Способы несанкционированного снятия наличных из банкоматов, виды атак и способы защиты

Докладчики:

Заместитель директора ОАО «КР и СО» **Алексей Зякун**

Технический директор ОАО «КР и СО» **Владимир Кормин**

16 марта 2017

Санкт-Петербург

Цель презентации

- Информирование членов Ассоциации Банков Северо-Запада о новых способах «интеллектуального» взлома банкоматов
- Сравнение различных способов защиты, представленных на рынке

Разработки специалистов ОАО «КР и СО»

Начиная с 1998 г специалисты ОАО «КР и СО» принимали участие в следующих проектах:

- 2002г - Pentium IV upgrade для банкоматов NCR (CCPB адаптер)
- 2006г - Диагностическая система ATMdesk
- 2008г - SDC EPP клавиатура для банкоматов NCR
- 2008г - SDC карт-ридер для банкоматов NCR
- 2010г - Банкомат LG NSYS, подключение к российским процессингам
- 2016г - Устройство защиты банкоматов от кибератак ATM Keeper

Jackpotting

- Три года назад банки не задумывались о возможности прямой выдачи наличных средств из защищенных сейфов – за последние три года ситуация в корне поменялась.
- В данной презентации рассматриваются как существующие методы атак, так и варианты которые могут возникнуть в обозримом будущем
- Проблемы описываемые в данной презентации касаются банкоматов всех производителей

Виды атак

Физическая атака

- Блокировка выдачи (захват)
- Захват карты
- Хищение банкомата
- Взлом сейфа

Мошенничество

- Частичное взятие наличных
- Хищение данных карт
- Хищение банкомата
- Скимминг

Кибератака

- Blackbox
- Вирусы
- Утилиты прямой выдачи

Виды кибератак #1

Программно-аппаратные

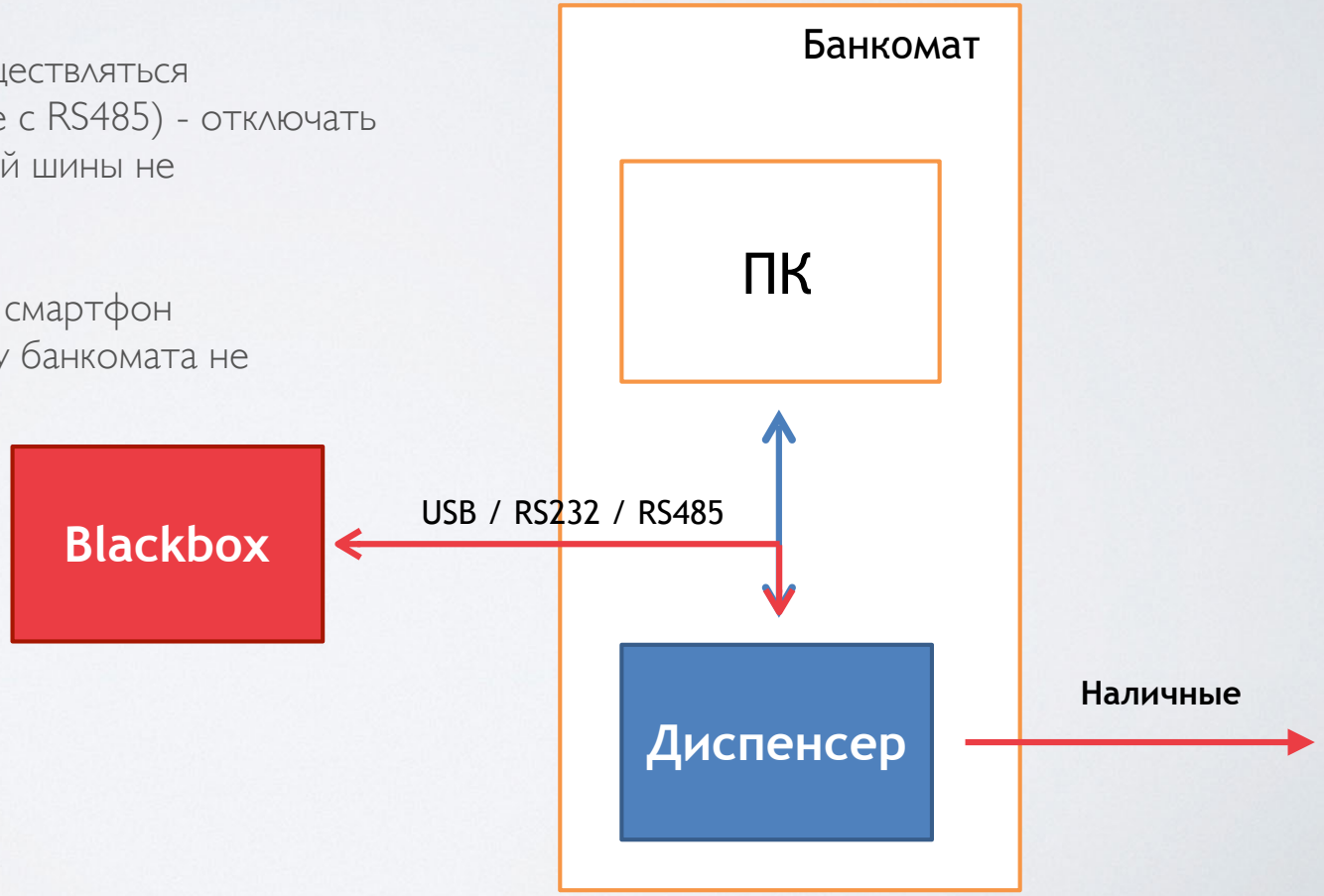
- **Blackbox**
- Main In The Middle
- Virtual Host
- Dispenser Switch Manipulation

