Защита информации в банковских технологиях

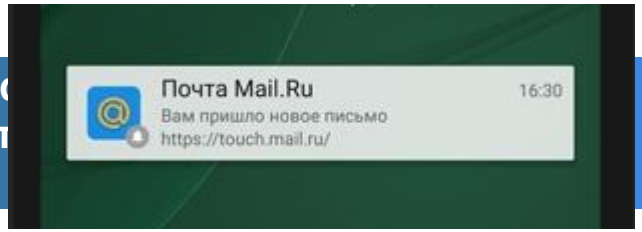
3.6 Алгоритм функционирования FMS

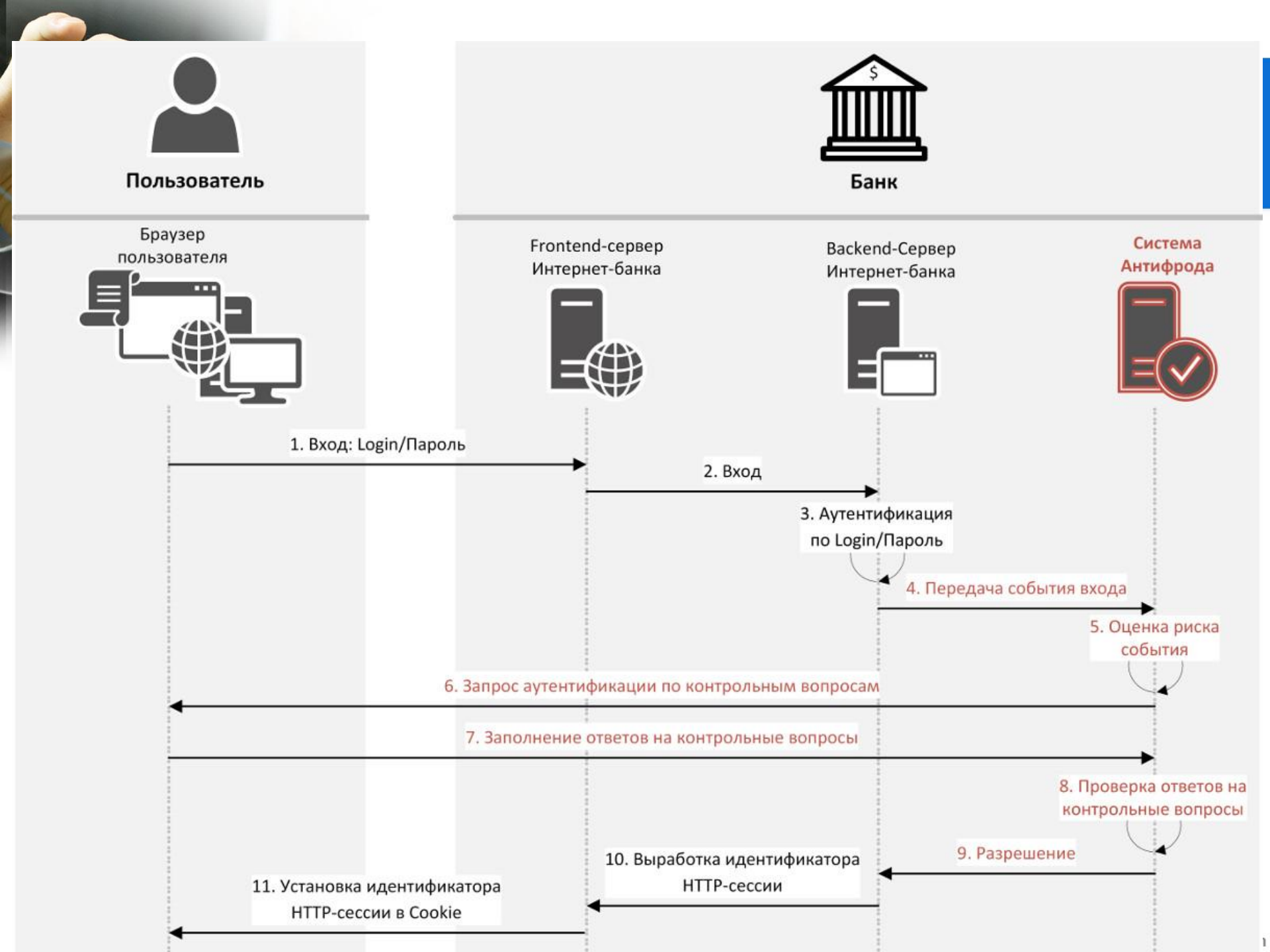
Способы проверки легитимности клиента

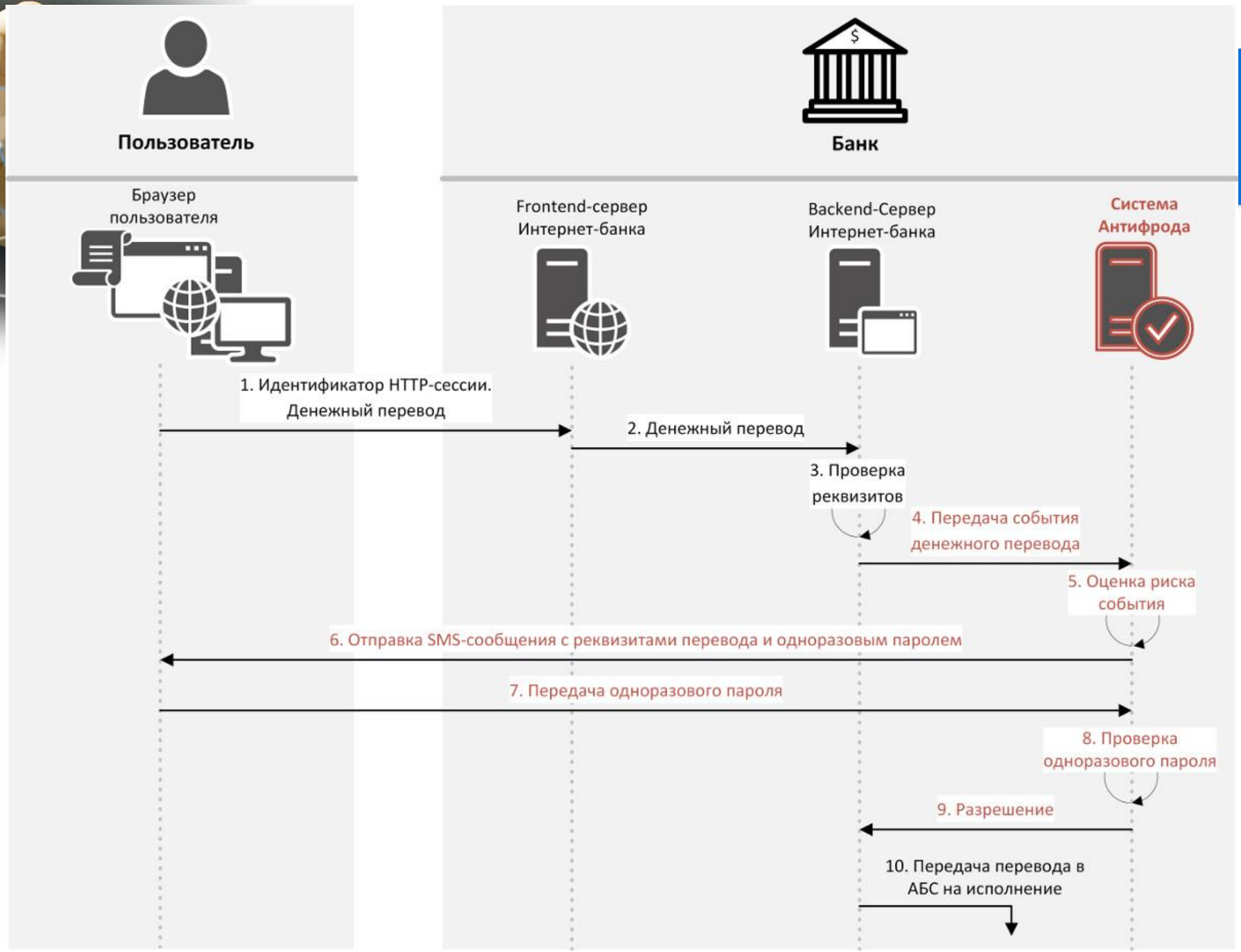
A Автоматический

1. Логин / пароль
2. SMS сообщение
3. Push уведомление

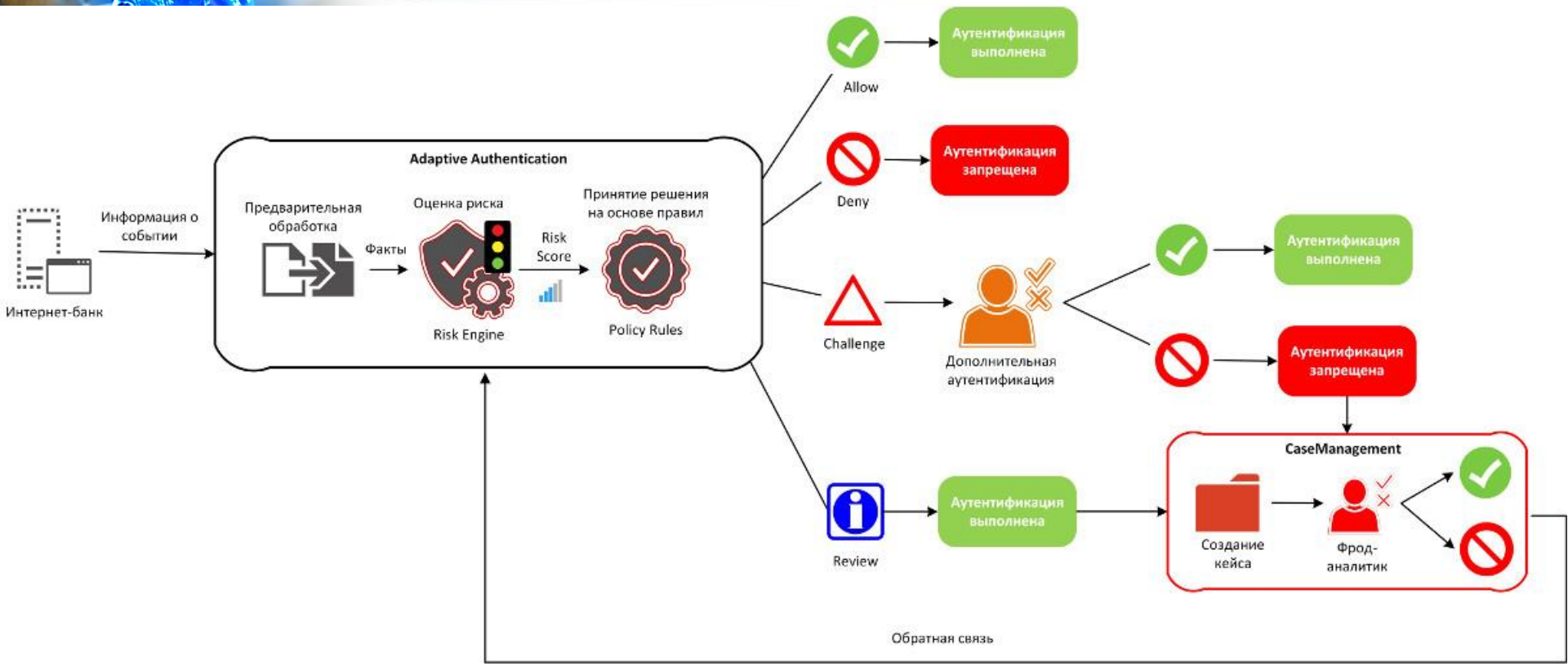
B В ручную с клиент




Пользователь
Банк
Браузер пользователя
Frontend-сервер Интернет-банка
Backend-Сервер Интернет-банка
Система Антифрода
1. Вход: Login/Пароль
2. Вход
3. Аутентификация по Login/Пароль
4. Передача события входа
5. Оценка риска события
6. Запрос аутентификации по контрольным вопросам
7. Заполнение ответов на контрольные вопросы
8. Проверка ответов на контрольные вопросы
9. Разрешение
10. Выработка идентификатора HTTP-сессии
11. Установка идентификатора HTTP-сессии в Cookie


Пользователь
Банк
Браузер пользователя
Frontend-сервер Интернет-банка
Backend-Сервер Интернет-банка
Система Антифрода
1. Идентификатор HTTP-сессии. Денежный перевод
2. Денежный перевод
