

PCI DSS

Стандарт безопасности данных индустрии платёжных карт

СЕРГЕЙ ШУСТИКОВ

Генеральный директор, CISA, PCI QSA, PCI 3DS Assessor

КОНТЕКСТ СЕМИНАРА



15 лет экспертизы в информационной безопасности

Deiteriy – поставщик услуг
информационной безопасности

Компания управляет тремя
специализированными брендами



| КОМПАНИЯ DEITERIY



 Технические проекты

 Исследования

 Обучение

Консалтинг, аудиты, обучение
16 лет ведём клиентов к безопасности



 Infrastructure as Code

 Опыт

 Процессы

Управление собственным защищённым облаком
11 лет строим и защищаем облачную инфраструктуру



 Векторы атак

 Уязвимости

 Технологии

Тестирование на проникновение, ASV-сканирование
16 лет находим и эксплуатируем уязвимости

| СЕРГЕЙ ШУСТИКОВ



Сооснователь, генеральный директор



PCI QSA (с 2008 года)
PCI 3DS Assessor



Certified Information
Systems Auditor



Сертифицированный
аудитор ГОСТ Р 57580

sergey.shustikov@deiteriy.com
+7 (812) 361-61-55

ЦЕЛИ СЕМИНАРА



Мы здесь, чтобы:



Обучить стандарту PCI DSS

как новичков, так и опытных специалистов



Усилить распространение знаний

и опыта внутри платёжной индустрии



Унифицировать

подходы и принципы в работе со стандартом



Обеспечить

эффективное прохождение QSA-аудита



Повысить безопасность

качество и скорость оказания платёжных услуг

ОРГАНИЗАЦИОННЫЕ ВОПРОСЫ

1

Когда можно
задавать вопросы?

2

Будет ли доступна
презентация?

3

Будет ли доступна
запись семинара?

КОМУ И ПОЧЕМУ НУЖЕН СТАНДАРТ PCI DSS?



Торгово-сервисные предприятия

Магазины, маркетплейсы, вендинг, отели, рестораны, авиакомпании...



Поставщики услуг

Дата-центры, процессинги, агенты, агрегаторы, системы бронирования...



Банки и платежные системы

Эквайеры, эмитенты, МПС

Всем, кто принимает
оплату по картам



в свою пользу или выполняя
роль платежного агента

Всем, кого попросил регулятор



- Россия: платежная система «Мир»
- глобально: Visa, MC, UnionPay, AmEx, JCB, Discover и другие...

Всем, кто влияет на
конфиденциальность
карточных данных



предоставляя инфраструктуру и
сервисы для их обработки,
передачи, хранения и защиты

Всем, для кого это требование
контрагента



в соответствии с договором

КРАТКИЙ ЭКСКУРС В ИНДУСТРИЮ ПЛАТЁЖНЫХ КАРТ

Схема работы платёжных систем "open-loop"

