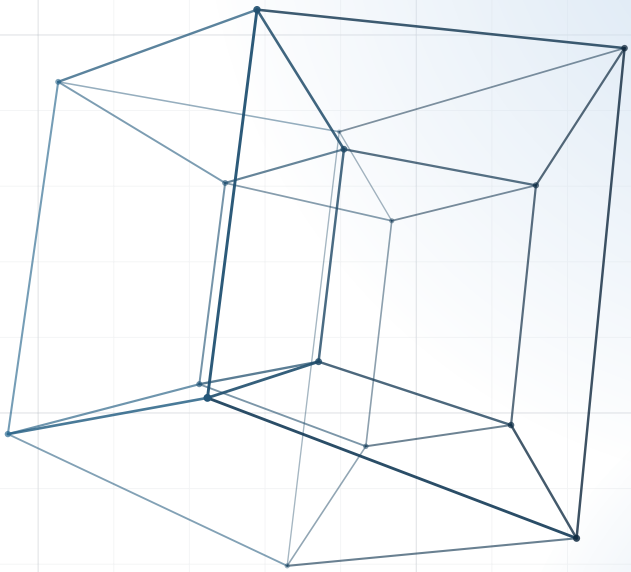
OPEN SOURCE



ИНЖЕНЕРИЯ ПЛАТЕЖЕЙ

Oleg Y. Danilkiff

Открытая книга о карточных платежах, СБП и платёжной инфраструктуре

2026

Инженерия платежей
© 2019–2026 Oleg Y. Danilkiff

Книга распространяется на условиях лицензии Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0). Полный текст: creativecommons.org/licenses/by-nc/4.0

Книга не заменяет консультацию профильного специалиста: архитектурные, юридические и комплаенс-решения принимаются с привлечением людей, которые несут за это профессиональную ответственность. Упоминание организации, продукта или сервиса не означает рекомендацию.

DOI: 10.5281/zenodo.19884844 *ORCID:* 0009-0002-8031-2575

Актуальная версия PDF: github.com/danilkiff/payments-book/releases.
Сообщить об ошибке: github.com/danilkiff/payments-book/issues.

Издание 2026 года; сборка 2026-09-27, `d358bb0`.

Предисловие

Подключить платёжный шлюз можно за день: SDK, сумма, номер карты, ответ `00` «Approved» — и кажется, что дело сделано.

Ощущение лёгкости рассеивается, когда приходит первый *chargeback*. Эмитент начинает отклонять каждую пятую транзакцию с кодом `05` «Do Not Honor» без объяснения причин. Процессинг формирует клиринговый файл, в котором суммы не сходятся с авторизациями, и непонятно, ошибка это или нет. Аудитор спрашивает, почему PAN записан в логах, и разговор переходит к нарушениям PCI DSS. К этому моменту выясняется, что `00` ничего не гарантировал.

Парадокс платёжной индустрии: подключить шлюз — один день; понять, что произошло после `Approved`, — годы. Знания в ней передаются устно, со всеми изъянами устной передачи.

Они *фрагментарны*: специалист по эмиссии не объяснит клиринг, специалист по PCI DSS не открывал EMV Book 2, архитектор не читал положение Банка России № 762-П. Каждый защищает свой участок и называет соседний «не моей зоной ответственности».

Они *искажаются при передаче*: «Visa штрафует за магнитную полосу» — верно не всегда и не в каждом регионе; у правила «3-D Secure переносит ответственность» — десяток исключений. Без первоисточника отличить правило от его упрощённой версии невозможно, а за ошибку платят чужими деньгами.

Их *не хватает на растущую команду*: одного носителя знаний на двадцать инженеров недостаточно, и новый человек приходит к тому же самому фольклору, через который прошёл его предшественник.

Эта книга выросла из заметок, которые я делал для себя несколько лет, пытаясь свести воедино источники, описывающие платежи на разных языках: технические спецификации (прежде всего EMVCo и PCI SSC), правила платёжных систем и российскую нормативную базу. Каждый написан в своей традиции, использует свою терминологию и предполагает своего читателя; согласовать их оказалось труднее, чем я предполагал вначале.

Я держался правила: ни одно утверждение в книге не должно опираться на цеховое знание без указания первоисточника. Там, где источники расходятся — а они расходятся чаще, чем хотелось бы, — расхождение отмечено явно. Там, где я не уверен, я говорю об этом прямо: «не знаю», а не «кажется как будто бы». Эта калька с английского *seems like* проросла в российский финтех как мягкий способ пофантазировать; в книге её нет.

Ошибки есть и будут: веду книгу *pro bono*, сроков правки не обещаю. Сверяйте важные факты с первоисточниками: открытыми спецификациями, нормативными актами, правилами систем — они старше этой книги и переживут её.

Предварительных знаний о платежах не требуется. Требуется готовность открыть EMV Book 2 на странице 67, чтобы убедиться, что я ничего не перепутал; без этого большая часть материала останется абстракцией.

О.Д., 2026

Как читать книгу

Книгу можно читать линейно: каждая часть опирается на предыдущие. Выборочное чтение начинается с первой части.

Часть I, «Движение денег», разбирает базовые понятия, без которых остальная книга превращается в набор разрозненных деталей: что считается деньгами в банковской инфраструктуре, кто кому должен и в какой момент, чем авторизация отличается от расчёта, как устроена сама карта и её идентификаторы, как выглядит жизненный цикл операции и как кодируются сообщения ISO 8583.

Часть II, «Безопасность и протоколы», отвечает на вопрос, почему платёжной системе вообще стоит доверять. Карта доказывает подлинность чипом, токен заменяет PAN, не разрушая жизненный цикл операции, криптография даёт общий язык секретов и подписей, 3-D Secure переносит проверку держателя в электронную коммерцию, а PCI DSS определяет цену хранения чувствительных данных. Эти главы остаются на уровне общих механизмов; конкретные сети появятся в следующей части.

Часть III, «Платёжные системы», сравнивает эти механизмы в конкретных системах: Visa и Mastercard, Мир, UnionPay, национальные карточные сети СНГ, СБП, мгновенные платежи мира, открытый банкинг, QR-кошельки, BNPL, цифровые валюты центральных банков. К каждой системе ставятся одни и те же вопросы: кто владеет правилами, какой документ главный, как достигается окончательность расчёта, что меняется для банка, продавца и процессинга при переходе с одной системы на другую. Глубина намеренно асимметрична: системы, которые чаще встречаются русскоязычному инженеру, разобраны подробнее, чем международные карточные сети.

Часть IV, «Жизнь после запуска», переходит с языка «как должен работать платёж» на язык того, что происходит с платежом уже в эксплуатации. Регулирование, идентификация клиентов и ТСП, ПОД/ФТ, санкционный скрининг, фрод, подписки, сверка, диспуты, управление отказами — темы, которые в компании распределены по разным командам, хотя сходятся на одних и тех же операциях.

Часть V, «Архитектура», снова собирает компоненты в систему: платёжный шлюз, внутренний реестр обязательств, мультивалютная логика, процессинговый центр. Эта часть показывает, какой компонент за что отвечает и почему роли разделены именно так.

Главная ошибка перевода в финтехе — насильственная русификация: «обратный вызов» вместо вебхука, «криптограмма авторизационного запроса» там, где достаточно ARQC. В книге другой подход: русский канон для устоявшихся российских понятий (ТСП, эквайер, сверка, фрод); английский — для индустриальных терминов, перевод которых мешает узнаванию (chargeback, PayFac, EMV, 3-D Secure, interchange). Первое упоминание даёт пару «русский (*english*)», далее — короткая форма. Полный список — в Глоссарии.