3. Проверка реквизитов
4. Передача события денежного перевода
5. Оценка риска события
6. Отправка SMS-сообщения с реквизитами перевода и одноразовым паролем
7. Передача одноразового пароля
8. Проверка одноразового пароля
9. Разрешение
10. Передача перевода в АБС на исполнение

Алгоритм функционирования FMS



Этапы обработки событий FMS

Предварительная обработка	**структурирование данных (парсинг), поиск пользователя и его устройства в базе данных, получение истории пользователя и его устройства**
Оценка риска	**скоринг, нормализация по полученной на первом этапе информации**
Принятие решения	**определение на основании правил, задаваемых фрод-аналитиком, значения риска и ответного действия FMS**

Виды ответов FMS

ALLOW

разрешить действие (дополнительного процесса не требуется)

DENY

запретить действие (дополнительного процесса не требуется)

CHALLENGE

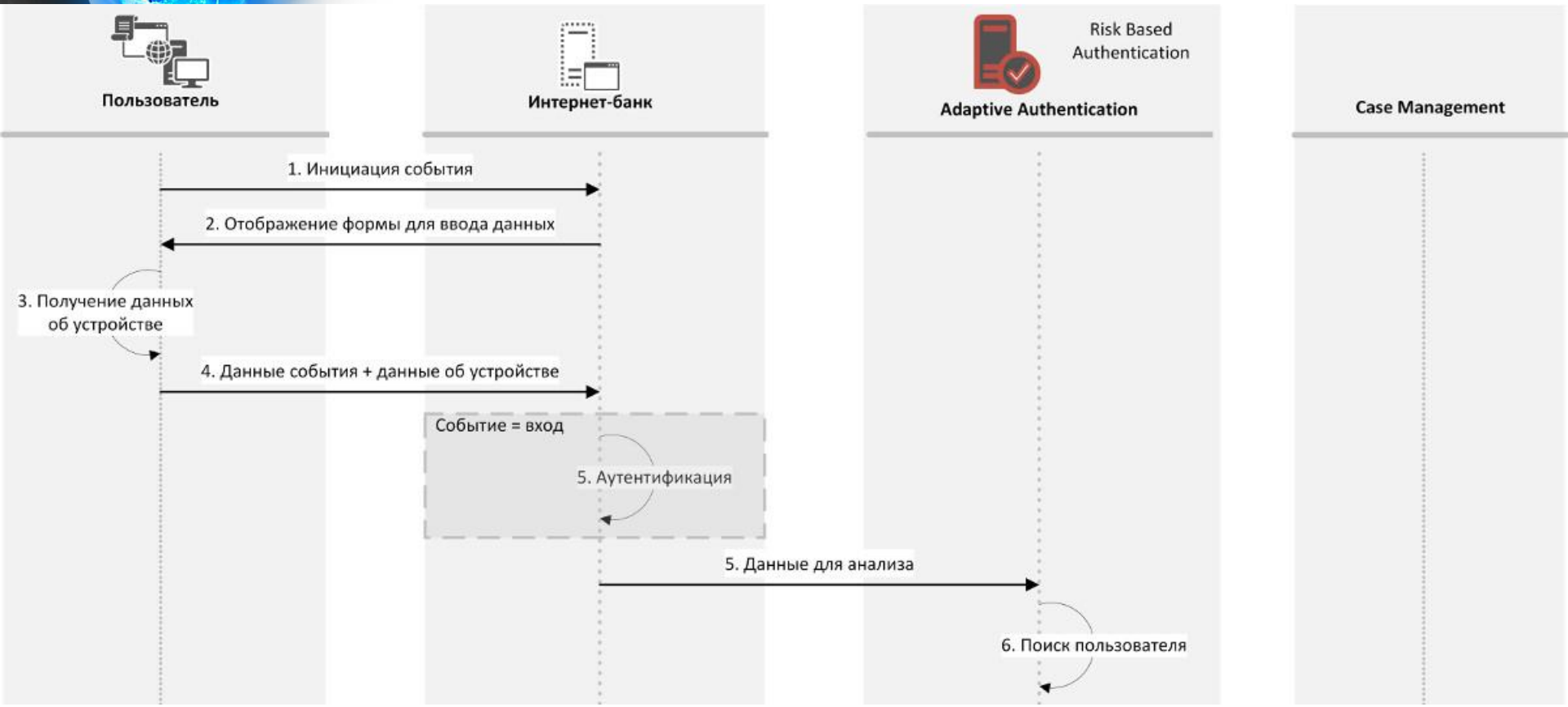
произвести дополнительную аутентификацию (по завершению проверки, в зависимости от результата - FMS разрешает или запрещает данное событие)

