует магнитная полоса, которая содержит информацию, необходимую для проведения операций. На этой полосе может быть записано до трех дорожек, но чаще используются только две — Track1 и Track2. На дорожке Track1 хранятся номер карты, дата окончания срока действия, сервисный код, имя владельца, а также могут находиться дополнительные значения PIN Verification Key Indicator, PIN Verification Value, Card Verification Value. Track2 дублирует информацию на Track1 за исключением имени владельца.

Для осуществления платежей с помощью магнитной полосы через POS-терминал или снятия наличных в банкомате устройству необходимо считать только вторую дорожку. Поэтому атака заключается в копировании информации, записанной на Track2. Эти данные используются для изготовления дубликатов карт, и преступники могут продать их в дарквебе. На теневом рынке дампы банковских карт составляют четверть всей продаваемой информации, а средняя стоимость одной карты — 9 долларов.

Долгое время преступники использовали физические наклейки на картридере — скиммеры, которые считывали информацию непосредственно с магнитной полосы. На сегодняшний день банки уже научились защищаться от таких атак и повсеместно устанавливают средства антискимминга. Тем не менее похитить данные можно и без использования накладных скиммеров. Перехват возможен в двух случаях:

- во время передачи данных между банкоматом и процессинговым центром;
- во время передачи данных между ОС банкомата и картридером.

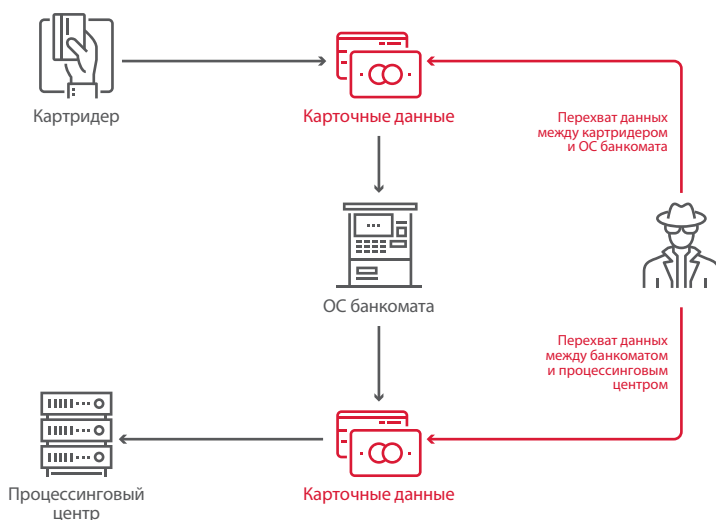


Рисунок 26. Варианты атак, направленных на перехват карточных данных

Кратко рассмотрим сценарии атак. Они схожи с теми, что мы разбирали ранее, и основаны на отсутствии шифрования передаваемых данных и аутентификации между устройствами.

### Перехват данных, передаваемых между банкоматом и процессинговым центром

В данном случае атака возможна из-за передачи полного значения Track2 в открытом виде и отсутствия шифрования при взаимодействии между банкоматом и процессингом на прикладном уровне, поскольку практически во всех банкоматах используются протоколы NDC и DDC, не предусматривающие шифрования данных. Подключившись к сети банкомата и прослушивая сетевой трафик, злоумышленник получает информацию о платежных картах.

Атака возможна  
в **58%** банкоматов

#### Wireshark · Follow TCP Stream (tcp.stream eq 0)

```
00000000 00
00000001 01 60 31 31 1c 30 30 32 1c 1c 1c 31 3a 1c 3b 34 .`11.002 ...1:.;4
00000011 38 3d 8
00000021 31 38 30 38 32 30 31 32 34 38 31 33 30 30 30 30 18082012 48130000
00000031 30 35 33 30 3f 1c 1c 41 41 20 20 20 20 20 20 1c 0530?...A A .
```

Рисунок 27. Перехват данных Track2 в открытом виде

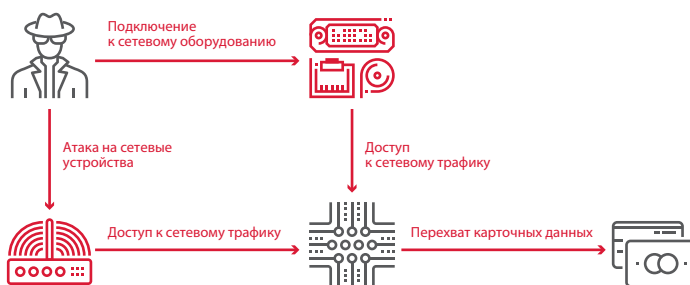


Рисунок 28. Перехват данных между банкоматом и процессинговым центром



Атака возможна  
в **100%** банкоматов

### Перехват данных, передаваемых между ОС и картридером, по USB или COM

В ходе этой атаки между системным блоком банкомата и картридером подключается устройство, которое перехватывает содержимое дорожек магнитной полосы платежных карт. Подобные атаки возможны из-за отсутствия аутентификации и шифрования данных при взаимодействии с картридером и передачи данных карты в открытом виде. Эти недостатки были обнаружены во всех исследуемых банкоматах.