Если место в продвинутой главе непонятно, ищите ответ в главах части I: на её словаре движения денег, сообщений и обязательств построено всё остальное.

Оглавление

Часть I

Движение денег

Покупатель прикладывает карту или нажимает кнопку на странице оплаты, терминал печатает чек или приложение сообщает об успешной оплате — и кажется, что произошло одно событие, в котором деньги «перешли» от плательщика к получателю. За этим событием стоят разные понятия: сообщение о намерении совершить операцию, денежное обязательство между участниками и собственно расчёт, который может произойти позже, по другому каналу и по другим правилам.

Смешение этих понятий искажает базовые термины книги. *Авторизация* становится *переводом* денег. *Клиринг* превращается в подтверждение того, что и так случилось, а регуляторные требования — в посторонний нарост на техническом потоке.

Платёжная система связывает их между собой. Она фиксирует, кто и когда меняет запись в своём учёте и в какой момент операция становится необратимой. До этого момента её ещё можно отозвать, оспорить, скорректировать.

Часть начинается с базовых вопросов: что вообще считается деньгами в банковской инфраструктуре, кто несёт обязательства и как одно учреждение узнаёт, что другое должно изменить состояние счёта. Дальше — формы денег и различие между банковским переводом и карточной операцией. После этого — сама карта, её идентификаторы и признаки подлинности; без этого PAN, ответ авторизации и фактический расчёт сливаются воедино, хотя относятся к разным уровням системы.

Каждая глава части возвращается к сквозным темам:

- жизненный цикл и базовые этапы карточной операции — отклонения от них рассматриваются в последующих частях;
- контроль безопасности — как система убеждается, что операция допустима, карта подлинна, держатель легитимен;
- юридические роли и то, почему техническая архитектура оказывается одновременно правовой.

1 Деньги между банками

Клиент банка А переводит сто тысяч рублей клиенту банка Б; в мобильном приложении это одно действие: ввести сумму, нажать кнопку, дождаться статуса «исполнено». На каждой ступени этого пути меняются форма денег, обязанная сторона и система учёта, в которой это обязательство зафиксировано. Что именно движется между участниками, кто имеет право менять учётные записи и в какой момент перевод считается исполненным — вопросы этой главы.

1.1 Формы денег

Деньги существуют в нескольких формах, и каждая подчиняется собственным правилам учёта, хранения и передачи. Разработчик, впервые столкнувшись с платёжной системой, видит деньги как поле `amount` с типом `decimal`, которое можно увеличить или уменьшить. Эта модель работает в коде и перестаёт работать, когда деньги переходят из одной формы в другую.

Российское право различает формы рубля: наличные, безналичные деньги и, с 2023 года, цифровой рубль. 161-ФЗ отдельно вводит *электронные денежные средства*: юридически это особая конструкция рядом с наличной и безналичной формами [1].

Наличные

Передача наличных не требует посредника и завершается в момент физического вручения. Покупатель протягивает купюру продавцу, продавец кладёт её в кассу; расчёт окончен, никакой банк не участвует, никакая запись в реестре не нужна. Вопрос «дошли ли деньги?» не возникает в принципе: деньги перешли из рук в руки на глазах у обоих участников.

Юридически наличные — обязательство Центрального банка. По Федеральному закону от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации» банкноты и монета Банка России обеспечиваются всеми его активами [2]. Эмиссия наличных — монопольное право ЦБ; безналичные деньги, напротив, создают коммерческие банки, выдавая кредиты.

Безналичные деньги

Когда клиент вносит сто тысяч рублей на счёт в банке, наличные перестают существовать как наличные и превращаются в запись на банковском счёте, то есть в обязательство коммерческого банка перед клиентом. У клиента больше нет той же купюры — у него появилось требование к банку, юридически отличное от наличных, с которыми он только что пришёл.

Различие между наличными и безналичными в обыденной жизни незаметно, пока банк выдаёт наличные по первому требованию. По Федеральному закону от 23.12.2003 № 177-ФЗ «О страховании вкладов» базовое страховое возмещение покрывает до 1,4 миллиона рублей на одного вкладчика в одном банке; с 30 октября 2025 года для рублёвых вкладов, удостоверенных безотзывными сберегательными сертификатами сроком свыше трёх лет, действует отдельное покрытие до 2,8 миллиона рублей, и общий потолок по двум видам вкладов достигает 4,2 миллиона рублей.

Страхование покрывает риск банка: безналичные деньги — обязательства коммерческого банка, а коммерческий банк может обанкротиться. Банкнота в кармане от банкротства конкретного банка не зависит [3].

В платёжных системах безналичные деньги требуют изменения записей минимум в двух местах. Если оба счёта находятся в одном банке, операция сводится к внутрибанковской проводке и выполняется мгновенно. Банк контролирует оба счёта и меняет записи атомарно. Если счёта расположены в разных банках, две независимые учётные системы должны *согласованно* изменить свои записи, не потеряв и не удвоив деньги по пути. Для этого и существуют *корреспондентские счета* — счета, которые один банк открывает в другом банке для проведения межбанковских расчётов.

Электронные денежные средства и цифровой рубль

161-ФЗ описывает электронные денежные средства (ЭДС) как денежные средства, предварительно предоставленные лицом оператору, который учитывает их без открытия банковского счёта и обязуется переводить их по распоряжениям этого лица [1]. ЭДС существуют в виде кошельков вроде тех, что когда-то предлагали Яндекс.Деньги (ныне ЮMoney) и Qiwi: клиент пополняет кошелёк, оператор хранит баланс и по команде переводит средства получателю. Банковский счёт не открывается, остаток кошелька не покрывается страхованием вкладов.

Для инженера, проектирующего платёжный продукт, различие между безналичными деньгами и ЭДС проявляется в лицензировании и лимитах. Оператор ЭДС обязан быть кредитной организацией (банком или небанковской кредитной организацией, НКО), а лимиты на остаток и оборот зависят от *уровня идентификации клиента*: для неперсонифицированных и упрощённо идентифицированных пользователей закон задаёт разные пороги по остатку и операциям; для персонифицированных пользователей лимиты выше [1].

Федеральный закон от 24.07.2023 № 340-ФЗ «О цифровом рубле» [4] добавил к наличным и безналичным деньгам третью форму рубля: цифровой рубль — прямое обязательство Банка России, хранящееся на платформе ЦБ; коммерческие банки лишь предоставляют клиентам доступ к этой платформе. По обязанной стороне цифровой рубль ближе к наличным, чем к безналичным; передача всегда проходит через платформу и оставляет прослеживаемый след. Архитектура цифрового рубля разобрана в гл. 24, взаимодействие с системой быстрых платежей (СБП) — в гл. 19.

1.2 Корреспондентские счета

Банк А списывает средства со счёта отправителя — это его внутренняя операция. Зачислить деньги на счёт получателя в банке Б он не может, потому что чужой учётной системой не управляет. Решение этой проблемы появилось задолго до компьютеров и карточных сетей — корреспондентские счета.

У такого счёта две стороны, и названия их закрепились ещё в итальянской банковской практике. Счёт, открытый *нашим* банком *в чужом*, называется *ностро-счётом* (от итальянского *nostro* — «наш»); тот же самый счёт с точки зрения банка, в котором он открыт, называется *лоро-счётом* (от итальянского *loro* — «их»). Один и тот же счёт всегда одновременно ностро для одного банка и лоро для другого: термин фиксирует лишь точку зрения.