Виды ответов FMS

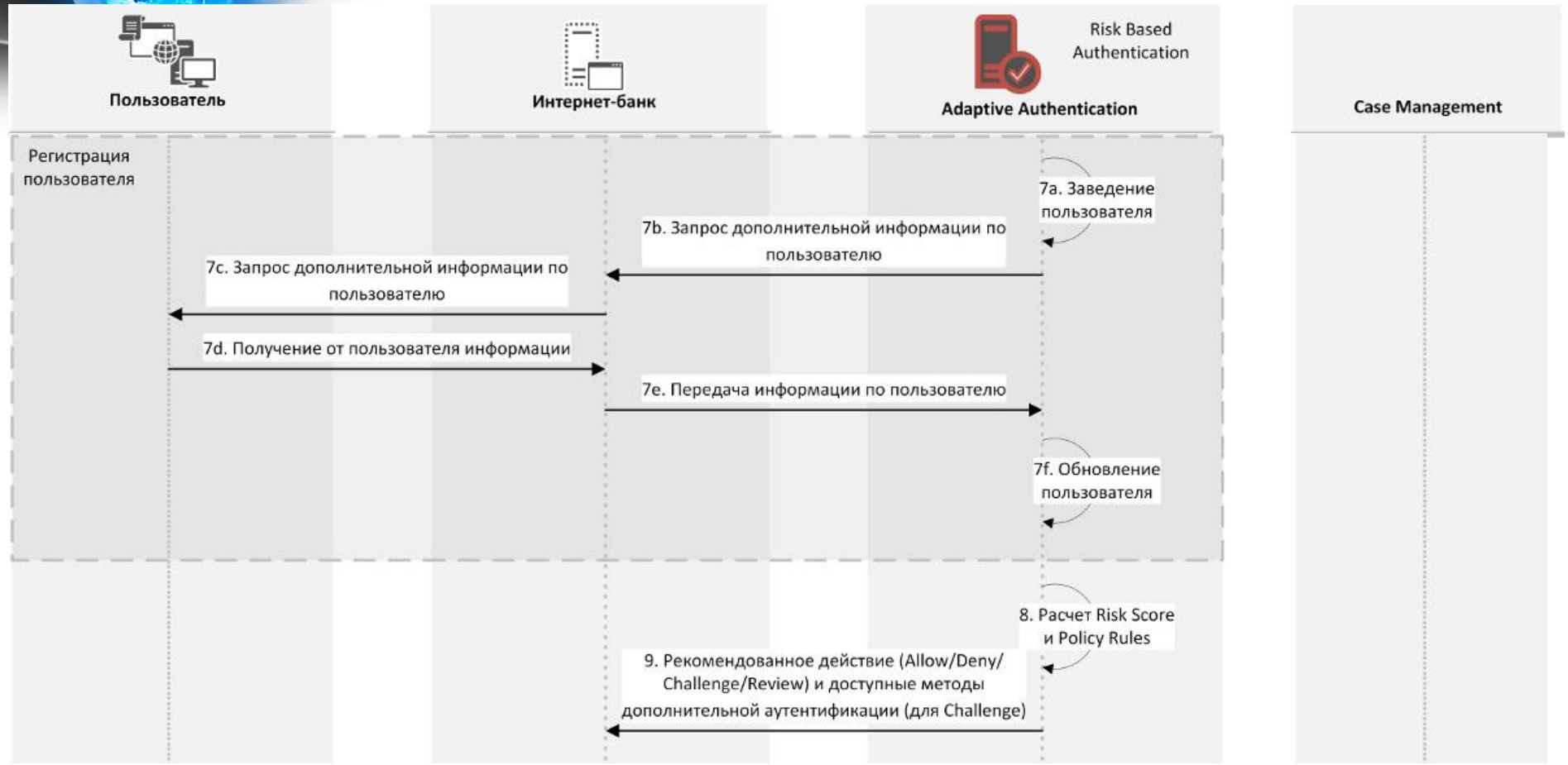
REVIEW

(постобработка) разрешить действие, но при этом создать кейс в компоненте Case Management для последующей маркировки, расчета скоринга и обработки фрод-аналитиком

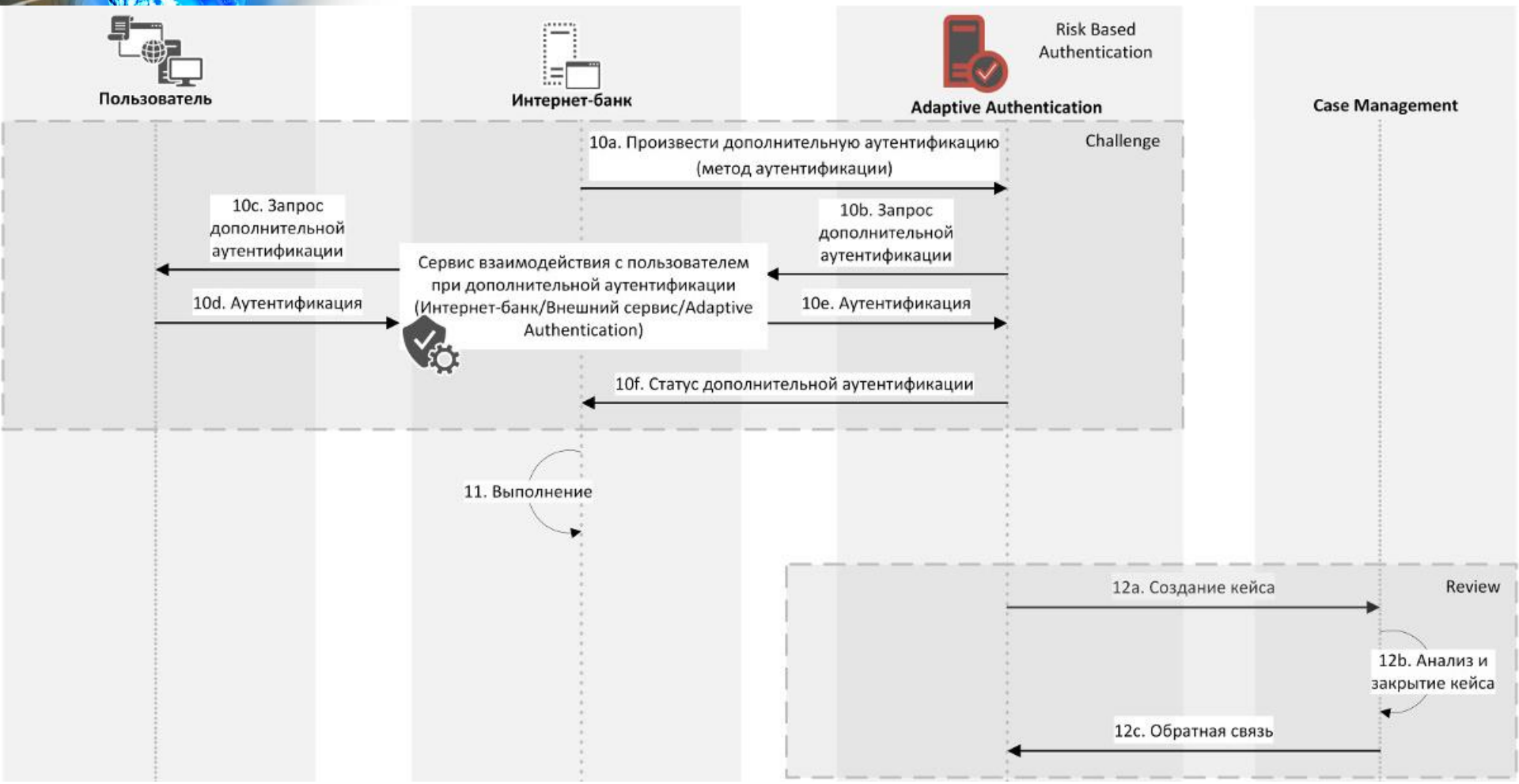
Обработка события в FMS



Обработка события в FMS



Обработка события в FMS



3.7 Автоматические кассовые аппараты (АТМ). Аппаратное и программно обеспечение

ATM - Automatic Teller Machine (автоматический кассовый аппарат)

ATM

специализированное устройство, предназначенное для обслуживания клиента без участия банковского персонала