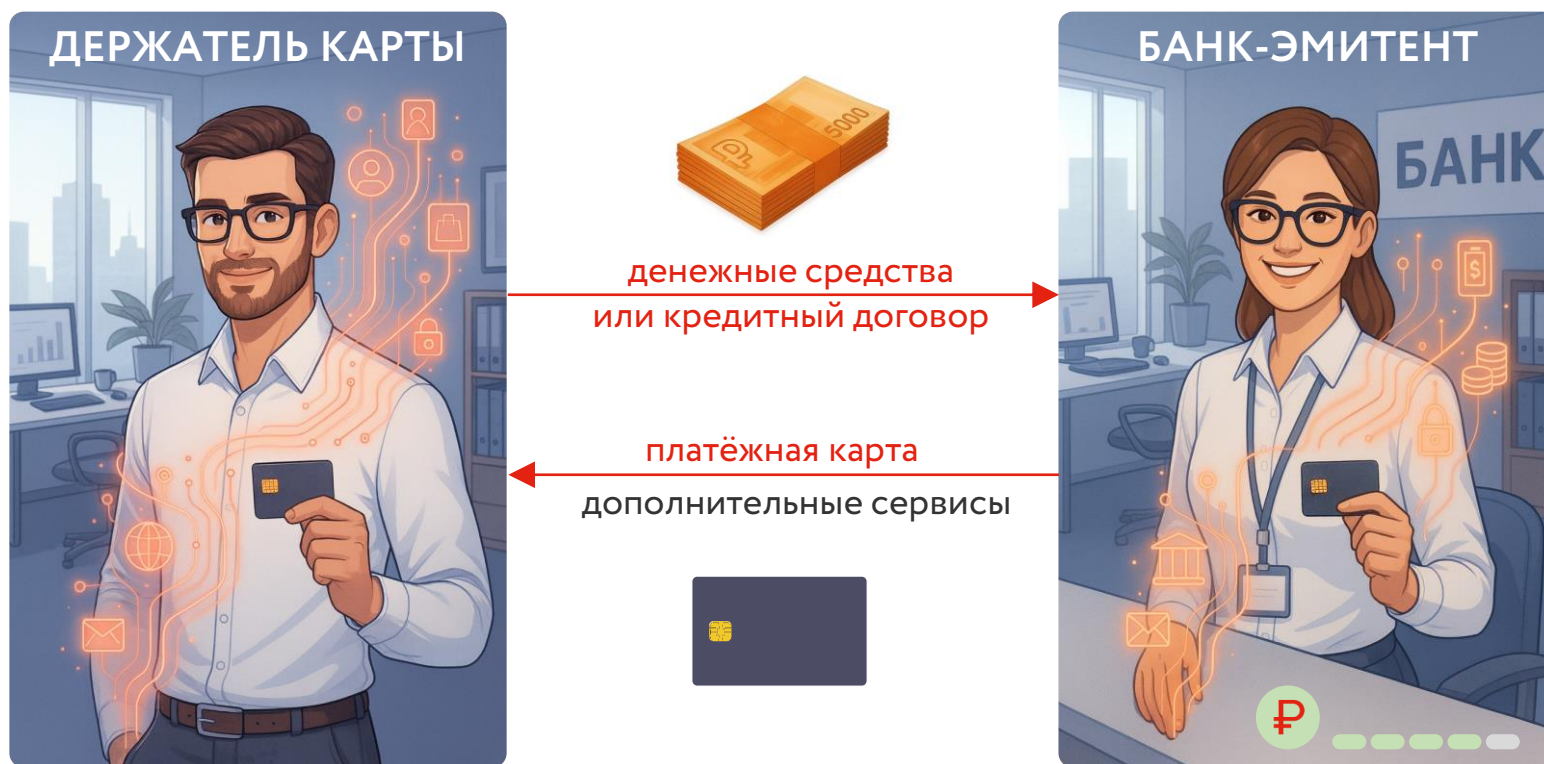
Эмиссия

- Выпуск **банком-эмитентом** платёжной карты и её выдача **держателю карты**
- Карта может быть как дебетовой, так и кредитной
- Выдача карты может осуществляться как физически, так и в электронном виде – отправкой её **данных** держателю
- Возможна привязка дополнительных **сервисов**: премиум-банкинга, консьерж-бюро, программ лояльности

Эквайринг

- Подключение торгово-сервисных предприятий к **банку-эквайеру** для приёма платежей по картам
- Различают виды эквайринга:
 - ✓ **POS-терминалы** - физическая оплата картой
 - ✓ **электронная коммерция** - ввод данных карты в форму на сайте или в мобильном приложении
 - ✓ **АТМ** – выдача наличных в банкоматах

ЭМИССИЯ



ДЕРЖАТЕЛЬ КАРТЫ



Владеет физической картой или данными виртуальной карты



Имеет право распоряжаться денежными средствами на счёте карты



Может выполнить 3DS-авторизацию



Пользуется дополнительными услугами эмитента, например программами лояльности

Возможности

- Открыл счёт в банке-эмитенте
- Имеет возможность оплатить товары и услуги везде, где на терминале есть логотип МПС
- Является единственным источником дохода всех остальных участников системы

Риски

- Является носителем карточных данных в открытом виде
- Наиболее уязвимый элемент системы
- Подвержен социальной инженерии

БАНК-ЭМИТЕНТ



Выпускает платёжные карты и передаёт их держателям



Имеет возможность авторизовывать карточные транзакции



Принимает решение о том, нужна ли ли 3DS-авторизация для транзакции



Осуществляет операции по счетам держателей карт

Возможности

- Оперирует денежными средствами клиентов
- Может предоставлять дополнительные сервисы для держателей карт: программы лояльности, консьерж-бюро, ко-брендинговые карты

Риски

- Обрабатывает карточные данные в открытом виде
- Хранит критичные аутентификационные данные

| ЭКВАЙРИНГ

Два этапа эквайринга карточной транзакции

Авторизация

- Происходит непосредственно при применении платёжной карты на POS-терминале или вводе карточных данных в платёжную форму
- Суть в получении разрешения банка-эмитента совершить данную транзакцию на данном терминале по данной карте
- Имеет таймаут, по истечении которого и не получении ответа, терминал считает транзакцию отклонённой

Клиринг и взаиморасчет

- Обычно инициируется в конце рабочего дня торгового-сервисного предприятия при закрытии смены
- В электронной коммерции может быть инициирован одновременно с авторизацией
- Суть в удовлетворении взаимных финансовых требований участников платёжной индустрии друг к другу

ЭКВАЙРИНГ: АВТОРИЗАЦИЯ



ТОРГОВО-СЕРВИСНОЕ ПРЕДПРИЯТИЕ



Торгово-сервисное предприятие, торговец, мерчант (от англ. merchant) – любой бизнес, принимающий в оплату карты за **свои** товары или услуги



Заклучил договор с банком-эквайером на услуги эквайринга – приёма платёжных карт в оплату, в рамках платёжной системы имеет уникальный номер **merchant id**