Пусть банк А открыл корреспондентский счёт в банке Б (это ностро-счёт банка А и лоро-счёт для банка Б), и остаток счёта покрывает перевод. Клиент банка А инициирует перевод. Банк А списывает средства со счёта клиента и отправляет банку Б сообщение: «спиши сто тысяч с нашего ностро-счёта у тебя и зачисли на счёт такого-то получателя». Банк Б дебетует лоро-счёт банка А, уменьшая остаток, который банк А держит у него, и кредитует счёт получателя. Перевод завершён.

Эта схема требует прямых двусторонних связей между каждой парой банков: один из них должен открыть счёт у другого, а чаще оба открывают счёта друг у друга. При тысяче банков в стране число возможных пар составляет около полумиллиона, и поддерживать полмиллиона двусторонних отношений слишком дорого и трудоёмко.

Двусторонняя сеть превращается в звезду, когда появляется центральный корреспондент, у которого остальные банки держат корреспондентские счёта. В России эту роль выполняет Банк России. Банки переводят средства через счета, открытые в Банке России, и через ту же систему завершается расчёт по карточным операциям внутри страны [5]. Когда клиент банка А переводит деньги клиенту банка Б, последовательность событий такова (см. рис. 1):

- Банк А списывает средства со счёта отправителя.
- Банк А направляет платёжное поручение в платёжную систему Банка России.
- Банк России дебетует корреспондентский счёт банка А и кредитует корреспондентский счёт банка Б. Фактическое перемещение денег между банками происходит здесь: оба счёта находятся в одной учётной системе Центрального банка, и он изменяет обе записи атомарно.
- Банк Б зачисляет средства на счёт получателя. Этот шаг отражает уже состоявшийся расчёт во внутреннем учёте банка Б.

На схеме счёт 40817 — счёт физического лица. В учёте банка корреспондентский счёт в Банке России отражается на балансовом счёте 30102 по Плану счетов кредитных организаций, установленному Положением Банка России от 24.11.2022 № 809-П «О Плане счетов бухгалтерского учёта» [6]. В платёжных реквизитах используется двадцатизначный корреспондентский счёт, открытый в Банке России; его значение берут из Справочника БИК платёжной системы Банка России. Приложение 5 к Положению Банка России от 03.12.2025 № 876-П «О платёжной системе Банка России» описывает БИК, Справочник БИК и реквизиты «Номер счета», «Тип счета» [5, 7]. Первые пять цифр этого счёта — 30101: это сторона баланса Банка России, а не счёт 809-П кредитной организации [8].

Поле «БИК» в реквизитах перевода идентифицирует банк в платёжной системе Банка России; Справочник БИК Банк России предоставляет в формате ED807 [5]. В карточных расчётах банк определяется по BIN (Bank Identification Number).

В международных расчётах единого центрального корреспондента нет. Роль посредников берут на себя крупные *банки-корреспонденты*, и цепочка растягивается до трёх-четырёх звеньев: от банка отправителя через одного или нескольких посредников к банку получателя. Каждое звено образует пару корреспондентских счетов, каждая проводка означает дебет одного счёта и кредит другого. На каждом переходе банк-посредник может удержать комиссию, конвертировать валюту и задержать перевод для проверки на соответствие требованиям регулятора, в том числе санкционным и антиотмывочным. Международный банковский перевод дорог и медлителен; карточные сети отличаются единой расчётной инфраструктурой и предсказуемым сроком расчёта.

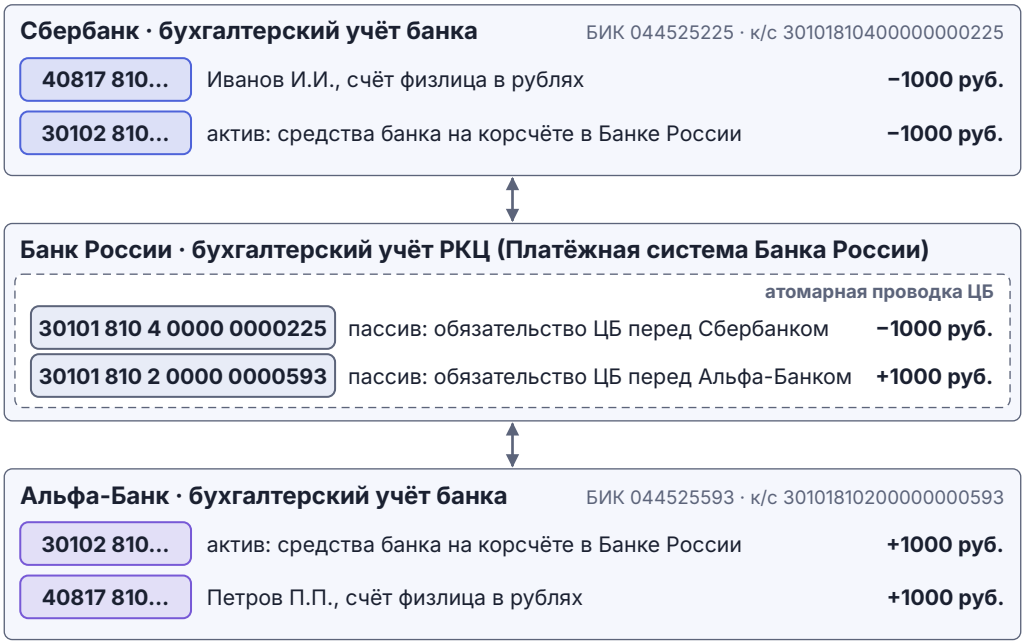


Рис. 1 — Перевод 1000 руб. из Сбербанка в Альфа-Банк через корреспондентские счета в Банке России.

1.3 Платёжная инфраструктура: ПС Банка России, SWIFT, СПФС

Корреспондентские счета определяют, *где* учитываются деньги. *Как* банк А передаёт банку Б (или Центральному банку) распоряжение о переводе, в каком формате и с какими гарантиями доставки, определяет платёжная инфраструктура — системы и протоколы, через которые передаются платёжные сообщения и проводится расчёт.

Платёжная система Банка России

Основу внутрироссийских межбанковских расчётов составляет платёжная система Банка России. Через неё проходят и обычные клиентские переводы, и налоговые платежи, и операции на межбанковском рынке [5]. Она предлагает несрочный перевод рейсами для рутинного потока и срочный перевод (RTGS) для крупных межбанковских операций.

Обычные переводы накапливаются в течение операционного дня и проходят несколько *расчётных рейсов*. После каждого рейса банк получает результат; окончательный расчёт включает проверку достаточности средств на корреспондентском счёте, формирование внутридневной очереди и, где возможно, взаимозачёт. Рейсовый расчёт покрывает основной объём рутинных платежей: зарплаты, оплату поставщикам, коммунальные платежи. Банку хватает небольшого остатка на корреспондентском счёте: часть входящих и исходящих платежей зачитывается внутри рейса.

Срочные платежи проходят через сервис срочного перевода ПС Банка России по модели RTGS (Real-Time Gross Settlement, валовой расчёт в реальном времени). Каждый платёж проводится отдельно и немедленно, без накопления и без взаимозачёта. Средства списываются с корреспондентского счёта банка-отправителя и зачисляются на счёт банка-получателя по каждому платежу отдельно [5]. Срочный перевод обходится банку дороже, чем несрочный рейсовый, и даёт почти мгновенную окончательность расчёта, которой требуют крупные межбанковские сделки и операции денежного рынка. Исторически функцию RTGS внутри ПС Банка России выполняла отдельная компонента БЭСП (банковские электронные срочные платежи), переставшая проводить переводы 2 июля 2018 года; её функции перенесены в Перспективные платёжные сервисы (ППС) Банка России.