Основные функции

1. Выдача наличных
2. Платежи

Способы установки АТМ

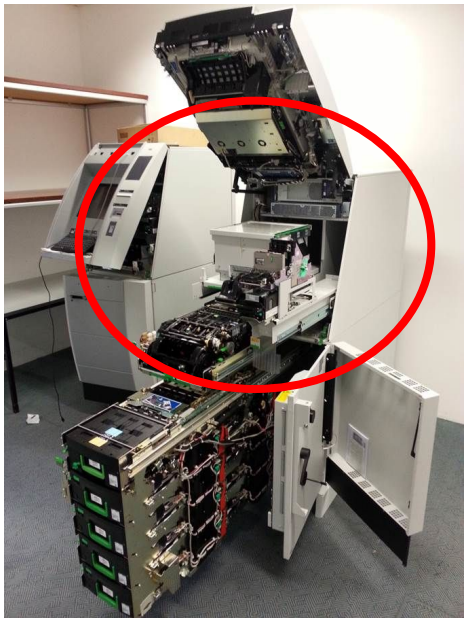
Напольный

Встраиваемый

Основные части АТМ

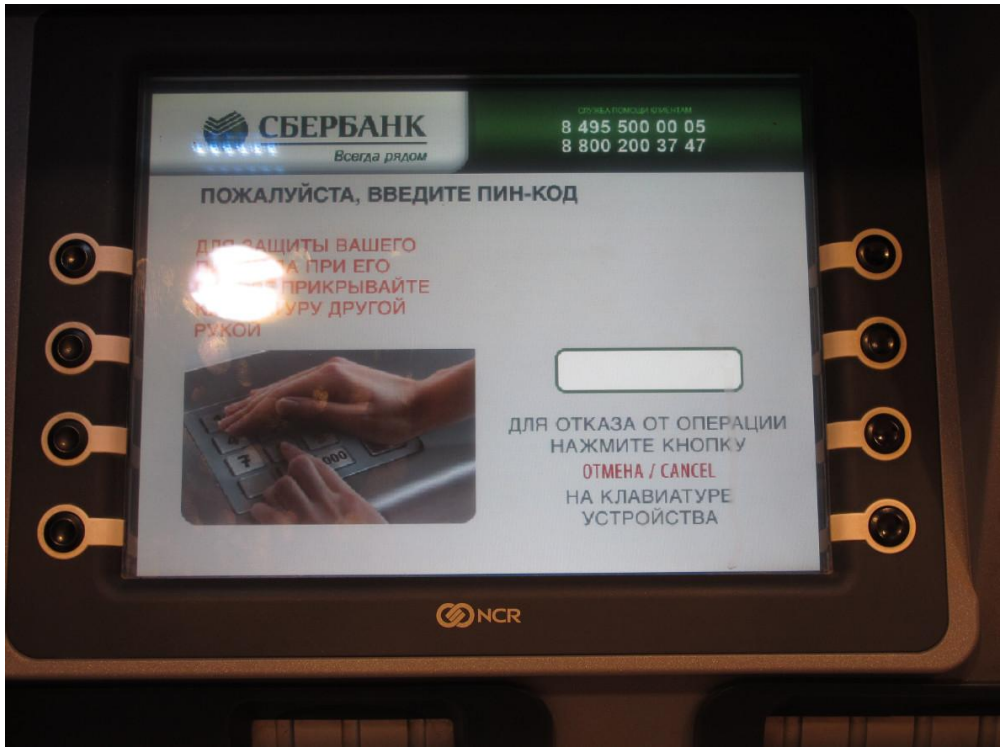
Сервисная зона

Предназначена для обслуживания банкомата специалистом (системный блок, дисплей и функциональная клавиатура, клавиатура (pin-pad), карт-ридер, чековый принтер, шлейф подключения диспенсера). Имеет слабую физическую защиту



Системный блок

Дисплей и функциональная клавиатура



Пользовательская клавиатура (pin-pad)

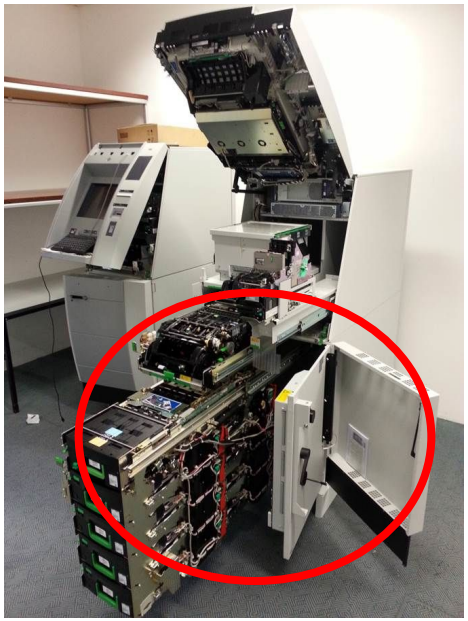
Карт-ридер

Чековый принтер

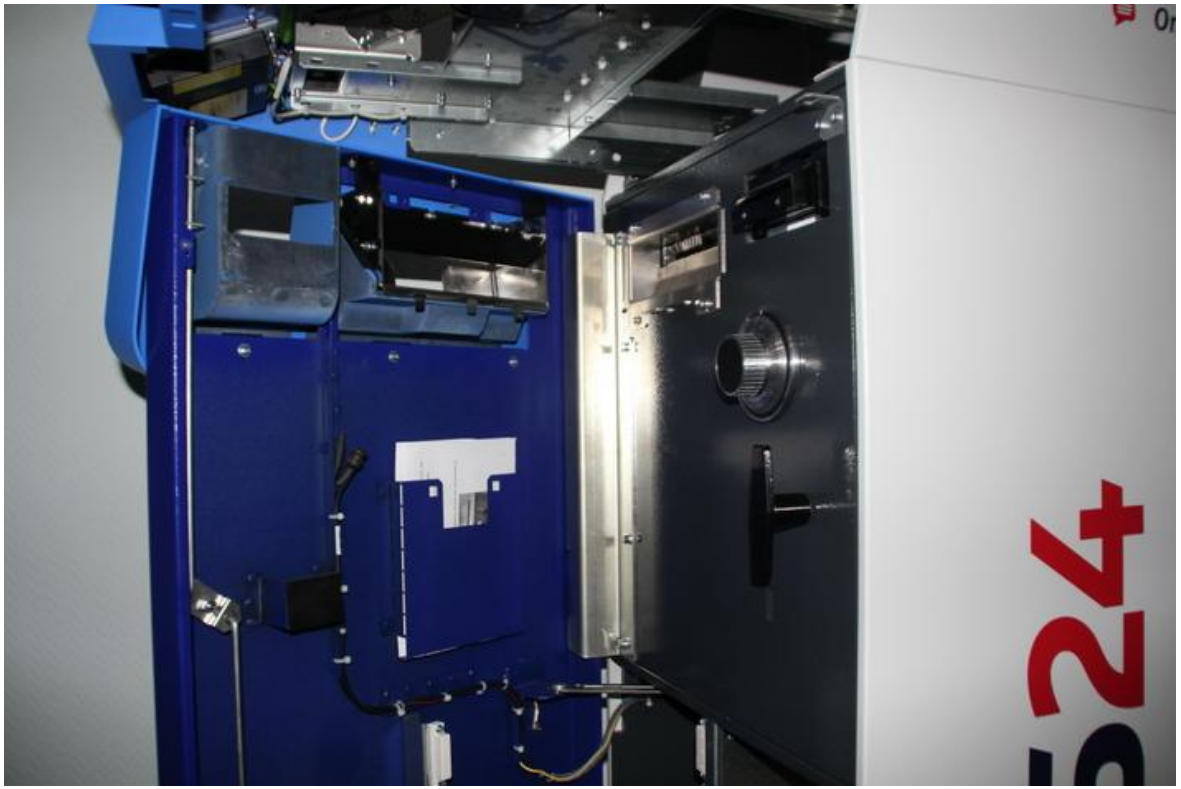
Основные части АТМ

Сейф

Предназначен для хранения кассет с купюрами и размещения устройства их выдачи. Выполняется из высокопрочных материалов



Сейф



Кассеты для купюр

Диспенсер

Программное обеспечение банкомата

ОС	**Работа устройства обеспечивается в рамках Windows (XP, 7 …) Embedded**
Банковское приложение	**Обеспечивает взаимодействие пользователя с периферийным оборудованием банкоматом через API реализованный в соответствии со стандартом XFS (eXtension for Financial Services)**
Драйвер устройства (SPI)	**Обеспечивает управление определенным устройством (диспенсер, pin-pad и т.д.)**

Взаимодействие устройств банкомата

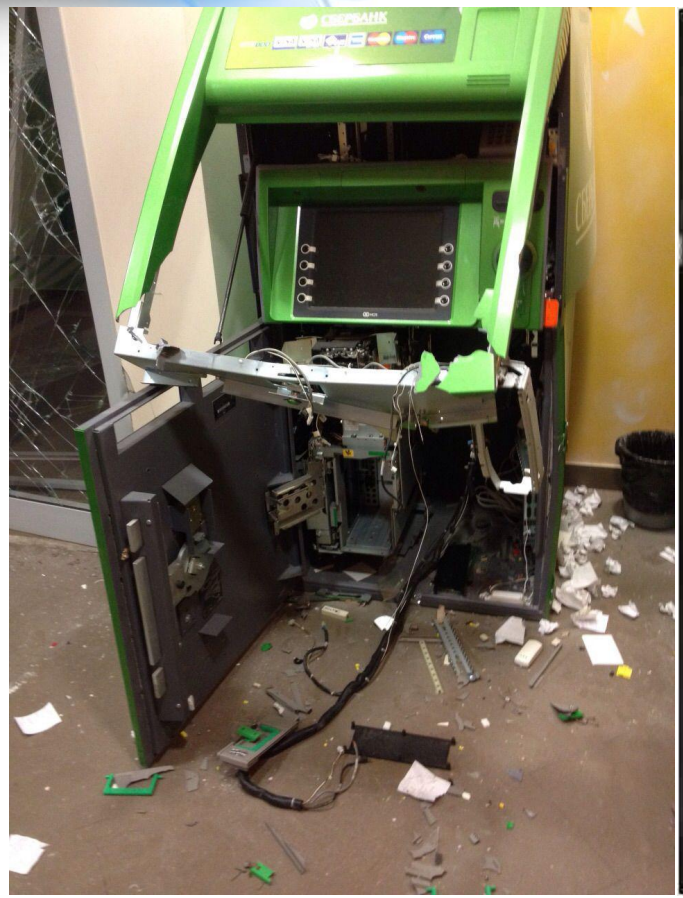
Типовые особенности обеспечения безопасности банкомата