Может работать с эквайером не напрямую, а через посредника – шлюз или агрегатор

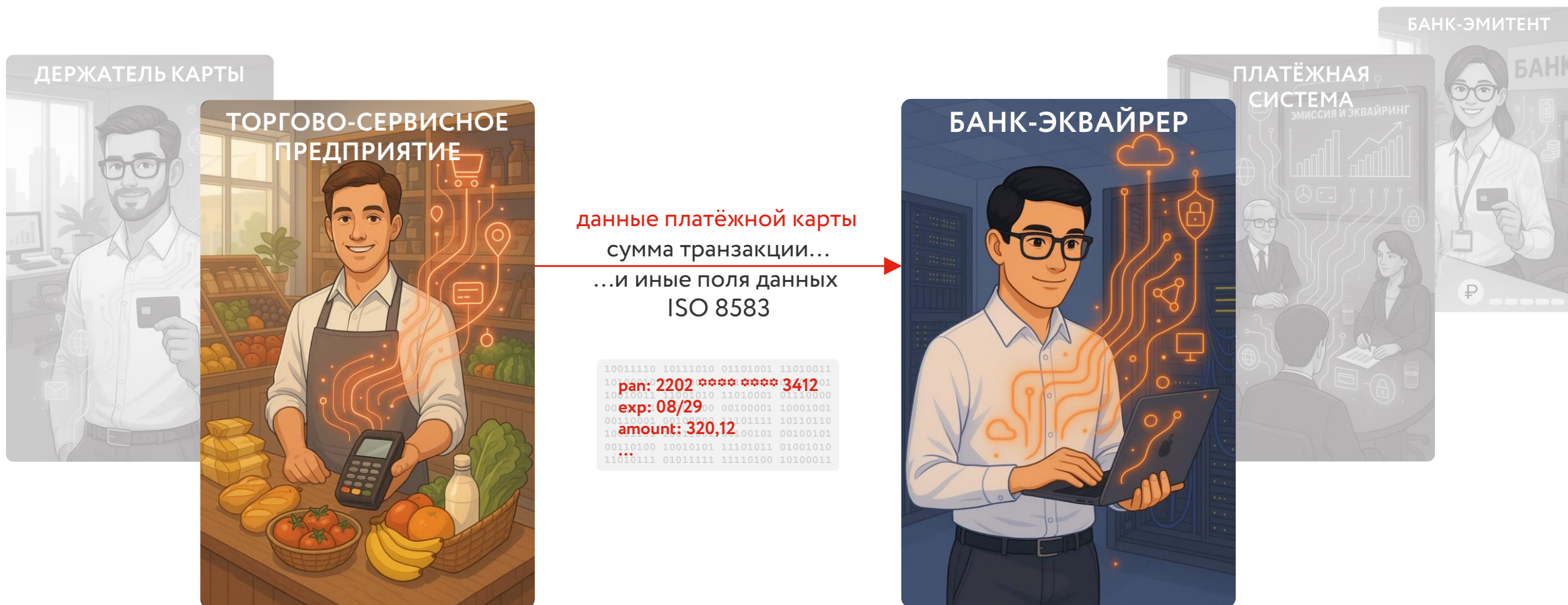
Возможности

- Открыл счёт в банке-эквайере
- Имеет один или несколько физических или виртуальных терминалов для приёма карт
- Каждый терминал в рамках платёжной системы имеет уникальный номер **terminal id**

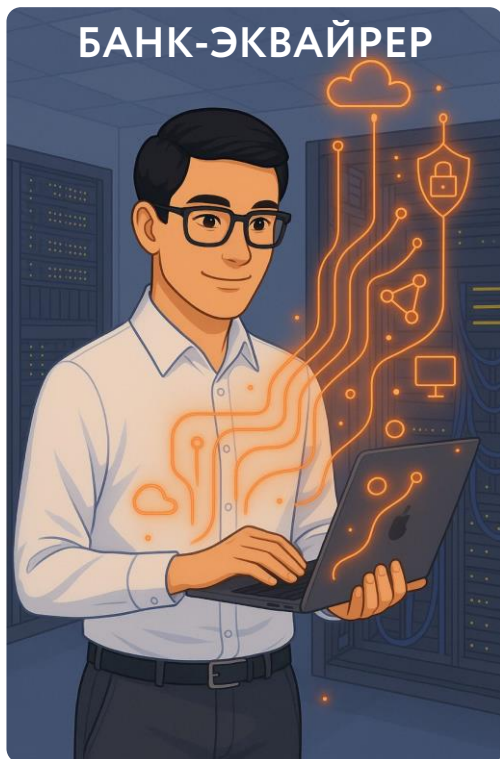
Риски

- Обработывает карточные данные в открытом виде
- Богатое видовое разнообразие: отели, магазины, вендинг, эл. коммерция
- Широкий спектр технологий

ЭКВАЙРИНГ: АВТОРИЗАЦИЯ



БАНК-ЭКВАЙРЕР



-  Банк-эквайрер – (от англ. acquiring bank) – банк – участник платёжной системы, оказывающий торгово-сервисным предприятиям услуги эквайринга
-  POS-эквайринг в точках продаж при помощи физических платёжных терминалов
-  ATM-эквайринг – выдача наличных в банкоматах
-  Эквайринг электронной коммерции при помощи программных интерфейсов (API)

Возможности

- Является прямым или косвенным участником платёжной системы
- Наделен правом и обязанностью требовать соответствия стандарту от подключенных к нему мерчантов и поставщиков услуг

Риски

- Обработывает карточные данные в открытом виде
- Несёт все риски подключенных к нему мерчантов и поставщиков услуг

ЭКВАЙРИНГ: АВТОРИЗАЦИЯ



МЕЖДУНАРОДНАЯ ПЛАТЁЖНАЯ СИСТЕМА



Платёжная система (международная платёжная система, МПС), в узком смысле – организация – оператор платёжной системы (англ. payment brand)



Сообщество банков, объединенных идеей удобства платежей между держателями карт эмитентов системы и мерчантов, подключенных к эквайерам системы



Поддерживает баланс между распространением платёжных возможностей и управлением рисками, порождаемыми доступностью технологий

Возможности

- Определяет правила платёжной системы, в том числе в части управления рисками
- Обладает статистикой по всем транзакциям платёжной системы

Риски

- Обработывает карточные данные в открытом виде
- Управляет рисками системы в целом

ЭКВАЙРИНГ: АВТОРИЗАЦИЯ



ЭКВАЙРИНГ: АВТОРИЗАЦИЯ



- 🔑 Верны ли PIN или CVV2?
- ⚠️ Нужна ли 3DS-авторизация?
- ₽ Возможна ли блокировка суммы?
- 🕵️ Каков результат антифрод-скоринга?