Программные

- Malware
- Fileless
- Command prompt

Схема blackbox атаки

- Blackbox - RS232/RS485/USB контроллер + Программное обеспечение для управления диспенсером
- Управление диспенсером может осуществляться параллельно с ПК банкомата (в случае с RS485) - отключать системный блок от коммуникационной шины не обязательно
- В качестве blackbox может выступать смартфон управляемый извне - злоумышленник у банкомата не является специалистом



Виды кибератак #2

Программно-аппаратные

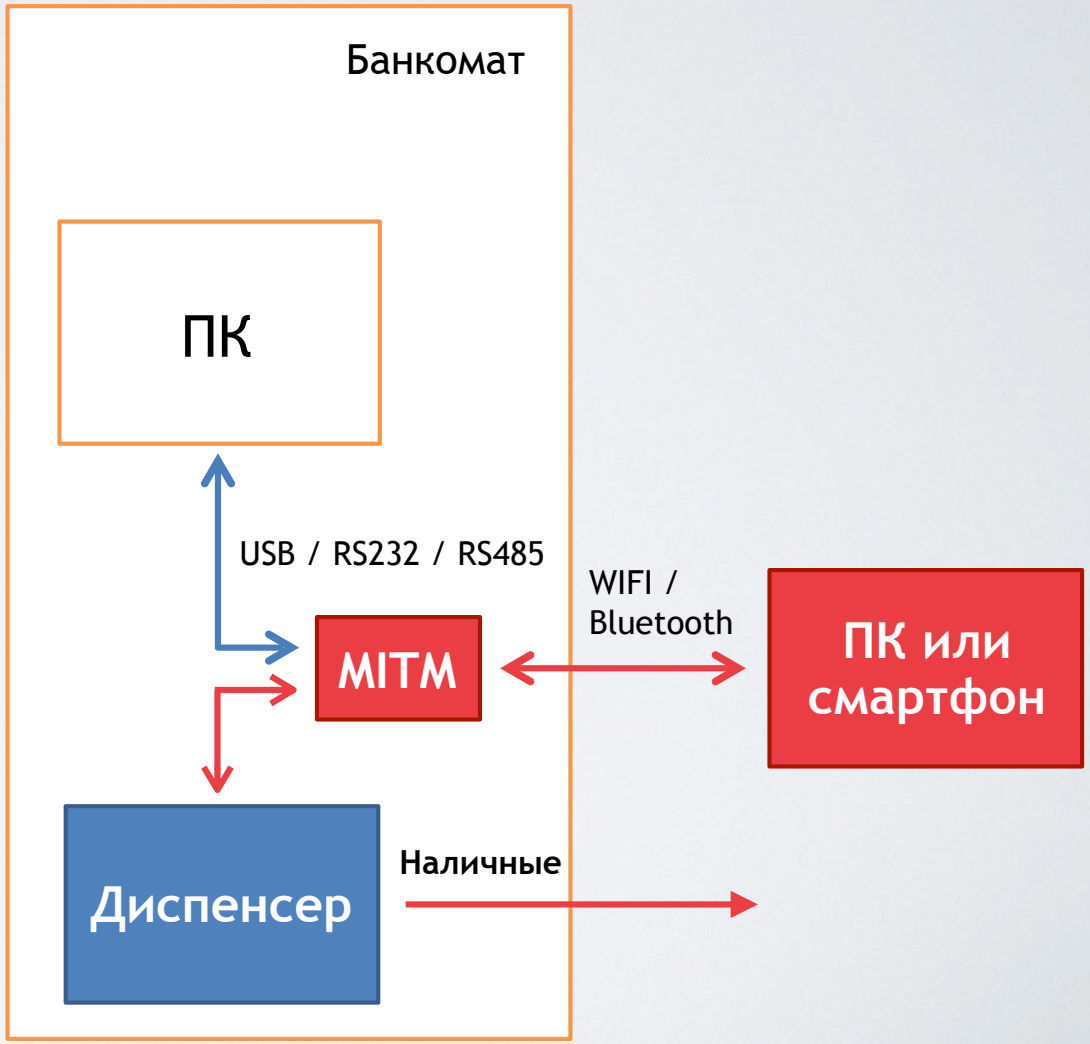
- Blackbox
- **Main In The Middle**
- Virtual Host
- Dispenser Switch Manipulation