Шифрование	**Защищает информацию передаваемую между банкоматом и банком (VPN). Информационный обмен между устройствами, как правило, не защищается. Информация поступающая из pin-pad шифруется самим pin-pad**
Физическая защита	**Уделяется особое внимание противодействию хищению купюр. Сервисная зона защиты не имеет**
Техническая охрана	**Используются средства охранной сигнализации обеспечивающие фиксацию вскрытия устройства, перемещение, нагрев. В базовой комплектации система видеонаблюдения как правило не устанавливается**

3.8 Атаки на ATM

Основные угрозы безопасности АТМ (направленные на денежные средства)

Взлом сейфа



Основные угрозы безопасности АТМ (направленные на денежные средства)

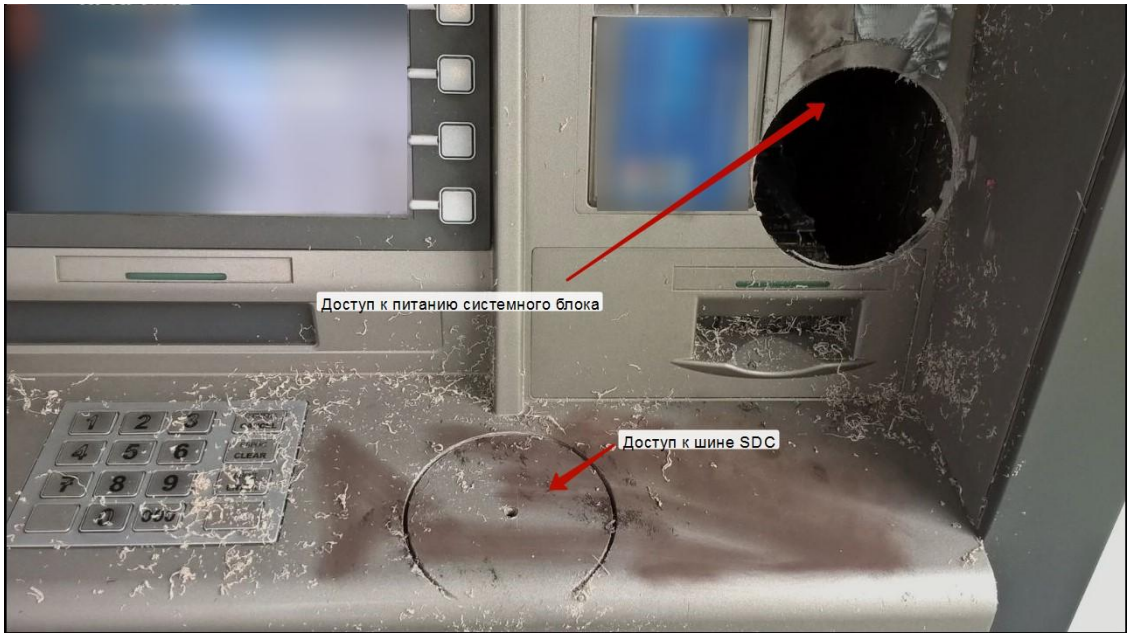
Похищение банкомата

Для обеспечения безопасности используется охранная сигнализация и СВН

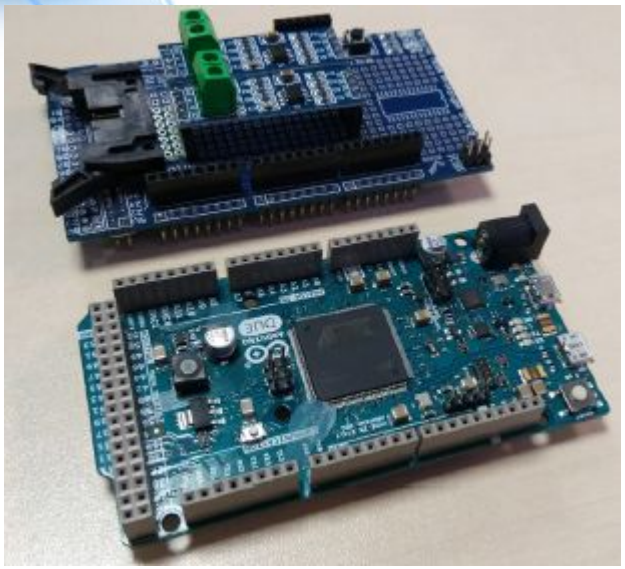
Атака Black Box
(направленные на денежные средства)

Цель

Подключение в сервисной зоне к диспенсеру устройства злоумышленника для управления выдачей купюр с помощью специального ПО



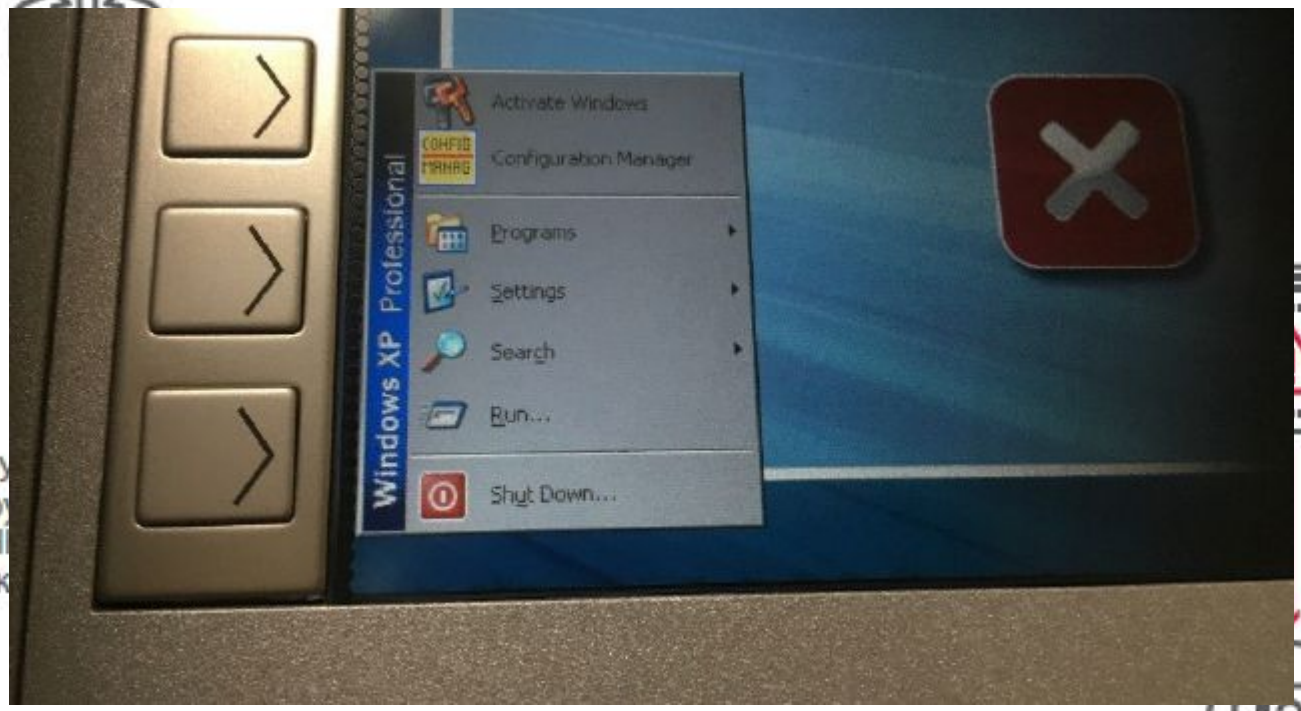
Атака Black Box (направленные на денежные средства)