Успех

- Блокировка суммы на счёте держателя карты
- Внесение транзакции в журнал авторизованных
- Формирование кода ответа и кода авторизации
- Дообучение антифрод-систем



Неуспех

- Формирование кода ответа
- Дообучение антифрод-систем

ЭКВАЙРИНГ: АВТОРИЗАЦИЯ



ЭКВАЙРИНГ: АВТОРИЗАЦИЯ



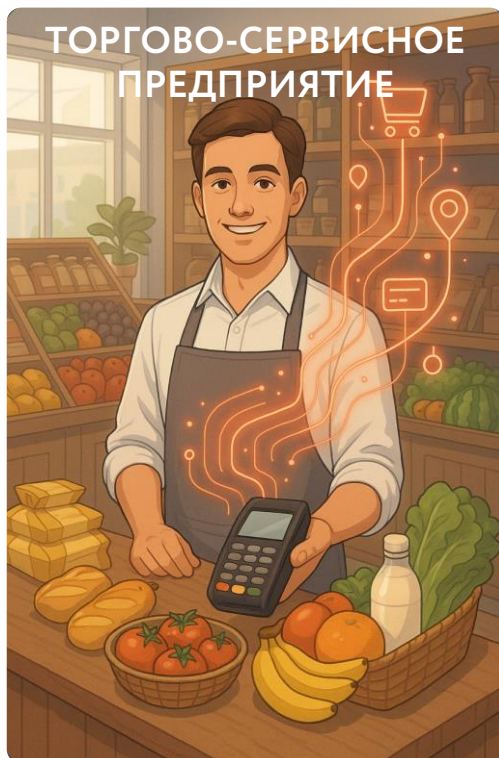
ЭКВАЙРИНГ: АВТОРИЗАЦИЯ



ЭКВАЙРИНГ: АВТОРИЗАЦИЯ



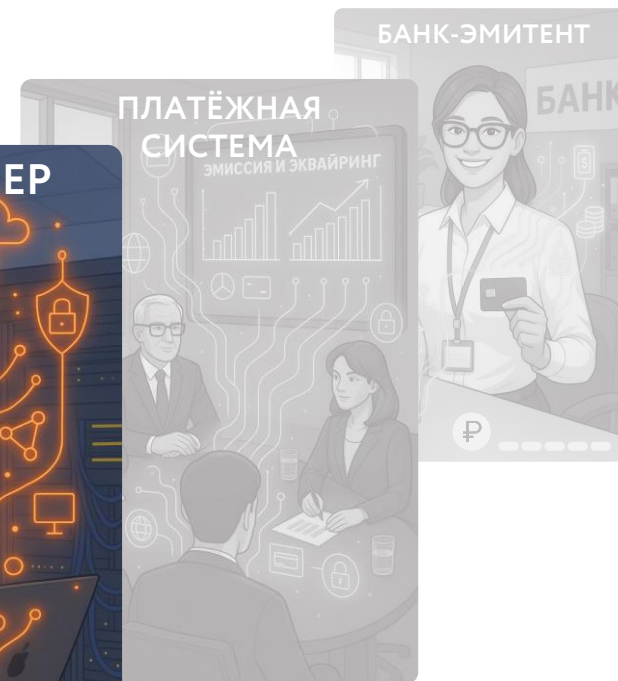
| ЭКВАЙРИНГ: КЛИРИНГ И ВЗАИМОРАСЧЁТ



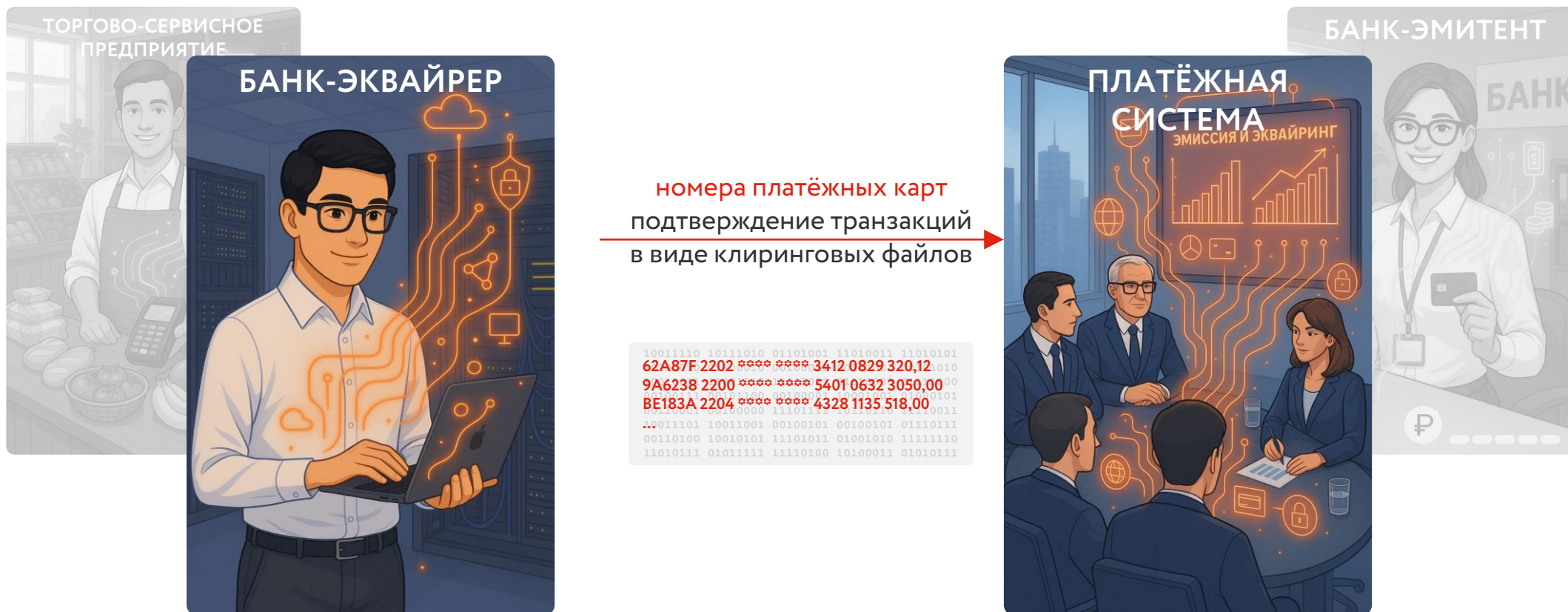
номер платёжной карты
подтверждение транзакции...
...и иные поля данных
ISO 8583

```
10011110 10111010 01101001 11010011
10100010 10100010 11010001 01110000
10010011 10100010 11010001 01110000
00110001 00100000 00100001 10001001
00110001 00100000 101111 10110110
10100011 100101 00100101
00110111 11101011 01001010
11010111 01011111 11110100 10100011
```