Сервис срочного перевода ПС Банка России и система быстрых платежей (СБП) быстро завершают платёж, но обслуживают разных клиентов. Сервис срочного перевода работает как *межбанковская* система RTGS для крупных и срочных платежей между банками, тогда как СБП — *розничная* платёжная система для мгновенных переводов физических лиц и оплаты покупок, работающая через инфраструктуру НСПК (Национальной системы платёжных карт).

SWIFT и СПФС

Международные межбанковские расчёты традиционно работают через SWIFT (Society for Worldwide Interbank Financial Telecommunication) — кооперативную организацию, основанную в 1973 году и объединяющую около 11 500 участников более чем в 200 странах: банки, финансовые организации и крупные корпорации [9].

SWIFT доставляет структурированное сообщение от одного банка к другому — например, инструкцию «переведи столько-то с нашего ностро-счёта у тебя на счёт такого-то клиента». Фактическое движение денег происходит по корреспондентским счётам, описанным в предыдущем разделе, а за исполнение инструкции отвечает банк-получатель.

Сообщения SWIFT исторически передавались в формате MT (Message Type): MT103 — клиентский перевод, MT202 — межбанковский перевод, MT940 — выписка по счёту. Переход к MX перевёл платёжные инструкции на XML-формат на базе ISO 20022. К 22 ноября 2025 года SWIFT по программе CBPR+ (Cross-Border Payments and Reporting Plus, миграция трансграничных платежей и отчётности на ISO 20022) завершил период сосуществования MT и ISO 20022; для платёжных инструкций ISO 20022 стал базовым форматом [10, 11].

СПФС (Система передачи финансовых сообщений) — инфраструктура обмена финансовыми сообщениями Банка России, созданная как российская альтернатива SWIFT. Банк России описывает СПФС как канал передачи электронных сообщений по финансовым операциям; сами расчёты кредитные организации проводят по корреспондентским счетам [12]. По функциональности СПФС аналогична SWIFT: передаёт структурированные финансовые сообщения и поддерживает несколько форматов — SWIFT MT, ISO 20022 (MX), УФЭБС (унифицированные форматы электронных банковских сообщений Банка России) и пользовательские форматы, согласованные участниками.

От SWIFT СПФС отличается юрисдикцией: систему контролирует Банк России, данные хранятся в Российской Федерации, подключение регулируется российским законодательством.

Банку, обслуживающему и внутрироссийские, и международные переводы, нужны СПФС для внутренних операций и SWIFT (или его альтернативы) — для международных. Форматы сообщений пересекаются (ISO 20022, SWIFT MT), но маршрутизация, правила идентификации участников и требования комплаенса различаются; модуль, общий для обоих каналов, должен применять к каждому сообщению правила его канала.

1.4 Банковский перевод и карточная транзакция

Карточная транзакция устроена сложнее классического банковского перевода. Когда покупатель прикладывает карту к терминалу, деньги *не переходят* к продавцу сразу. Банк, выпустивший карту (эмитент), лишь подтверждает готовность заплатить; банк продавца (эквайер) получит деньги позже, а фактическое межбанковское урегулирование произойдёт после клиринга и расчёта (роли участников описаны в разделе 2.2).

Авторизация занимает доли секунды. Терминал отправляет запрос по платёжной инфраструктуре, эмитент проверяет карту, баланс и лимиты, прогоняет операцию через антифрод и возвращает код одобрения `00` или код отказа. При одобрении эмитент резервирует сумму на счёте держателя карты, но не списывает её окончательно и не переводит деньги в расчёты.

Клиринг (*clearing*) происходит позже, в конце операционного дня. Эквайер собирает все авторизованные операции за день и передаёт их в карточную сеть клиринговым файлом — структурированным набором записей с реквизитами транзакции, суммой, валютой и ссылкой на авторизацию. Карточная сеть сопоставляет клиринговые записи с авторизациями, рассчитывает комиссии и формирует итоговые расчётные позиции для банков-участников.

Расчёт (*settlement*) завершает цикл. Карточная сеть или уполномоченный расчётный банк инициирует фактическое перемещение денег между корреспондентскими счётами банков. Эквайер получает причитающуюся сумму за вычетом комиссий, эмитент окончательно списывает средства со счёта держателя карты. Для внутрироссийских карточных операций обработка и клиринг проходят через инфраструктуру НСПК, а расчёты завершаются в платёжной системе Банка России [5].

Из-за отставания расчёта от авторизации холды (*hold*) на карте держателя сохраняются по нескольку дней, пока клиринговая запись не будет сопоставлена с авторизацией. Авторизация может прийти на одну сумму, а в клиринге — на другую: типичный случай — ресторан, где чаевые добавляются уже после получения кода одобрения. Отмена карточного платежа зависит от стадии, на которой транзакция находится в момент отмены: авторизации, клиринга или расчёта.

Разделение *на авторизацию и клиринг* продиктовано скоростью и масштабом. Банковский перевод допускает задержку в минуты или часы (СБП сократила её до секунд), и каждый перевод обрабатывается индивидуально. Карточный платёж должен завершиться за секунды: покупатель стоит у кассы, а межбанковский расчёт по каждой покупке задержал бы очередь.

Разделение *на авторизацию и расчёт* даёт мгновенный ответ без мгновенного перемещения денег: эмитент обещает заплатить, продавец отпускает товар, фактический перевод происходит позже, пакетами, через расчётную инфраструктуру карточной сети. Встречные потоки взаимозачитываются, и объём межбанковских проводок сокращается по сравнению с индивидуальным расчётом каждой транзакции.

Жизненный цикл карточной транзакции, от прикладывания карты к терминалу до расчёта, подробно разбирается в гл. 5; формат сообщений на этапе авторизации рассматривается в гл. 6. Если перевод между двумя счетами в разных банках — это согласованное изменение записей в двух местах, то карточная транзакция — это обещание заплатить, которое выполняется позже. Между обещанием и исполнением возникает расчётный риск: эмитент может одобрить операцию и обанкротиться до клиринга.

Этот риск принимает на себя платёжная сеть: правила Visa и Mastercard обязывают её возместить эквайеру неурегулированную сумму, если эмитент не исполнит обязательство по расчёту, а участники с повышенным риском вносят обеспечение деньгами, аккредитивами или гарантиями материнской структуры. Механизм покрытия разобран на примере Visa в разделе 14.2.

Внутрироссийские карточные операции через ОПКЦ НСПК завершаются клирингом и расчётом в следующий операционный день: ОПКЦ формирует клиринговую позицию, а расчётные услуги по национальным платёжным инструментам Банк России оказывает по корреспондентским счетам участников [1]. Международные операции Visa и Mastercard рассчитываются по календарю клиринговой сессии конкретной валюты; для долларовых платежей типичный срок расчёта — T+1 [13, 14]. Под неурегулированные авторизации эмитент держит на счёте уполномоченного расчётного банка сети обеспечение: денежный депозит, аккредитив или гарантию материнской структуры. Если у эмитента к моменту утреннего расчётного цикла не хватает остатка, сеть закрывает позицию из этого обеспечения и приостанавливает или прекращает членство эмитента в сети. При добровольном прекращении членства это обеспечение освобождается только после закрытия расчётного риска по операциям эмитента: неурегулированным авторизациям и незакрытым *chargeback*.