Внешний вид устройства

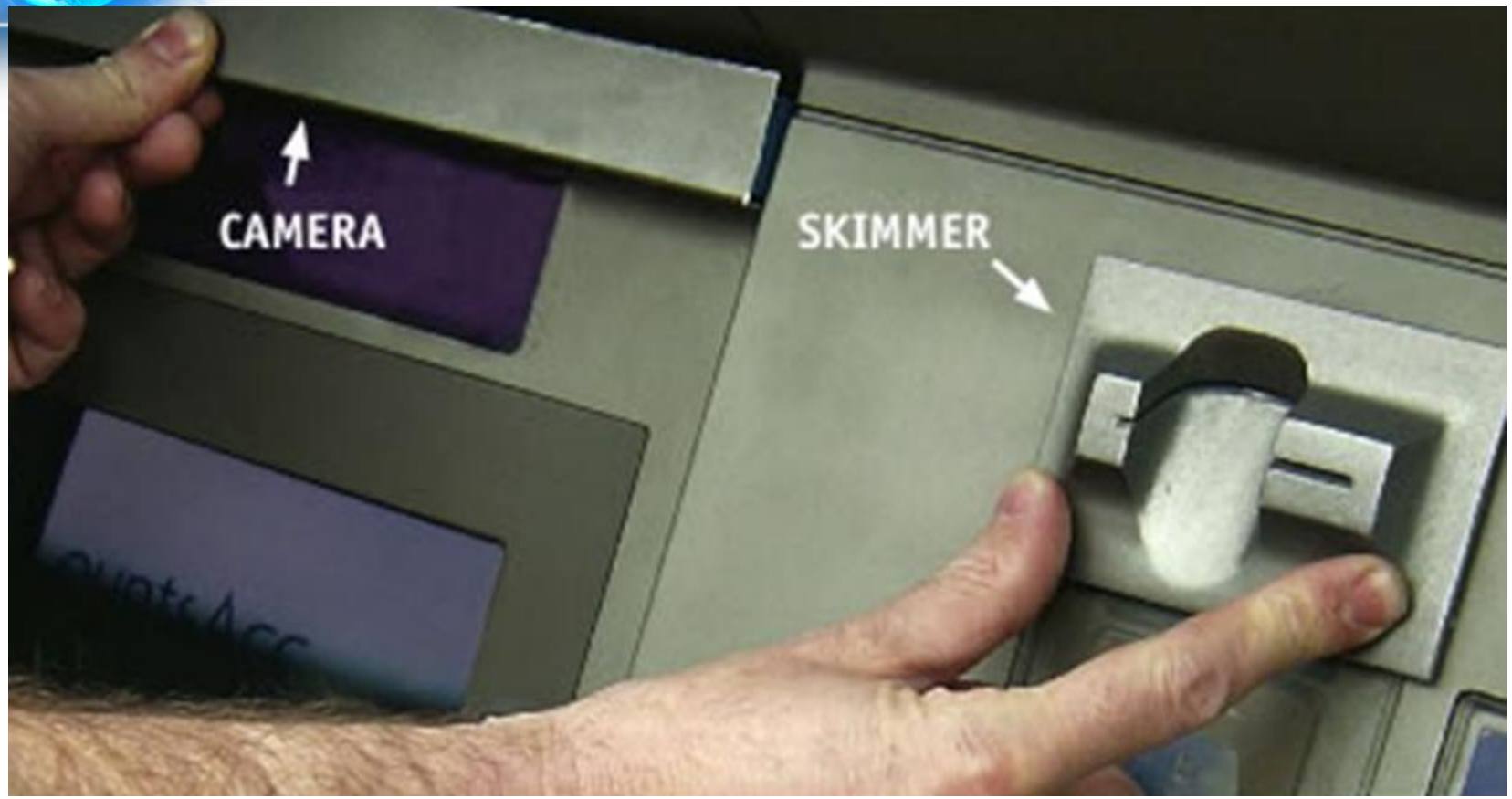
Главное окно специального ПО

Выход из режима инфокиоска (направленные на денежные средства)



Основные угрозы безопасности АТМ (направленные на платежную карту)

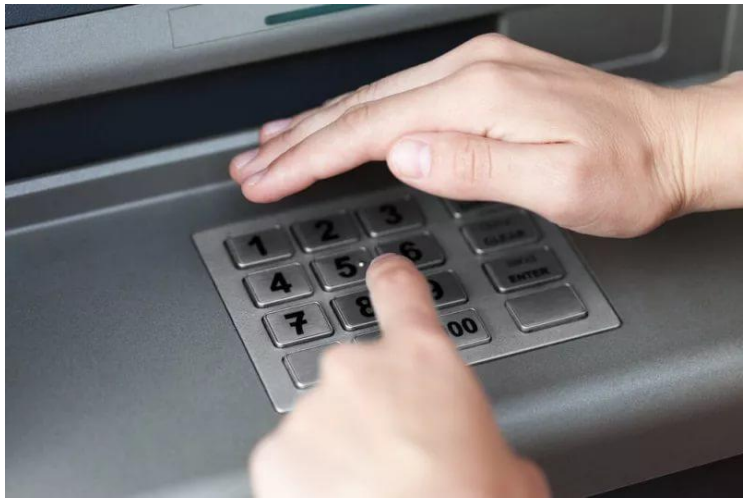
Скиминг



Современный скиммер устанавливается внутрь карт-ридера банкомата

Антискиминговый модуль

Накладной pin-pad



Противодействие атакам

2008

$9 Million
stolen by a gang from 130 ATMs in 49 cities in just 10 hours after hacking RBS World Pay

2009

First Malicious ATM Malware "Skimmer"
harvests data and allows to dispense cash

2011

$13 Million
stolen using 22 cloned FIS prepaid cards after hack to remove limits

2013

"Ploutus" ATM Malware
hits Latin America

Hacking of an Indian Card Processor
results in $45 million cashed out on thousands of ATMs around the world

2014

"Annunak/ Carbanak" Malware
hits up to 100 financial institutions across 11 countries

Malware "Tyupkin/Padpin"
$1 million stolen on at least 18 ATMs in Malaysia

2015

New ATM Malware
Green Dispenser

Black Box Attacks
resurface globally

2016

"Skimmer" ATM Malware
returns

"ATM Ripper" Malware
results in $350,000 stolen in Thailand

Cobalt Hacking Group
infiltrates banks in at least 14 countries and cashes out on ATMS

2017

Jackpotting Attack
results in $2.5 million stolen from 40+ ATMs in Taiwan

New Variant of "Ploutus" ATM Malware
emerges in North America

Chinese ATM Malware "Rufus"
attacks ATMs in India

2018

Jackpotting Attacks
resurface globally

Black Box Attacks
strike twice in Latin America

"Peralta" ATM Malware
new variant reported in Latin America

"Unlimited Operations" FBI Advisory
attack targets the redemption points

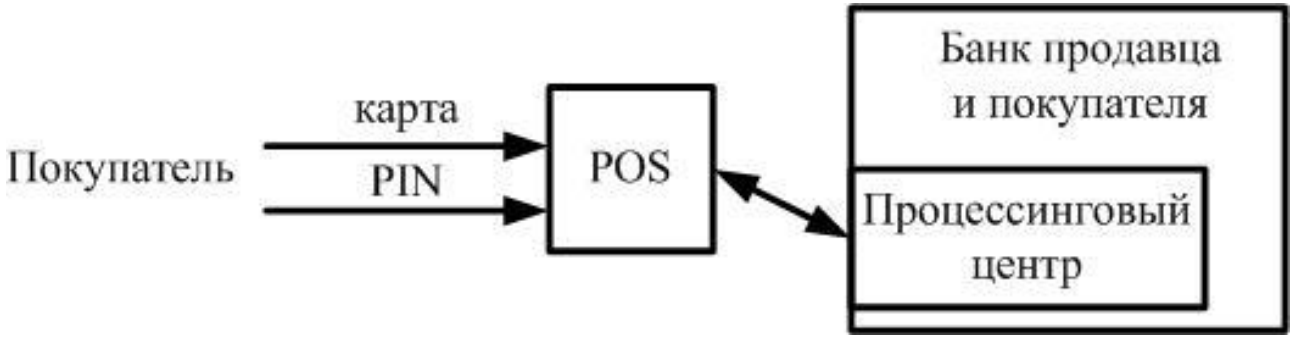
3.9 Системы обеспечения расчета в точке продажи (POS)

POS – Point Of Sale
(расчет в точке продажи)