Программные

- Malware
- Fileless
- Command prompt

Схема Man In The Middle атаки

- В ходе атаки злоумышленник перехватывает и подменяет сообщения, которыми обмениваются диспенсер и системный блок банкомата
- Если трафик между ПК и диспенсером шифруется - MITM может заниматься его расшифровкой (даже RSA, если реализован не корректно - а такое бывает)
- Опасность такой атаки заключается в том, что диспенсер и системный блок банкомата не догадываются о присутствии MITM в канале
- MITM может быть вмонтирован в проводку, стандартный разъем или исполнен в виде устройства банкомата (например USB hub), что затрудняет его обнаружение



Виды кибератак #3

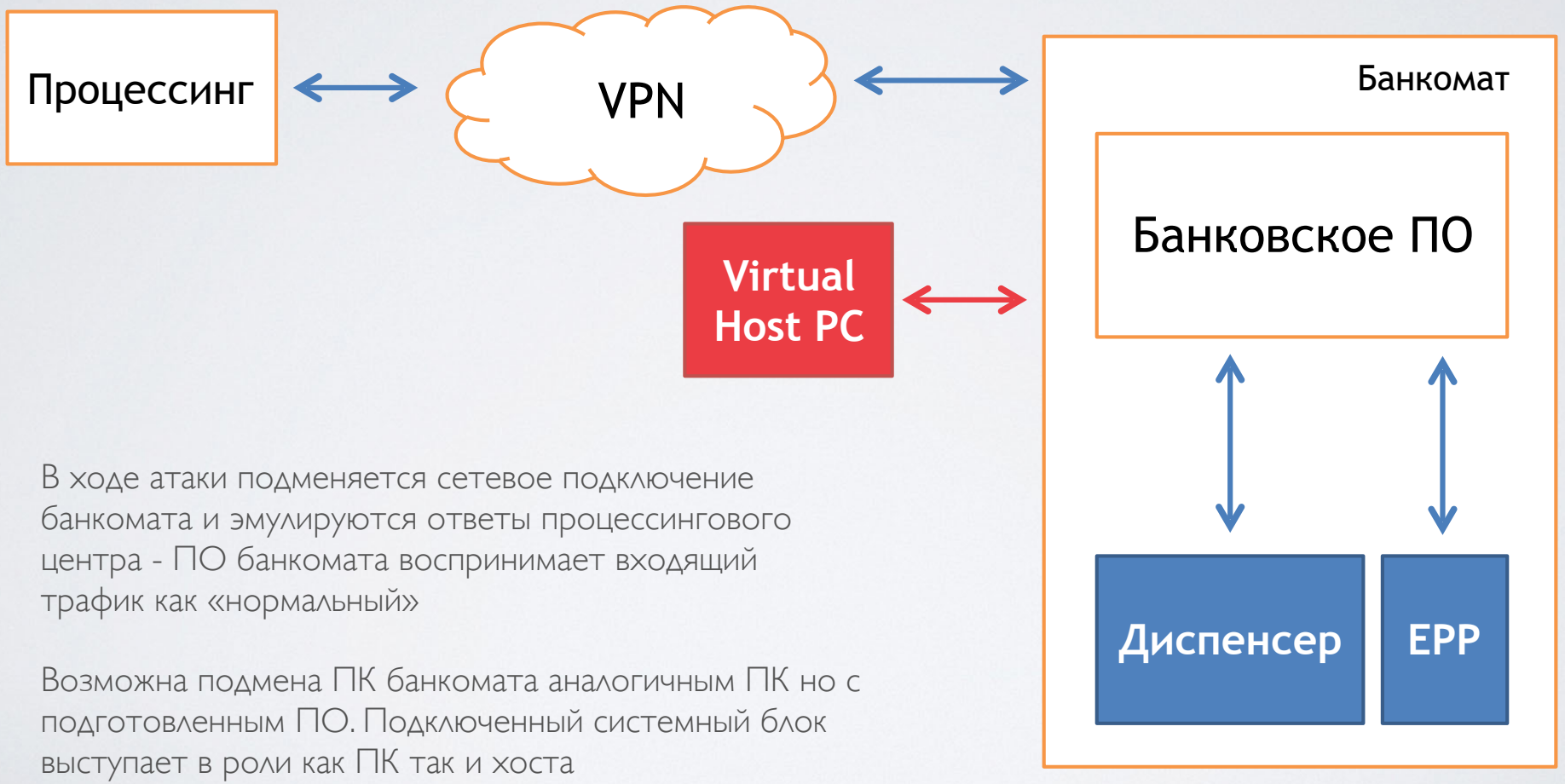
Программно-аппаратные

- Blackbox
- Main In The Middle
- **Virtual Host**
- Dispenser Switch Manipulation

Программные

- Malware
- Fileless
- Command prompt

Схема Virtual Host атаки



- В ходе атаки подменяется сетевое подключение банкомата и эмулируются ответы процессингового центра - ПО банкомата воспринимает входящий трафик как «нормальный»
- Возможна подмена ПК банкомата аналогичным ПК но с подготовленным ПО. Подключенный системный блок выступает в роли как ПК так и хоста