### Перехват данных, передаваемых между ОС и картридером, с использованием вредоносного ПО

Чтение данных из картридера может осуществляться и без использования аппаратного устройства, однако в этом случае злоумышленнику необходимо установить на банкомат свою вредоносную программу. Это можно сделать любым из перечисленных в этом отчете способов: путем загрузки во внештатном режиме или с внешнего носителя, через прямое подключение к жесткому диску, с помощью устройства для эмуляции пользовательского ввода или в результате сетевой атаки.

Во всех банкоматах отсутствовала аутентификация при обмене данными с картридером, а значит, к картридеру могло обратиться любое устройство. Проведение атаки ограничивается лишь возможностью выполнения вредоносного кода в ОС банкомата.



Рисунок 29. Перехват данных между картридером и ОС банкомата



Вредоносная программа Skimer, известная с 2009 года, продолжает активно развиваться. В 2016 году была обнаружена новая версия Skimer, которая способна похищать данные платежных карт, включая PIN-коды. Преступники устанавливали ВПО через внутреннюю сеть банка или при физическом доступе к банкомату. Зараженный банкомат мог месяцами собирать данные, не вызывая никаких подозрений. Затем преступники забирали собранную информацию. Злоумышленник подходил к банкомату, вставлял специальную карту и вводил сессионный ключ для активации ВПО, после чего Skimer мог записать все данные на карту или распечатать на бумаге для чеков. Помимо Skimer известны и другие программы, используемые для кражи данных банковских карт, например Ripper и Suceful.

В 2016 году в Японии злоумышленники за три часа сняли с поддельных банковских карт 12,7 млн долларов. В августе 2018 года похожей атаке подвергся индийский Cosmos Bank: преступники похитили более 11 млн долларов, используя клонированные карты.





## Рекомендации

1. Применять шифрование при обмене данными с картридером и не передавать полное значение магнитной полосы Track2 в открытом виде.
2. Следовать приведенным в нашем отчете рекомендациям по противодействию атакам, направленным на выполнение произвольного кода в ОС банкомата.
3. Следовать приведенным в отчете рекомендациям по противодействию сетевым атакам, направленным на перехват трафика между банкоматом и процессинговым центром.

## Заключение

Логические атаки на банкоматы год от года набирают популярность, а ущерб от них исчисляется миллионами долларов. В первую очередь эти атаки направлены на владельцев банкоматов, однако могут затронуть и клиентов банка — в том случае если злоумышленникам удастся скопировать информацию с платежных карт. При проведении работ по анализу защищенности мы выявляем уязвимости, связанные с сетевой безопасностью, недостатками конфигурации, недостаточной защитой периферийных устройств. В совокупности эти недостатки позволяют злоумышленникам похитить деньги из банкомата или перехватить данные банковских карт. При этом используемые механизмы безопасности не являются серьезным препятствием для реализации атак: почти во всех случаях была выявлена возможность обхода установленных средств защиты. Обычно банки используют одну и ту же конфигурацию на множестве банкоматов, поэтому успешная атака на один банкомат позволяет преступникам провести целую серию аналогичных атак с использованием того же сценария.

Рекомендации, приведенные в данном отчете, направлены на противодействие различным видам логических атак, следование этим правилам позволит повысить уровень защищенности банкоматов. Для того чтобы снизить риск атак, необходимо в первую очередь уделить внимание физической защите сервисной зоны, так как доступ ко встроенному компьютеру и точкам подключения периферийного оборудования является необходимым условием для эксплуатации большей части обнаруженных уязвимостей. Необходимо вести регистрацию и мониторинг событий безопасности: это позволит вовремя реагировать на возникающие угрозы. Помимо этого, важно регулярно проводить анализ защищенности банкоматов, чтобы своевременно выявлять и устранять существующие уязвимости. Анализ защищенности может дополнительно включать в себя исследование (реверс-инжиниринг) используемого ПО, в частности решений класса Application Control, ПО для работы с XFS, прошивок сетевого оборудования. Такие исследования показывают высокую эффективность, поскольку позволяют выявить уязвимости нулевого дня и обеспечить защиту от новых, неизвестных ранее векторов атак.

## О компании

ptsecurity.com  
pt@ptsecurity.com  
facebook.com/PositiveTechnologies  
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.