pan: 2202 **** * 3412
exp: 08/29
amount: 320,12
auth: 62A87F



| ЭКВАЙРИНГ: КЛИРИНГ И ВЗАИМОРАСЧЁТ



ЭКВАЙРИНГ: КЛИРИНГ И ВЗАИМОРАСЧЁТ



ЭКВАЙРИНГ: АВТОРИЗАЦИЯ



Была ли транзакция авторизована?



Возможно ли списание суммы?

62A87F 2202 **** * 3412 0829 320,12

Успех

- Списание заблокированной суммы со счёта держателя карты
- Пополнение страхового депозита эмитента в платёжной системе



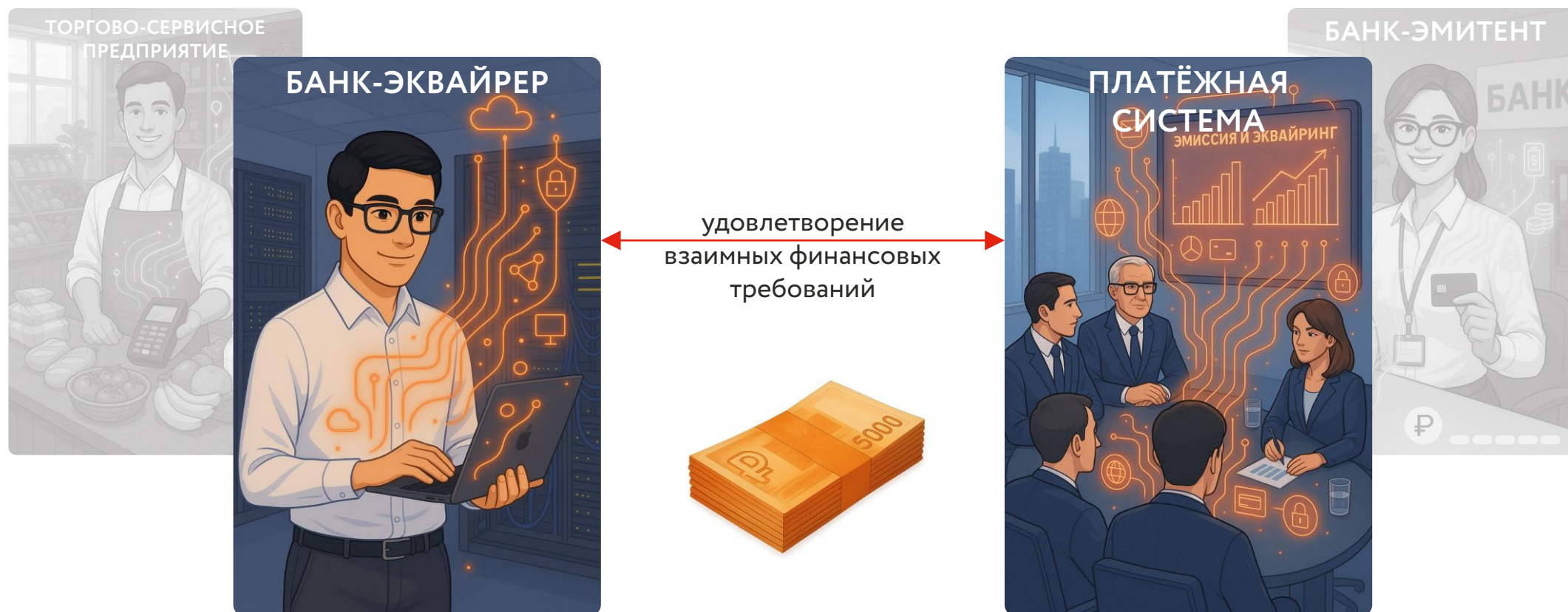
Неуспех

- Инициирование диспута
- Формирование технического овердрафта

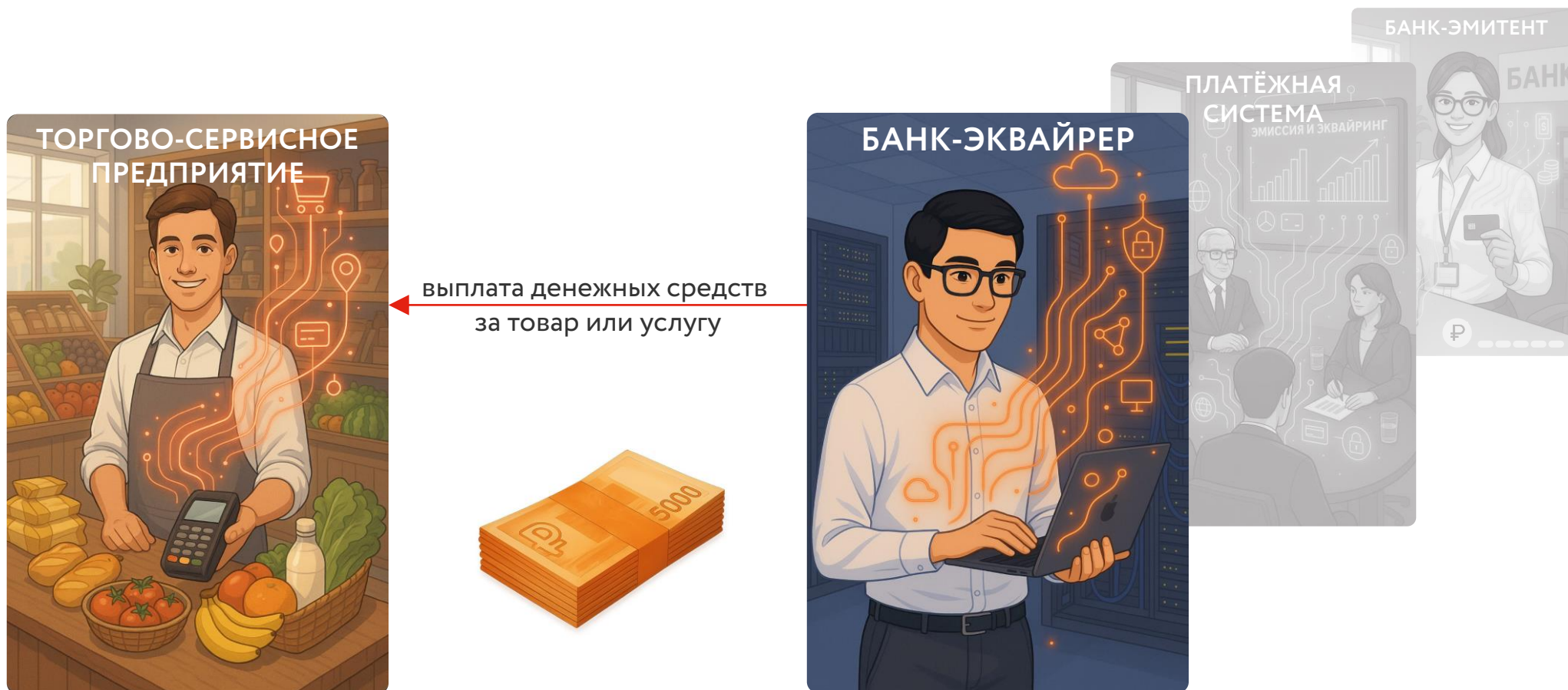
ЭКВАЙРИНГ: КЛИРИНГ И ВЗАИМОРАСЧЁТ



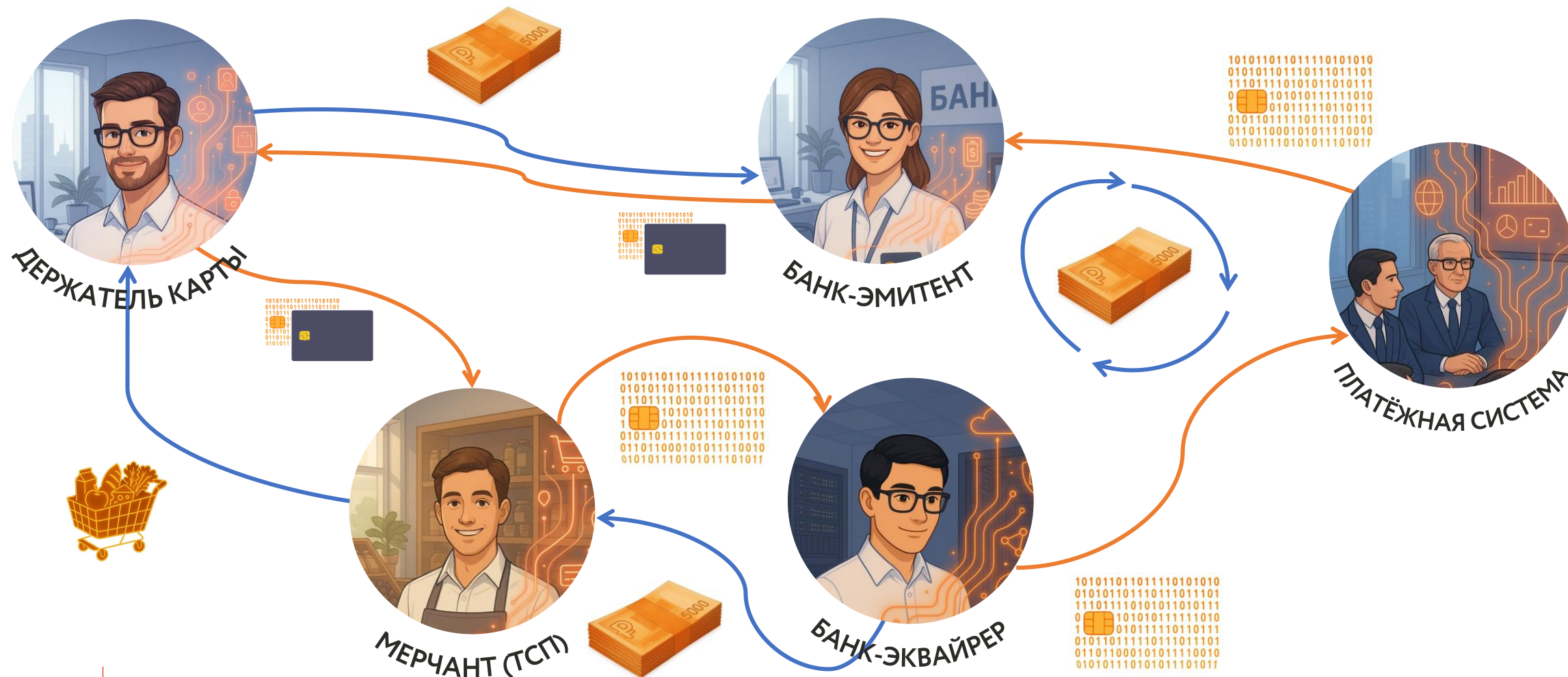
ЭКВАЙРИНГ: КЛИРИНГ И ВЗАИМОРАСЧЁТ



ЭКВАЙРИНГ: КЛИРИНГ И ВЗАИМОРАСЧЁТ



ИНДУСТРИЯ ПЛАТЁЖНЫХ КАРТ



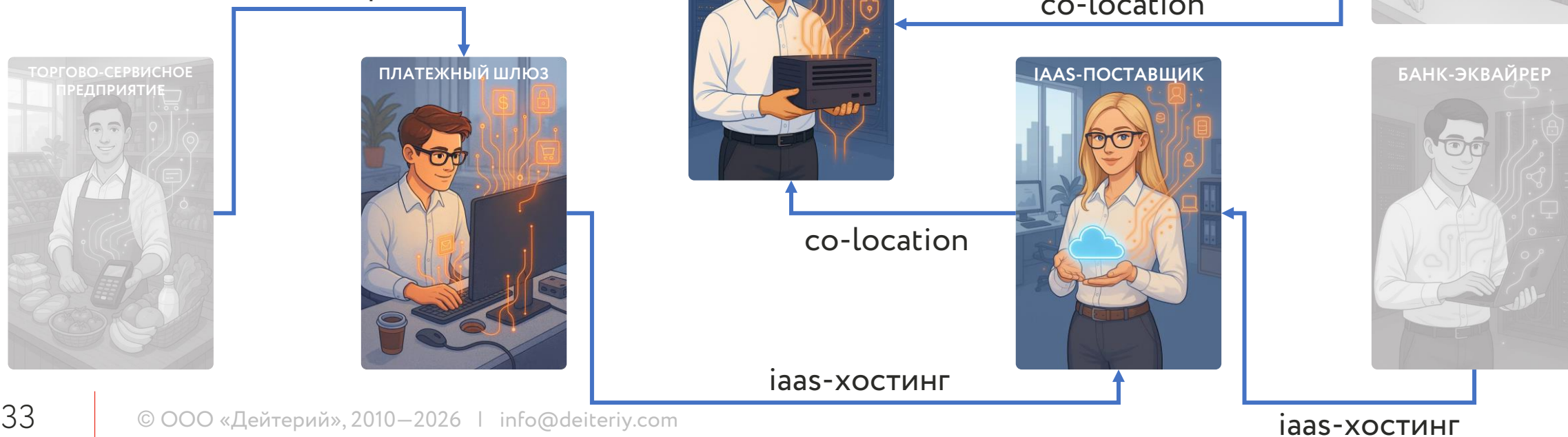
ПОСТАВЩИКИ УСЛУГ

системы бронирования
курьеры
агрегаторы

маркетплейсы

токенизаторы
консьерж-бюро
платежные агенты

SaaS



ПОСТАВЩИК УСЛУГ



Поставщик услуг, сервис-провайдер (от англ. service provider) – любой бизнес, оказывающий услуги другим участникам индустрии платёжных карт



Природа оказываемых услуг такова, что поставщик услуг прямо или косвенно может повлиять на конфиденциальность карточных данных