Глава 2 разбирает участников карточной экосистемы — эмитента, эквайера, сеть, процессор, шлюз, фасилитатор — и экономику взаиморасчётов через interchange; гл. 3 углубляется в функции эмитента и эквайера: CMS, TMS, маршрутизацию, обработку диспутов. К карточной транзакции как к технической последовательности сообщений книга возвращается в гл. 6 на уровне формата ISO 8583.

2 Карточная экосистема

Между покупателем и продавцом оказываются два банка, карточная сеть и нередко ещё процессор или PSP (payment service provider, провайдер платёжных услуг). Конструкция держится на межбанковской комиссии (interchange): эмитент знает клиента и несёт кредитный риск, эквайер подключает продавца и отвечает за приём, сеть передаёт сообщения, а расчёт между банками проходит в несколько фаз.

2.1 Четырёхсторонняя модель

Держатель карты (cardholder) инициирует платёж. Продавец — торгово-сервисное предприятие, ТСП, merchant — принимает его. Эмитент (issuer) отвечает за сторону плательщика, эквайер (acquirer) — за сторону продавца. Вместе они образуют четырёхстороннюю модель (four-party model, иногда four-corner model), на которой построены платёжные системы Visa, Mastercard и Мир [5, 13, 15]. Поверх этой конструкции работает карточная сеть (card network, payment scheme). Сеть задаёт правила, передаёт сообщения и проводит расчёты, но юридически остаётся вне сделки между покупателем и продавцом.

Покупатель и продавец не могут провести карточный платёж вдвоём: им не хватает ни масштаба, ни доверия. Продавец не проверит, есть ли у покупателя деньги на счёте в другом банке; покупатель не гарантирует оплату без участия своего банка. Между ними встают банки: эмитент знает покупателя и подтверждает его платёжеспособность, а эквайер знает продавца и обязуется зачислить ему деньги после расчёта. Карточная сеть связывает их общими правилами и технической шиной, избавляя от необходимости договариваться напрямую. Развёрнутые определения эмитента и эквайера — в разделе 2.2.

Без карточной сети каждый из N эмитентов и M эквайеров должен был бы заключать двусторонний договор — $N \times M$ соглашений. Карточная сеть сводит эту задачу к $N + M$. Каждый эмитент подписывает одно лицензионное соглашение с сетью, каждый эквайер — своё. С этого момента карта любого эмитента принимается у любого эквайера, потому что оба подчиняются единым правилам сети. Карта Visa, выпущенная региональным банком в сербском Нови-Саде, работает в терминале

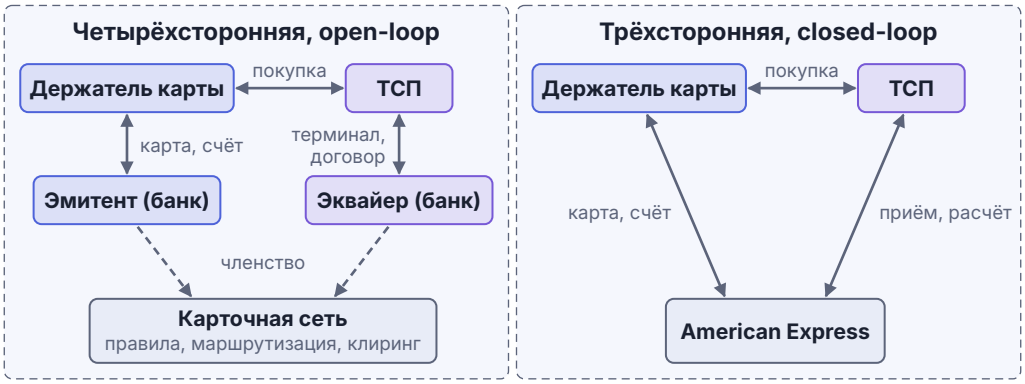


Рис. 2 — Четырёхсторонняя и трёхсторонняя модели в сравнении.

кофейни в Лиссабоне, хотя банк туриста и банк кофейни никогда не слышали друг о друге.

Для держателя карты и продавца инфраструктура почти невидима. Покупатель видит «одобрено» или «отказано», продавец получает деньги в оговорённый расчётный срок. За каждым событием стоит последовательность сообщений: от терминала через эквайера и карточную сеть к эмитенту и обратно, и каждый её участник принял решение, обновил свой реестр и взял на себя часть ответственности за результат.

2.2 Участники

Эмитент

Когда держатель карты прикладывает её к терминалу, авторизационный запрос получает эмитент и за доли секунды решает, одобрить или отклонить. Эмитент проверяет баланс или доступный кредитный лимит, статус карты, географические и временны́е ограничения, правила антифрода и, при необходимости, результат аутентификации — PIN, 3-D Secure. Ответ `00` — «операция одобрена» — означает обязательство оплатить эту транзакцию при клиринге; при любом другом коде продавец получает отказ, и покупателю придётся платить другим способом.

Экономика эмитента опирается на несколько источников дохода: процентный доход по кредитным картам, годовое обслуживание, комиссия за операции — снятие наличных, конвертация валюты — и interchange, межбанковская комиссия, которую эмитент получает с каждой покупки. Interchange мотивирует банки выпускать карты, предлагать кешбэк и мильные программы; всё это финансируется из комиссии, которую платит продавец. Механика interchange разбирается в разделе 2.3.

Эквайер

Эквайер подписывает с ТСП договор эквайринга, по которому обязуется принимать карты определённых платёжных систем, перечислять ТСП причитающиеся суммы за вычетом комиссии и обрабатывать chargeback при оспаривании транзакции покупателем. Взамен ТСП платит эквайеру торговую уступку (merchant service charge, MSC) — процент от суммы каждой транзакции, покрывающий расходы всех участников, включая interchange и комиссию сети.

Эквайер несёт риски, связанные с ТСП. Если продавец обанкротится, не доставит товар или окажется мошенником и покупатели инициируют chargeback, финансовую ответственность перед карточной сетью несёт эквайер — он принял это ТСП на обслуживание. Перед подключением эквайер проводит проверку (*underwriting*) и оценивает бизнес-модель, финансовое состояние, категорию деятельности по MCC (Merchant Category Code, код категории ТСП по ISO 18245) [16] и репутационные риски. После подключения он отслеживает уровень chargeback, подозрительные схемы операций и соответствие правилам сети.

Карточная сеть

Карточная сеть (или, в терминологии 161-ФЗ, *платёжная система*) устанавливает правила, по которым работают остальные участники, и поддерживает техническую инфраструктуру для передачи авторизационных сообщений, клиринга и расчёта [5, 13, 15].

Visa управляет сетью VisaNet, через которую проходят все авторизации и клиринговые файлы; Mastercard — сетью Banknet; НСПК (Национальная система платёжных карт) — национальной инфраструктурой, через которую маршрутизируются все внутрироссийские карточные транзакции независимо от бренда на карте [17]. Перевод внутрироссийского трафика прошёл поэтапно в 2015 году: Mastercard переключился на ОПКЦ (операционный и платёжный клиринговый центр НСПК) с 1 апреля 2015 года, Visa завершила миграцию к концу мая того же года. Правила сети (*scheme rules*) насчитывают сотни страниц и регламентируют детали — от размера логотипа на карте до порядка обработки диспутов, от требований к безопасности терминала до сроков расчёта между участниками.