Виды кибератак #4

Программно-аппаратные

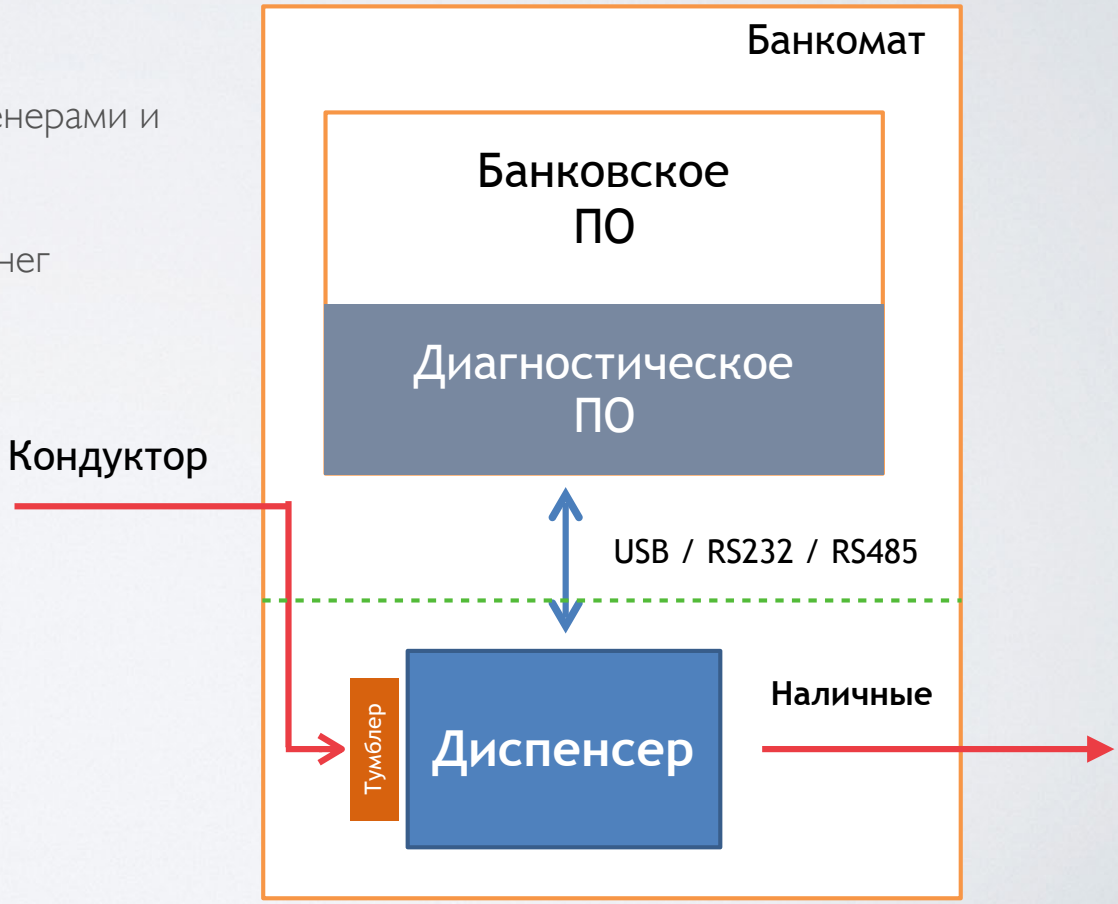
- Blackbox
- Main In The Middle
- Virtual Host
- **Dispenser Switch Manipulation**

Программные

- Malware
- Fileless
- Command prompt

Схема атаки Dispenser Switch Manipulation

- Один из самых старых видов атак