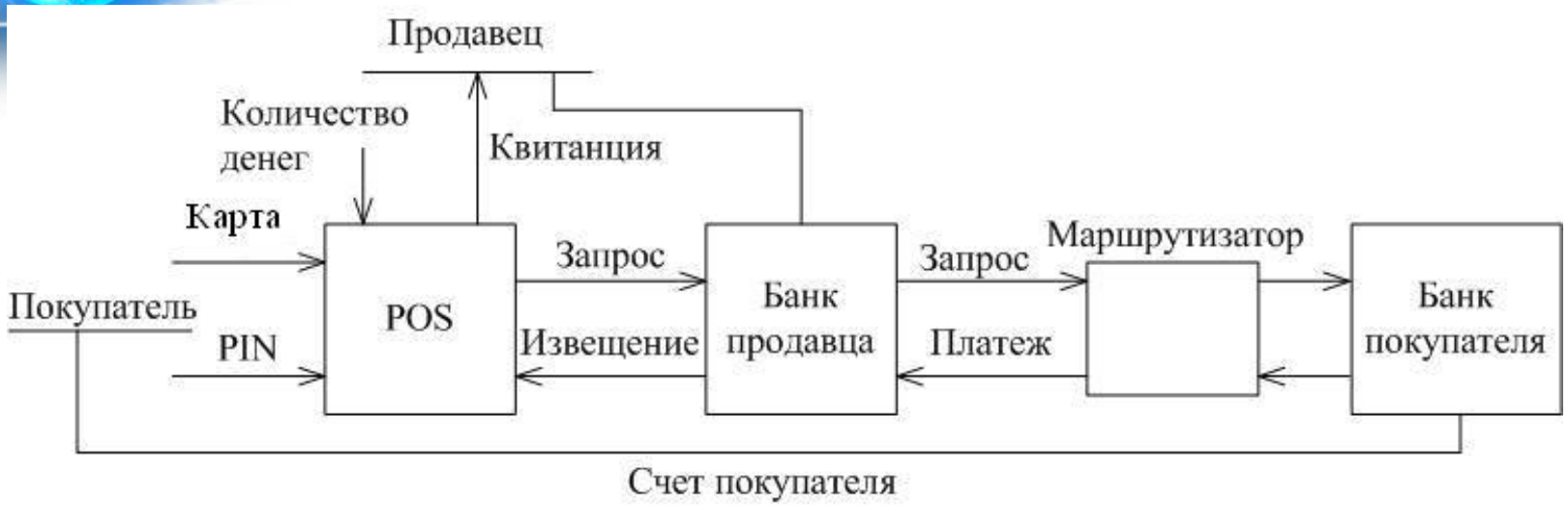
POS

обеспечивают расчет продавца и покупателя в торговом предприятии (магазине) без использования наличных денег

Банк эквайер и банк эмитент – один банк



Банк эквайер и банк эмитент – разные банки



Угрозы безопасности POS терминалов

Обратное трассирование

если злоумышленник получит ключ шифрования, то он будет пытаться восстановить значения PIN, использованные в предыдущих транзакциях

Прямое трассирование

если злоумышленник получит ключ шифрования, то он будет пытаться восстановить значения PIN, использованные в последующих транзакциях

Методы противодействия

Метод выведенного ключа	ключ для шифрования каждой следующей транзакции вычисляется путем одностороннего преобразования предыдущего ключа и параметров транзакции
Метод ключа транзакции	ключ для шифрования каждой следующей транзакции вычисляется путем одностороннего преобразования предыдущего ключа

Система mPOS (mobile Point Of Sale)

mPOS

отличается от POS терминала тем, что в качестве средства передачи информации используется смартфон к которому подключается карт ридер

Основные компоненты системы

1. **Смартфон**
2. **Специальное ПО**
3. **Карт-ридер**

Способы подключения карт-ридера к смартфону

1. **Через разъем «аудио» 3,5 мм**

2. 

Терминал WisePOS

NFC (Near Field Communication) – технология беспроводной передачи данных малого радиуса действия, для обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров

3.10 Системы резервного копирования данных

Способы копирования данных

Резервное копирование данных (backup)	процесс сохранения избыточных копий файлов и каталогов, находящихся на локальных дисках, на сменные носители
Архивирование данных (arhive)	процесс получения «слепка» файлов и каталогов в том виде, в котором они располагаются на первичном носителе (обычно диск) в данный момент времени

Методы резервного копирования данных

Полное

заданный набор файлов (например, файловая система) полностью записывается на сменный носитель. Служит основой для других методов

Достоинства

1. Надежность;
2. Восстановление выполняется из одной копии и как следствие выше скорость восстановления

Недостатки

1. Создание копии данных занимает много времени и ведет к большому расходу емкости накопителя

Методы резервного копирования данных

Инкрементный

представляет собой поэтапный способ записи информации. При использования этого способа первая запись на носитель является полной копией. На каждом последующем этапе переносятся только файлы, атрибуты которых изменились со времени предыдущей записи

Достоинства

1. Быстрота резервирования;
2. Минимальный расход емкости носителя

Недостатки

1. Длительное время восстановления данных

Методы резервного копирования данных

Дифференциальный

первая запись на носитель является полной копией. На последующих этапах копируются только файлы, которые изменились со времени проведения полного копирования

Достоинства

1. Для восстановления данных нужно две копии – последние полная и дифференциальная

Недостатки

1. Длительное время копирования данных

Функции систем резервного копирования данных (СРКД)

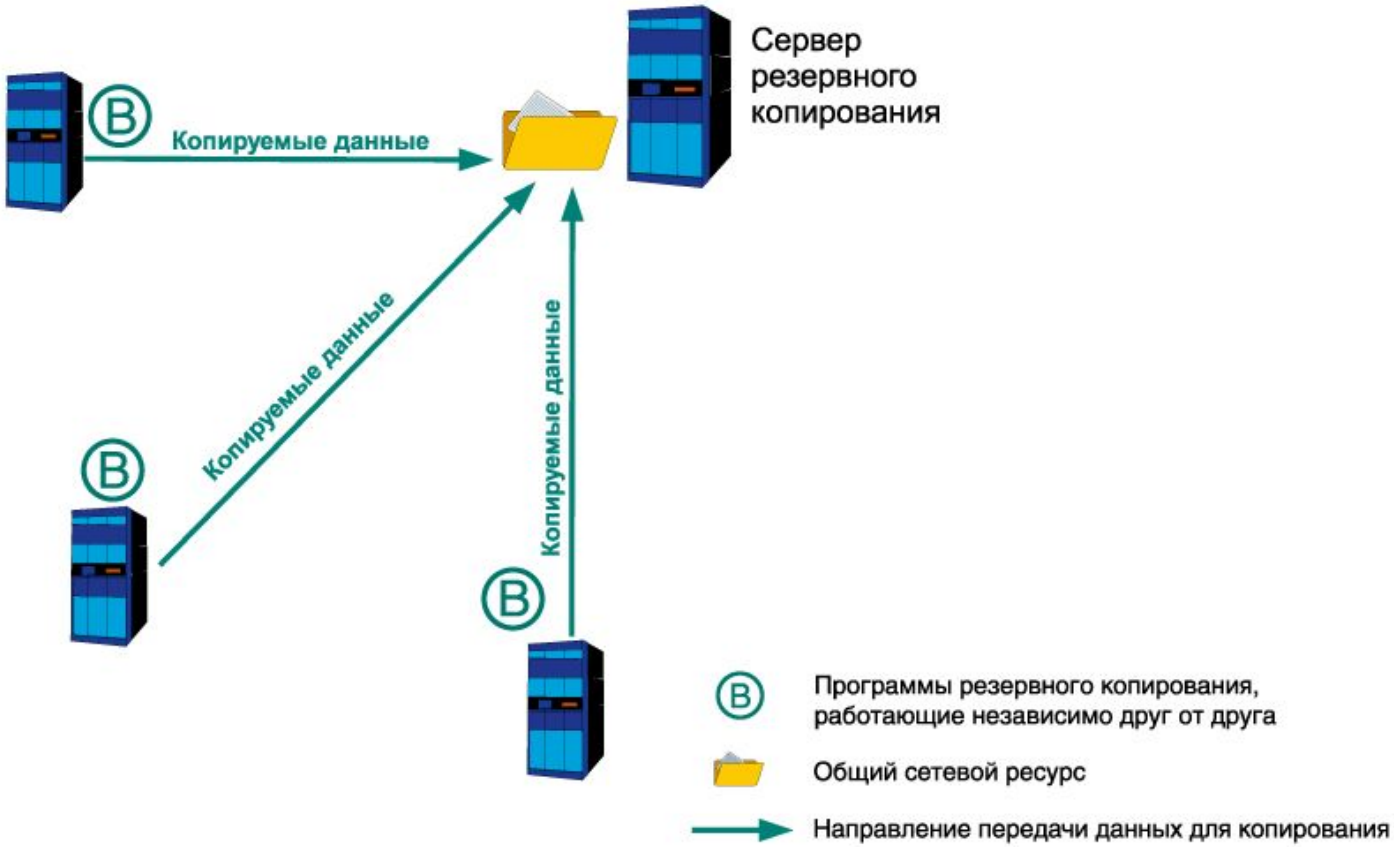
проведение регулярного автоматического копирования как системных данных, так и данных, создаваемых пользователями

A

оперативное восстановление данных (в случае утери или по каким то другим причинам)

B

Архитектура децентрализованной СРКД



Архитектура децентрализованной СРКД

ядро системы – некоторый общий ресурс

A

ПО, используемое для передачи данных с рабочих мест пользователей на сервер, функционирует независимо друг от друга