Доход карточной сети складывается из комиссий за обработку транзакций, оценочных сборов (assessments), лицензионных платежей участников и дополнительных сервисов: токенизации, скоринга антифрода, аналитики. В отличие от interchange, который эквайер платит эмитенту, комиссию сети платят и эмитент, и эквайер, каждый по своей шкале.

Процессор

Техническую часть работы эмитента и эквайера — формирование авторизационных сообщений, связь с карточной сетью, обработку клиринговых файлов, управление криптографическими ключами — банк часто передаёт отдельной организации, процессору (processor).

Эмитентский процессор (issuer processor) обрабатывает транзакции от имени эмитента: получает авторизационные запросы из карточной сети, сверяет их с данными карты и счёта, применяет правила эмитента и возвращает ответ. *Процессор торгового эквайринга* (acquirer processor) работает на стороне эквайера, принимает транзакции от терминалов, формирует сообщения в формате карточной сети, передаёт их на авторизацию и обрабатывает ответы. Один банк может использовать разных процессоров на стороне эмитента и эквайера; один процессор может обслуживать десятки банков.

НСПК к процессорам не относится: это инфраструктурный оператор национальной платёжной системы «Мир» и ОПКЦ [5, 17]. Сеть НСПК маршрутизирует внутрироссийский карточный трафик и выполняет сетевую коммутацию; коммерческий процессинг остаётся у банков и их подрядчиков. До приостановки операций Visa и Mastercard в России в марте 2022 года даже покупка по карте Visa в магазине в России шла через ОПКЦ НСПК, а не напрямую через VisaNet. Независимыми процессорами на рынке работают UCS[1], БПЦ Процессинг (на платформе SmartVista) и Compass Plus (TranzWare/TranzAxis).

Платёжный шлюз

Платёжный шлюз (payment gateway) выполняет узкую техническую задачу: шифрование карточных данных, формирование сообщения для эквайера, доставку 3-D Secure, возврат ответа на сайт продавца. Эквайринговый договор с ТСП и расчёты остаются за банком-эквайером, чьё подключение шлюз обслуживает. Технические интеграторы вроде PayKeeper или Best2Pay сочетают шлюз с функциями агрегатора и работают по партнёрским программам с несколькими банками-эквайерами одновременно.

[1] АО «Компания объединённых кредитных карточек» (КОКК), действует под брендом UCS; входит в группу Интеррос (как и Т-Банк с Росбанком).

Провайдер платёжных услуг (PSP)

Провайдер платёжных услуг (payment service provider, PSP) берёт на себя техническую сторону приёма платежей за продавцов, которые не хотят напрямую подписывать договор эквайринга с банком, интегрировать терминальное оборудование и вести сверку расчётных отчётов по chargeback. Продавец получает единый интерфейс вместо прямой банковской интеграции. PSP стоит между продавцом и одним или несколькими эквайерами, принимает платёжные данные или токен, формирует запрос в нужном формате, отправляет транзакцию выбранному партнёру и возвращает продавцу единый результат.

Если провайдер ограничивается технической ролью, он остаётся платёжным шлюзом; если поверх шлюза появляются функции эквайера или агента, он сам заключает договор с ТСП и участвует в расчётах. На международном рынке по этой модели работают Adyen и Stripe; в России — ЮKassa (на стороне НКО ЮMoney, экосистема Сбера), CloudPayments (ООО «КЛАУДПЭЙМЕНТС» как банковский платёжный агент Т-Банка), Robokassa и Best2Pay.

ПРАКТИКА

Если вы разработчик и интегрируете приём платежей, чаще всего вашим контрагентом будет PSP. Вызываете его API, получаете асинхронное уведомление о результате, используете его инструменты для возвратов и подписок. Эквайер, карточная сеть и эмитент скрыты за фасадом единого интерфейса; в повседневной работе хватает абстракции PSP. Но когда что-то идёт не так (транзакция зависла, пришёл chargeback с непонятным кодом причины, деньги не зачислились в ожидаемый срок), знание участников за фасадом показывает, где искать сбой.

Платёжный фасилитатор

Платёжный фасилитатор (payment facilitator, PayFac) — посредник, который подписывает с банком-эквайером один общий договор и подключает под ним множество субмерчантов от своего имени, избавляя банк от задачи индивидуального подключения каждого ТСП.

Прямого аналога PayFac в российском праве нет; роль реализуется через статус банковского платёжного агента (БПА) или агрегатора по 161-ФЗ [1]. АО КОКК (UCS) выступает агрегатором — БПА Т-Банка, ЮKassa агрегирует приём в экосистеме Сбера, а маркетплейсы Wildberries и Ozon строят отношения с продавцами по агентской модели и замыкают приём на собственные дочерние банки (ВБ Банк, Озон Банк). Полный разбор PayFac, MoR (Merchant of Record — юридический продавец перед карточной сетью) и pass-through как разных моделей распределения ответственности и их соотношения с БПА — в разделе 3.3.

Дескриптор — строка, которую держатель карты видит в выписке или мобильном банке рядом с операцией; её формирует та сторона, чьё имя проходит в карточной сети.

Таблица 1 — Сравнение технических посредников карточной обработки.

Признак	Процессор	Шлюз	PSP	Фасилитатор
Лицензия	—	—	агрегатор	БПА
Участвует в расчётах	нет	нет	да	да
Договор с ТСП	банк	банк	PSP	фасилитатор
Риск chargeback	нет	нет	общий с банком	на нём
Дескриптор	эквайер	эквайер	ТСП	субмерчант

Строка «Лицензия» группирует посредников по категориям 161-ФЗ;[1] строка «Договор с ТСП» показывает, с кем продавец заключает договор о приёме.[2] Роль посредника (шлюз, PSP или фасилитатор) не всегда совпадает с брендом: один провайдер может поставлять шлюзовую интеграцию одним клиентам и работать агрегатором для других.

Оркестратор

Десять лет назад продавцу часто хватало одного банка-эквайера; сегодня крупный международный *e-commerce*-бизнес работает с пятью-десятью эквайерами в разных странах, несколькими альтернативными методами оплаты и множеством валют. Несколько подключений снижают стоимость приёма, повышают долю одобрений и дают резерв на случай отказа одного из них.

Оркестратор (payment orchestrator) управляет подключениями к нескольким эквайерам и PSP и направляет каждую транзакцию по выбранному правилу — по стоимости, вероятности одобрения, географии покупателя или типу карты.

От PSP оркестратор отличается тем, что не имеет статуса агрегатора или БПА и не становится расчётным участником. Он не перемещает деньги — он выбирает, через кого их перемещать. Регуляторная нагрузка на оркестратор поэтому ниже, чем на PSP; финансовые роли остаются у подключённых через него эквайеров.

В облачной модели (*hosted orchestration*) продавец подключается к облачному сервису вендора, который держит коннекторы к эквайерам и управляет правилами маршрутизации от своего имени. В локальной (*self-hosted*) продавец или процессор берёт SDK и DSL (domain-specific language, предметно-ориентированный язык) правил маршрутизации и развёртывает у себя. Облачная модель требует меньше инфраструктуры на старте; локальная даёт полный контроль над правилами и данными транзакций.

Оркестратор окупается при работе с несколькими активными эквайерами, мультирегиональных выплатах или каскадных повторах транзакции. Главный риск — привязка к вендору (*vendor lock-in*) через логику маршрутизации: правила хранятся в формате вендора, и накопленные годами наработки трудно перенести в другую систему без потери точности.

[1] Собственная кредитная лицензия даёт фасилитатору больше свободы, чем статус БПА конкретного банка-эквайера.