- Обычно используется недобросовестными инженерами и инкассаторами
- Кондуктор может быть удален после изъятия денег



Виды кибератак #5

Программно-аппаратные

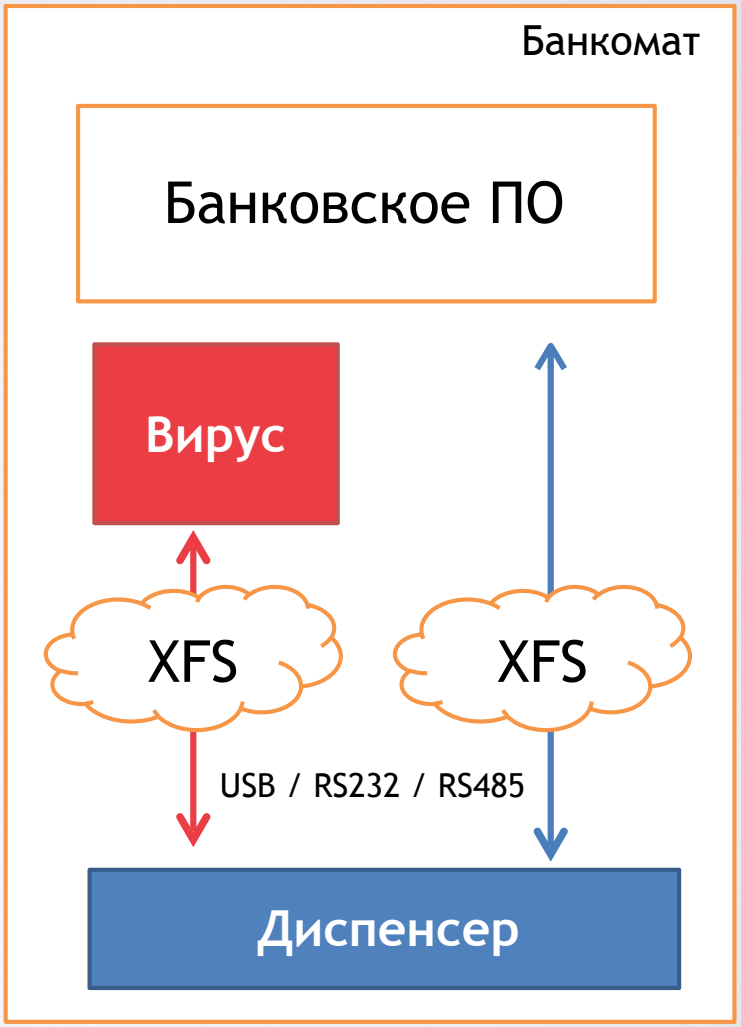
- Blackbox
- Main In The Middle
- Virtual Host
- Dispenser Switch Manipulation