Опирается на других поставщиков услуг, формируя сложные цепочки зависимостей

Возможности

- Оказывает услуги многим участникам индустрии платёжных карт
- Обеспечивает индустрию гибкостью, адаптивностью, масштабируемостью
- Стимулирует внедрение новых технологий

Риски

- Часто обрабатывает карточные данные в открытом виде **в больших объемах**
- Богатое видовое разнообразие: агенты, дата-центры, IaaS, SaaS, агрегаторы
- Широкий спектр технологий

ИСТОРИЯ ПЛАТЁЖНЫХ СИСТЕМ

1950



Фрэнк Макнамара и Ральф Шнайдер основали Diners Club International – первую в мире систему платёжных карт. В 1981 году Citibank купил франшизу Diners Club.

1961



Компания Japan Credit Bureau (JCB) основана японскими банками Sanwa Bank и Nippon Shinpan. В 1968 году JCB стала лидировать в Японии и вышла на мировые рынки.

1972



Банк Lloyds впервые поставил **online-банкомат**, работавший с пластиковыми картами. Ранее в 1966 году первый offline-банкомат установил Barclays банк на сервере Лондона.

1985 **DISCOVER**

Основана финансовая компания Discover Financial Services Inc.

В 2008 году Discover купила франшизу Diners Club у Citibank.

2006



American Express, Discover, JCB MasterCard и Visa основали Совет по стандартам безопасности индустрии платёжных карт – PCI SSC и разработали стандарт PCI DSS.

1958



Компания The American Express Co., занимавшаяся международными банковскими переводами, выпустила первую платёжную карту под брендом American Express.

Bank of America выпустил первую карту BankAmericard и учредил BankAmericard Service Corporation, которая в 1976 году стала работать под брендом VISA.

1966



United California Bank, Wells Fargo, Crocker National Bank, Bank of California образовали ассоциацию Interbank Card Association (ICA), которая объединилась с европейской карточной платёжной системой Europay International (1968) и британской Access (1972). С 1979 года платёжная система работает под брендом MasterCard.

1979



VISA установила первые электронные **POS-терминалы** в точках продаж. Это было развитие разработанной BankAmericard в 1973 году электронной системы авторизации, клиринга и взаиморасчётов. Для связи использовалась телефонная линия.

1992



Book Stacks Unlimited – книжный магазин, основанный Чарльзом Стэком в формате BBS, а в 1994 году – в виде Интернет-магазина Books.com.

В 1994 Джефф Безос запустил Amazon.com.

Эра **электронной коммерции** началась после внедрения Тимом Бернерсом-Ли протокола HTTP и публикации первого браузера WorldWideWeb.