B

Архитектура децентрализованных СРКД

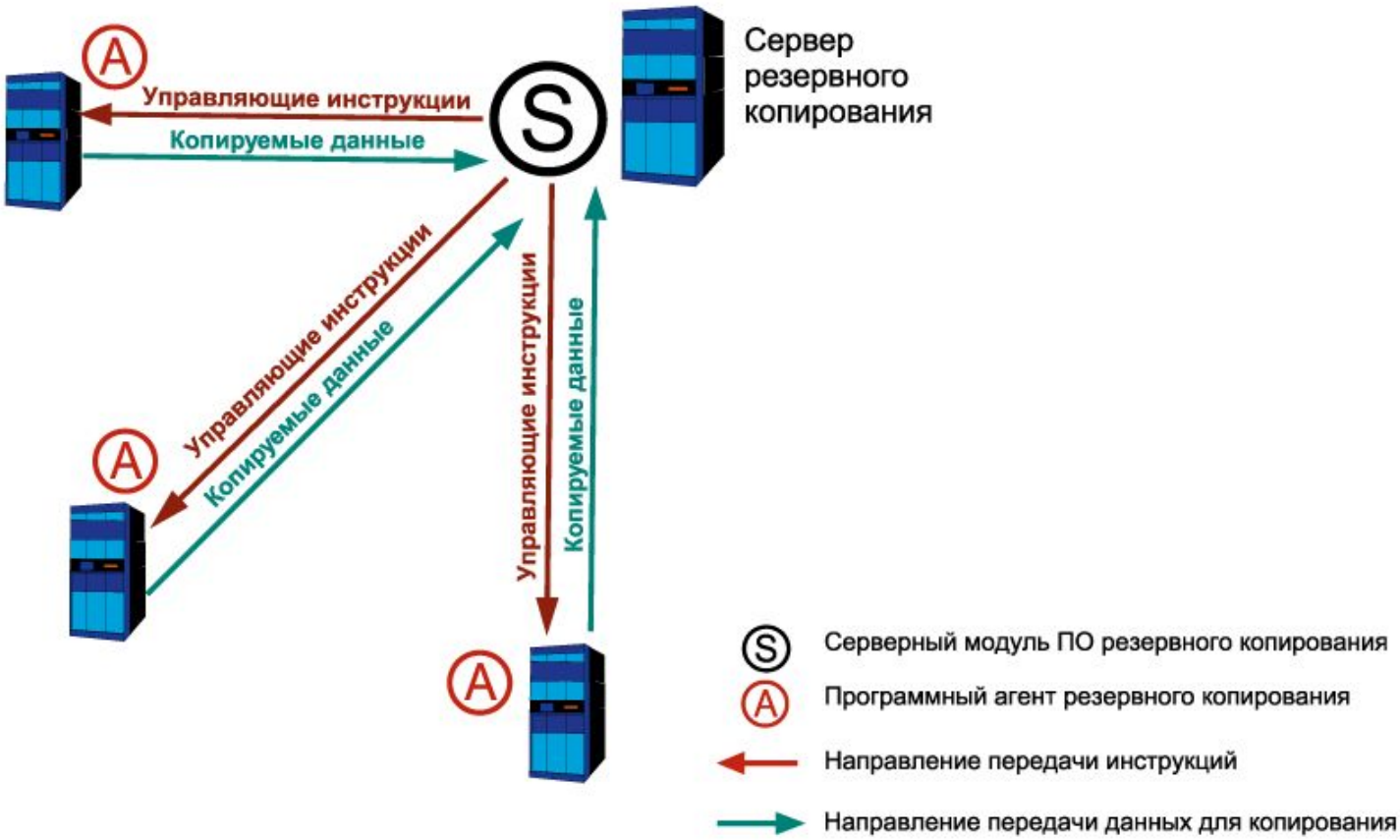
Достоинства

1. Простота реализации и невысокая стоимость;
2. Можно использовать «штатное» ПО встроенную в ОС

Недостатки

1. Сложность в настройке (расписание резервирования и т.д.);
2. Сложность в управлении;
3. Затруднен мониторинг системы

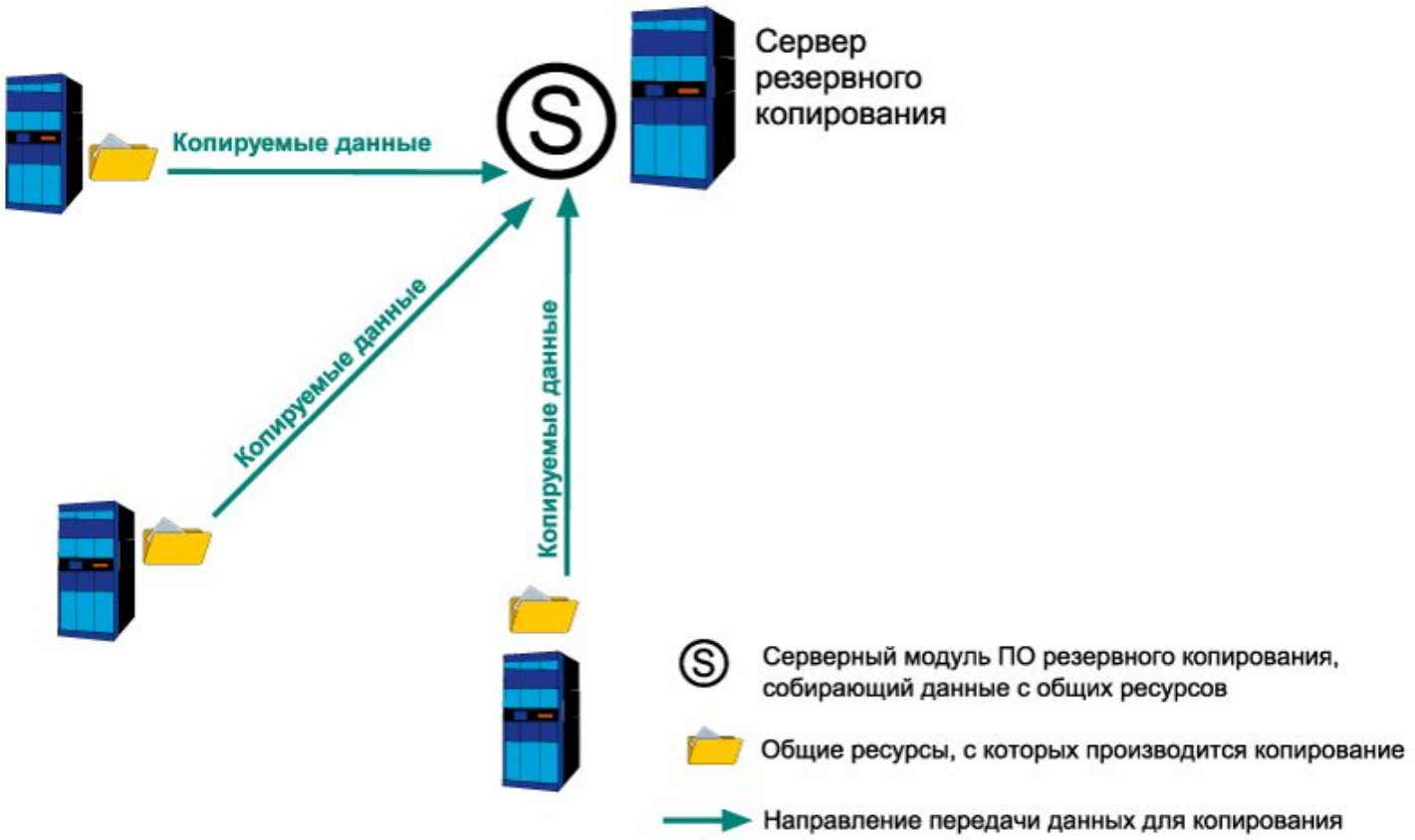
Архитектура централизованной СРКД



Программные компоненты СРКД

Сервер	отвечает за обработку трафика резервного копирования, ведет журналы операций и отвечает за обращение к накопителю для чтения – записи данных
Агент резервного копирования	отвечают за взаимодействие с сервером, обеспечивая передачу данных с клиента на сервер и обратном направлении
Консоль управления	управление системой осуществляется с консоли, устанавливаемой на одну из клиентских машин

Архитектура упрощенной централизованной СРКД



Архитектура смешенной СРКД

Off-site

Сервер

хранение зарезервированных данных за территорией предприятия

1. **Копирование на носитель**
2. **Использование «облачных сервисов»**

Требуется использование средств криптозащиты

Параметры СРКД влияющие на ее выбор

1. Время копирования - восстановления (производительность)
2. Нагрузка на канал
3. Нагрузка на дисковую систему сервера
4. Производительность сервера