Чисто программные

- **Malware**
- **Fileless**
- **Command prompt**

Схема Malware атаки

- Является программной разновидностью Blackbox. Вредоносное ПО запускается непосредственно на банкомате
- Существуют Fileless реализации - вредоносный файл загружается в память ПК и уничтожается после перезапуска банкомата
- Возможны реализации без установки ПО - выдача осуществляется средствами операционной системы - антивирусы, блокираторы не работают
- ПО может быть установлено как с внешнего носителя, так и централизованным деплоем через скомпроментированную банковскую сеть



Способы защиты от Jackpotting

Физическая защита
(Защита проводки и сервисной зоны)

Достоинства

- Простота понимания
- Низкая себестоимость (для производителя)

Недостатки

- Частичная защита от blackbox
- Прокладка дополнительной проводки
- Защита «до разъема»
- Отсутствие защиты от других видов jackpotting атак

Шифрование траффика

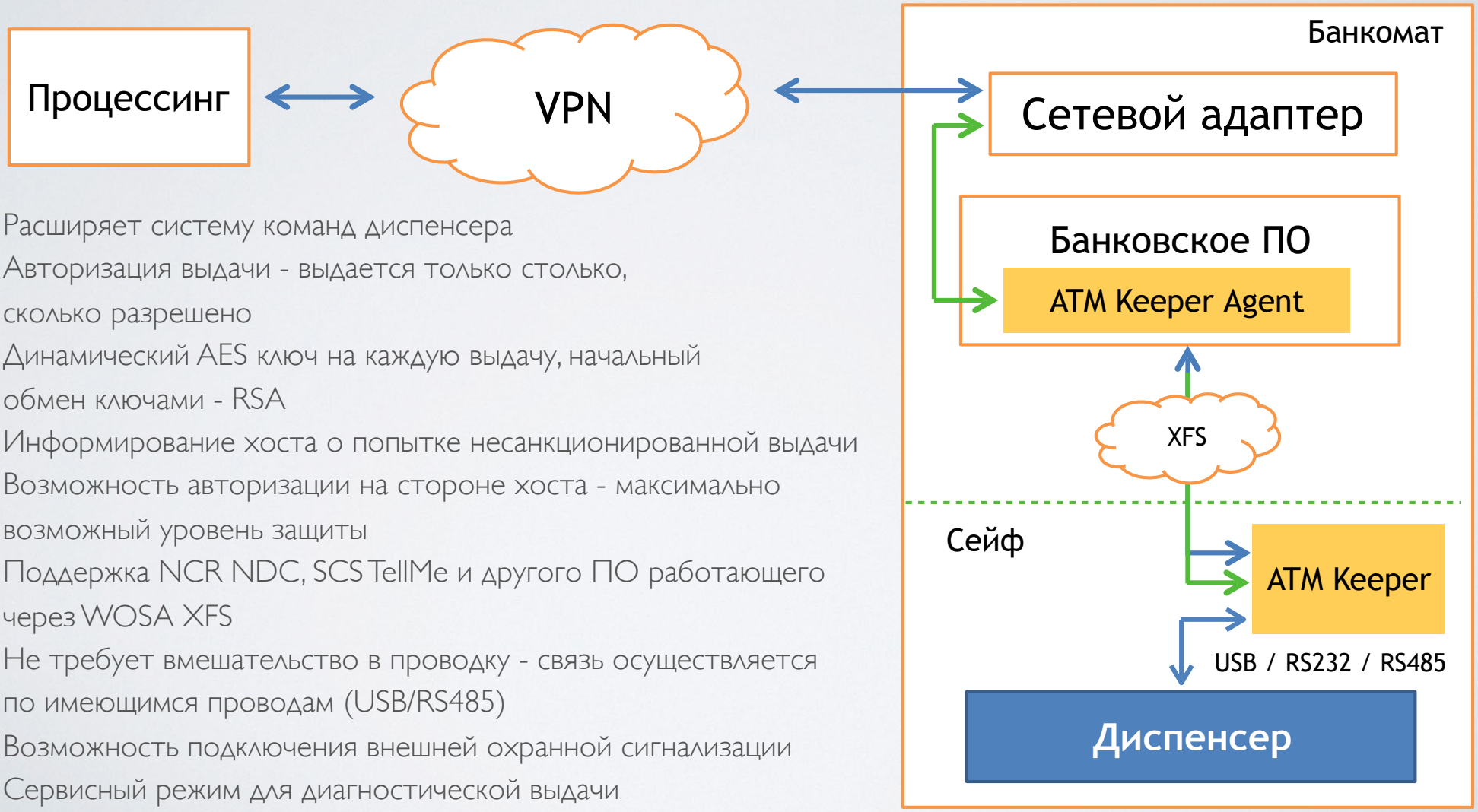
Достоинства

- При корректном исполнении защита работает
- Решение от производителя

Недостатки

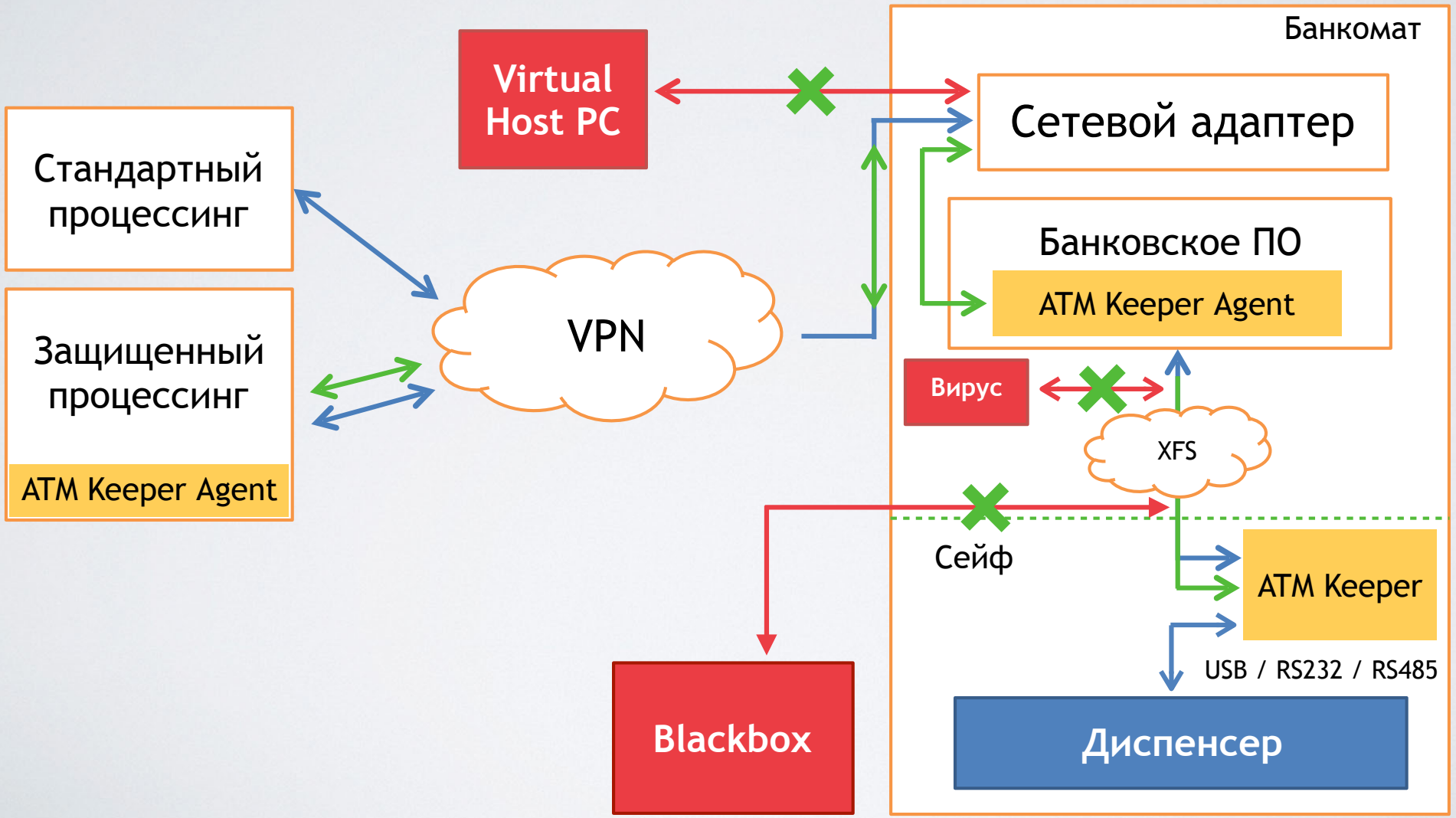
- Не всегда спасает
- Для старого парка банкоматов требуется модернизация железа - если предусмотрено
- Отсутствие защиты от других видов jackpotting атак