2015

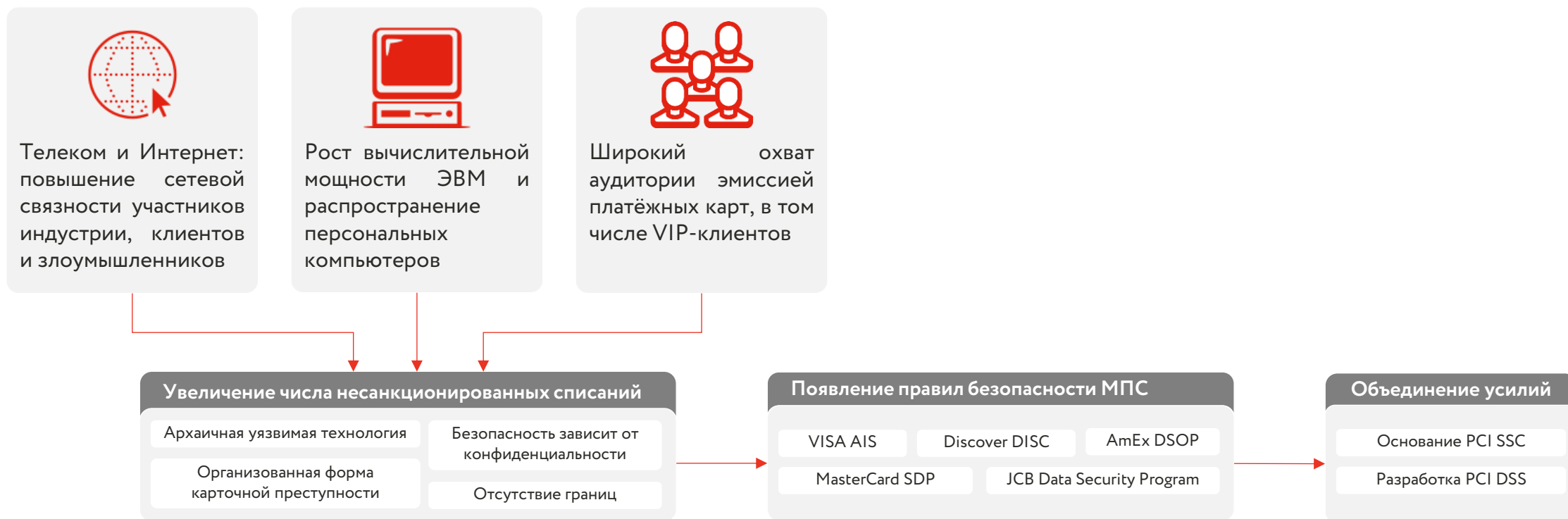


Основана российская платёжная система «Мир», оператором которой является АО «Национальная система платёжных карт» (НСПК).

В 2017 году НСПК включила в правила платёжной системы «Мир» требование об обязательном соответствии участников стандарту PCI DSS.

Данное требование является актуальным по сей день.

РАЗВИТИЕ ТЕХНОЛОГИЙ: РОСТ МОШЕННИЧЕСТВА И РЕАКЦИЯ ИНДУСТРИИ



ПРОГРАММА БЕЗОПАСНОСТИ ПС «МИР» в 2026: УРОВНИ ТОРГОВО-СЕРВИСНЫХ ПРЕДПРИЯТИЙ

	Level 1	Level 2	Level 3	Level 4
критерий:	более 6 млн транзакций в год	от 1 млн до 6 млн транзакций в год	от 20 тысяч до 1 млн транзакций в год через сайт или мобильное приложение	все остальные торгово-сервисные предприятия
ежегодно:	аудит с привлечением QSA-аудитора	аудит с привлечением QSA-аудитора	самооценка SAQ или аудит с привлечением QSA-аудитора, на усмотрение предприятия	на усмотрение банка-эквайрера
ежеквартально:	сканирование уязвимостей с привлечением российского поставщика ASV	сканирование уязвимостей с привлечением российского поставщика ASV	сканирование уязвимостей с привлечением российского поставщика ASV	на усмотрение банка-эквайрера

ПРОГРАММА БЕЗОПАСНОСТИ ПС «МИР» в 2026: УРОВНИ ПОСТАВЩИКОВ УСЛУГ

критерии:

Level 1

- обработка или передача более 300 тысяч номеров карт в год, или
- хранение в инфраструктуре более 300 тысяч номеров карт, или
- прямое подключение к операционному и платёжному клиринговому центру (ОПКЦ), или
- компрометация карточных данных в прошедшие 12 месяцев, или
- требование клиента или желание поставщика услуг создать конкурентное предложение

ежегодно:

аудит с привлечением QSA-аудитора

ежеквартально:

сканирование уязвимостей с привлечением российского поставщика ASV

Level 2

все остальные поставщики услуг

самооценка SAQ или аудит с привлечением QSA-аудитора, на усмотрение поставщика услуг

сканирование уязвимостей с привлечением российского поставщика ASV

ПРОГРАММА БЕЗОПАСНОСТИ ПС «МИР» версия 1.7: ЧТО НОВОГО?

Безопасность платежей



<https://www.nspk.ru/cards-mir/security/>

Общее правило для всех:
соответствие стандарту PCI DSS

Безопасность платежного программного обеспечения



- стороннее ПО: сертификация по стандарту PCI SSF
- собственное ПО: соответствие разделу 6 PCI DSS

Нефинансовые сервисы



- разрешается использовать только PAN и имя держателя карты
- стандарт ПС «Мир» по обеспечению безопасности данных в нефинансовых сервисах

ASV – только российский



- российская организация
- сканер хостится в России
- проксирование не допускается

Платежи по QR-коду



- Компоненты, участвующие в генерации QR-кода, должны входить в область оценки PCI DSS

Сервис проверки предприятий



- с 01.03.2026 обязанность эквайера при заключении и расторжении договора с ТСП
- код «08» – несоответствие PCI DSS



ДВА ПОДХОДА К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