[2] Договор о приёме определяет, кто отвечает за тариф, сроки и возвраты, и часто отличается от того, чьим именем платёж проходит в карточной сети.

2.3 Кто кому платит: экономика interchange

Эмитенты, эквайеры, карточная сеть и процессоры несут расходы: терминалы, обработка десятков тысяч авторизаций в секунду на пике[1], системы антифрода, кешбэк на карте покупателя. Распределение этих расходов между участниками описывает экономика interchange.

MSC: торговая уступка

Покупатель платит сто рублей, продавец получает не сто: за право принимать карточные платежи продавец платит эквайеру торговую уступку (merchant service charge, MSC, иногда merchant discount rate, MDR) — процент от суммы каждой транзакции, к которому может добавляться фиксированная плата за операцию. Из ста рублей продавец получает, скажем, девяносто восемь, а два уходят на оплату работы всех участников обработки.

MSC складывается из нескольких компонентов:

- **interchange** — межбанковская комиссия, которую эквайер платит эмитенту за каждую транзакцию. Это самая крупная составляющая MSC.
- **комиссия сети** (scheme fee, assessment) — плата, которую карточная сеть взимает за обработку транзакции, маршрутизацию, клиринг и расчёт. Существенно меньше interchange.
- **маржа эквайера** (acquirer markup) — то, что остаётся эквайеру после уплаты interchange и комиссии сети. Покрывает его собственные расходы на терминалы, процессинг, поддержку, риски, и даёт прибыль.

В договоре продавец видит MSC как одну ставку, но внутри она раскладывается на несколько денежных потоков: эмитент получает часть за выпуск и обслуживание платёжного инструмента, сеть — за инфраструктуру и обработку, эквайер — за подключение ТСП, текущую работу и риск.

Покупатель оплачивает дебетовой картой Visa 50 EUR в супермаркете по чиповой транзакции с MCC 5411 в зоне действия IFR (Interchange Fee Regulation, регламент ЕС о межбанковских комиссиях, 2015 год [20]). Суммарный MSC порядка 0,74 % складывается из трёх компонентов — interchange, scheme fee, acquirer markup. Для потребительской кредитной карты действует другой потолок IFR — 0,30 %, поэтому MSC поднимается примерно до 0,84 %. Разница в 0,05 EUR на одной транзакции мала; в масштабах крупного ретейлера с миллионами операций она определяет, стоит ли подталкивать покупателей к дебетовым картам и переключать трафик между эквайерами.

Interchange: зачем эквайер платит эмитенту

Деньги внутри сети текут от эквайера к эмитенту. Эмитент финансирует выпуск карт, обслуживание счёта, антифрод, кредитный риск и программы лояльности; коммерческая выгода от карточного приёма достаётся продавцу. Эту связку и замыкает interchange — за каждую покупку эквайер перечисляет эмитенту часть MSC.

Направление потока — от эквайера к эмитенту — определяется структурой издержек двустороннего рынка. Карточная сеть работает, пока активны обе стороны рынка — покупатели носят карты, продавцы их принимают. Продавец готов платить

[1] Visa в 2025 году заявляет пропускную способность VisaNet до 83 000 TPS при более 322 млрд транзакций в год [18]; у Mastercard, по словам её вице-президента в 2023 году, около 20 000 TPS на пике и более 400 млн транзакций в пиковые сутки [19].

за карточный приём, потому что карта увеличивает средний чек и устраняет расходы на инкассацию. Эмитент оплачивает выпуск и перевыпуск пластика, процессинг авторизаций, риск невозврата по кредитным картам, обслуживание споров и — если банк хочет конкурировать за держателя карты — кешбэк и мильные программы. Без interchange единственные источники дохода эмитента по дебетовой карте — годовое обслуживание и комиссия за снятие наличных; этого не хватает, чтобы окупить инфраструктуру массовой эмиссии. Тогда банки выпускают меньше карт, покупатели реже платят картой, продавцы видят меньше карточных транзакций, сеть сужается. Interchange разрывает этот цикл, перенося часть выручки от стороны, получающей коммерческую выгоду через продавца и эквайера, к стороне с наибольшими инфраструктурными расходами — эмитенту.

Альтернатива — прямые платежи от продавца эмитенту без посредника — потребовал бы $N \times M$ двусторонних соглашений, той самой комбинаторной проблемы, которую карточная сеть решает для маршрутизации. Interchange работает по тому же принципу: сеть задаёт единую таблицу ставок, и каждый участник подчиняется ей без переговоров с каждым контрагентом.

Когда Европейский союз ограничил interchange Регламентом IFR уровнем 0,2 % для дебетовых и 0,3 % для кредитных карт, последствия проявились на обеих сторонах рынка [20]. Эмитенты урезали программы лояльности, перешли на годовые комиссии за обслуживание и сосредоточили кешбэк на премиальных продуктах, не подпадающих под регулирование, — коммерческих картах и трёхсторонних схемах. Продавцы получили снижение MSC, но не всегда пропорциональное — часть экономии осталась у эквайеров в виде возросшей маржи.

Размер interchange задаёт карточная сеть; свободные переговоры между конкретным эмитентом и эквайером тут не работают. Ставка зависит от типа карты: дебетовая дешевле кредитной; от категории ТСП по MCC: продуктовый магазин платит меньше, чем ювелирный; от способа приёма: контактная транзакция дешевле ручного ввода номера карты; от географии: внутренняя транзакция дешевле международной. Полные таблицы interchange публикуются на сайтах Visa и Mastercard — сотни строк с различными комбинациями [21, 22].

ВАЖНО

Продавец платит эквайеру MSC; interchange — часть этой суммы, которую эквайер перечисляет эмитенту. Продавец может даже не знать, какую долю его MSC составляет interchange, если договор с эквайером предусматривает единую ставку (*flat rate*) вместо модели interchange++, при которой продавец видит interchange и маржу эквайера отдельно. Когда продавец «переплачивает за эквайринг», с эквайером он может торговаться только о марже. Interchange задаёт сеть, и снизить его продавец может лишь составом своих транзакций: долей дебетовых карт и способом приёма.

Регулирование interchange

Interchange остаётся предметом постоянных споров между торговыми сетями, банками и регуляторами. Продавцы считают ставки завышенными; банки отвечают, что резкое снижение interchange подорвёт программы лояльности и сократит стимулы к эмиссии карт; регуляторы ищут баланс между этими позициями.

В Европейском союзе спор привёл к уже упомянутому Регламенту IFR (2015) с потолками interchange для потребительских карт [20]. Регламент задаёт потолок, но не определяет, как рынок перераспределит последствия между продавцом, эквайером, эмитентом и держателем карты. В 161-ФЗ такого общего потолка для interchange не установлено [1].

Модель ценообразования: что видит продавец

В договоре эквайринга interchange показывают продавцу одним из способов:

- **flat rate** — единая ставка MSC на все транзакции, например 2,0 %. Модель предсказуема, но невыгодна для продавцов с высокой долей дебетовых карт, по которым interchange ниже.
- **interchange++** — продавец видит фактический interchange по каждой транзакции, комиссию сети и наценку эквайера отдельно. Прозрачная модель, но для анализа выписок нужна квалификация.
- **tiered pricing** — эквайер группирует транзакции в категории «квалифицированные», «среднеквалифицированные» и «неквалифицированные» с разными ставками. Модель непрозрачна и постепенно уходит с рынка.