ATM Keeper



- Расширяет систему команд диспенсера
- Авторизация выдачи - выдается только столько, сколько разрешено
- Динамический AES ключ на каждую выдачу, начальный обмен ключами - RSA
- Информирование хоста о попытке несанкционированной выдачи
- Возможность авторизации на стороне хоста - максимально возможный уровень защиты
- Поддержка NCR NDC, SCS TellMe и другого ПО работающего через WOSA XFS
- Не требует вмешательство в проводку - связь осуществляется по имеющимся проводам (USB/RS485)
- Возможность подключения внешней охранной сигнализации
- Сервисный режим для диагностической выдачи

ATM Keeper - блокировка Jackpotting



Итоги

- Угроза существует и она актуальна
- Существующие методы защиты закрывают проблему частично
- Для устранения угрозы банкам необходимо реализовывать превентивные мероприятия

Наши рекомендации

Административные меры

- Проводить регулярный инструктаж сотрудников и разъяснять как выявлять фишинговые рассылки с помощью которых злоумышленники попадают во внутреннюю сеть банка.
- СБ и IT отделам необходимо совершенствовать безопасность внутренней сети для снижения вероятности успешной реализации вирусной атаки

На банкомате

- Задать пароль доступа в BIOS. Желательно уникальный на банкомат
- Запретить загрузку с внешнего носителя
- Убедиться, что банковское ПО запускается под учетной записью с ограниченными правами:
    1. Меню «Пуск» отключено.
    2. Запуск диспетчера задач запрещен (включая вызов по Ctrl-Alt-Del)
    3. Доступ к внешним USB носителям/CDROM/FDD запрещен.

- Задать пароль администратора Windows, желательно уникальный на банкомат
- Настроить брэндмауэр - должны быть открыты только используемые TCP/IP порты
- Обмен с хостом должен осуществляйся через защищенный (SSL/VPN) канал связи
- Установить оборудование защиты от Jackpotting атак. Только защиты от Blackbox не достаточно

Спасибо за внимание

Наши контакты:

ATM Keeper
atmkeeper.pro

8 (800) 500 48 62
info@atmkeeper.pro