ПРАКТИКА

Если вы проектируете платёжную аналитику для ТСП или платформу управления платежами, поддержка модели interchange++ с детализацией до отдельной транзакции нужна большинству крупных продавцов.

2.4 Трёхсторонняя модель

Альтернатива четырёхсторонней схеме — трёхсторонняя модель (three-party model, closed-loop model), в которой одна организация совмещает роли эмитента, эквайера и карточной сети. Классический пример — American Express, Amex.

В чистой трёхсторонней модели Amex сам выпускает карты, сам подписывает договоры с продавцами и сам обрабатывает транзакции от начала до конца (см. рис. 2). Interchange здесь теряет смысл — нет двух банков, между которыми нужно передавать комиссию, и вся выручка от продавца (merchant discount) остаётся внутри одной организации. Amex получает полный контроль над клиентским опытом на обеих сторонах, и для держателя карты, и для продавца. Чтобы карта работала в новом магазине, Amex должен подписать договор с ним напрямую; в четырёхсторонней модели магазину нужен любой эквайер, подключённый к сети.

Ограничение масштаба объясняет, почему четырёхсторонняя модель доминирует. Visa и Mastercard принимаются практически в каждой торговой точке мира, тогда как Amex исторически сосредоточен в премиальном сегменте и покрытие у него у́же. Сам Amex давно открыл сеть для сторонних эмитентов и эквайеров: классический *closed-loop* дополнен партнёрской сетью [23].

Партнёрская сеть Amex (Global Network Services, GNS) подключает банки-партнёры одновременно в роли эмитента и эквайера на территориях, где сам Amex не выпускает карты напрямую [24]. Партнёр выпускает карты под брендом Amex, обслуживает счёт держателя, формирует MSC по тарифам сети и заключает договоры с местными продавцами; в обмен получает *issuer rate* — индивидуально согласуемую с сетью долю MSC, по структуре близкую к interchange, — и доступ к корпоративной клиентуре сети. В России по этой схеме работал Русский Стандарт (эксклюзивный эмитент Centurion с 2005 года, договор продлён в январе 2017 года на десять лет), действовавший до приостановки операций Amex в марте 2022 года [25]; Сбербанк выпускал Amex с 2010 года и прекратил эмиссию в декабре 2014 года [26], эквайринг — в августе 2016 года [27]. *Closed-loop* в чистом виде сохранился в нишах, где замкнутая работа с клиентом ценнее масштаба: корпоративные T&E-карты (Travel and Entertainment, командировочные и представительские расходы), ранние реализации Discover и JCB. Discover с середины 2000-х

повторил траекторию Amex и открыл сеть для сторонних эмитентов после покупки дебетовой PIN-сети Pulse (сделка закрыта 12 января 2005 года) [28]. JCB внутри Японии параллельно ведёт прямую эмиссию (direct), франчайзинговую сеть из более чем восьмидесяти финансовых учреждений (franchisee) и брендовую лицензию для торговых и потребительских кредитных компаний (licensee); за пределами Японии — лицензионные соглашения с локальными эмитентами и эквайерами [29].

Кредитные риски эмитента, операционные риски эквайера и их источники дохода — предмет следующей главы.

3 Эмитент и эквайер

Касание карты у терминала или нажатие «Оплатить» в браузере запускает два встречных процесса. Эмитент за секунды решает, готов ли взять на себя кредитный риск: действительна ли карта, хватает ли средств, не похожа ли операция на фрод. Эквайер принимает запрос, проводит его по нужному маршруту и рассчитывается с продавцом.

3.1 Эмитент

Эмитент (issuer) выпускает карту и принимает на себя кредитный риск транзакции. В момент покупки он должен решить, готов ли рассчитаться по операции через карточную сеть, а затем взыскать средства с держателя карты — списать с дебетового счёта или увеличить задолженность по кредитному. Поэтому у эмитента работа распределена между специализированными системами: одна ведёт жизненный цикл карты, другая принимает авторизационное решение, третья отвечает за аутентификацию в интернет-платежах.

В клиринг и расчёт эмитент входит только как получатель: пакет финансовых требований формирует и отправляет в сеть эквайер, а эмитент по этому файлу списывает с держателя. Банк, который занимается только эмиссией, клиринг не инициирует — в сеть он отправляет лишь ответы на чужие запросы (авторизационные, клиринговые, по диспутам).

Система управления картой (CMS)

Система управления картой (Card Management System, CMS) ведёт жизненный цикл карты: выпуск, смена статуса, блокировка, перевыпуск. CMS хранит реквизиты и связь со счётом, поддерживает статусы и лимиты, формирует задания на персонализацию и фиксирует события, которые позже потребуются поддержке, антифроду и разбору диспутов.

На этапе персонализации на карту загружаются апплет EMV (Europay/Mastercard/Visa, спецификация чиповых карт), ключи карты (UDK, Unique Derivation Key), производные от мастер-ключа эмитента IMK (Issuer Master Key), который остаётся в HSM (Hardware Security Module, аппаратный криптомодуль) эмитента, параметры управления риском эмитента (IAC, Issuer Action Codes, и прикладные офлайн-лимиты — последовательных операций и кумулятивной суммы), а также данные платёжного приложения AID (Application Identifier, идентификатор приложения) и Application Label; подробнее в гл. 7 [30—33]. Для карт Мир персонализация дополнительно включает установку приложения Мир (MPA, MIR Payment Application) с поддержкой криптографии ГОСТ; конкретный криптографический профиль зависит от программы эмиссии и продолжающегося перехода НСПК на отечественные алгоритмы; см. раздел 16.7.

Авторизационный хост

Авторизационный хост решает, можно ли по карте провести конкретную операцию. Когда запрос доходит от карточной сети до эмитента, хост последовательно

проверяет статус карты и срок её действия, доступность средств или свободного кредитного лимита, лимиты и признаки нетипичного поведения, см. гл. 29. Для транзакций EMV он также верифицирует криптограмму ARQC (Authorization Request Cryptogram, запросная криптограмма) через HSM [30, 31].

Если все проверки пройдены, хост формирует ответ `00` Approved и генерирует ARPC (Authorization Response Cryptogram), который возвращается карте для взаимной аутентификации. Если хотя бы одна проверка не проходит, хост возвращает соответствующий код ответа (*response code*), например `51` Insufficient Funds, `05` Do Not Honor или `14` Invalid Card Number, и отклоняет транзакцию [31, 34].

Отдельный сценарий — CMS недоступна, авторизационный хост работает. Без CMS хост не видит ни актуального статуса карты (заблокирована ли она, перевыпущена ли), ни текущего лимита, и у него остаётся выбор. Первый вариант — отклонить все транзакции; безопасно, но парализует приём по всему портфелю. Второй — работать по кэшу; хост хранит копию критических полей (статус, лимит, порог офлайн-авторизации) со сроком жизни записи кэша 5–15 мин и продолжает авторизовать в пределах кэшированных лимитов. Транзакции сверх кэшированного лимита хост отклоняет; по остальным эмитент принимает риск одобрения по устаревшим данным. После восстановления CMS хост синхронизирует остатки и фиксирует расхождения.

Сценарии эмитента (*issuer scripting*)

Вместе с ответом эмитент может прислать команду для карты — обновить офлайн-PIN, сбросить счётчики, заблокировать приложение, изменить лимиты. Механизм *issuer scripting* и правила EMV для него разобраны в разделе 7.8.

ACS — сервер аутентификации

В интернет-платежах к проверке карты, лимита и криптограммы добавляется вопрос, действительно ли покупку инициировал держатель. У эмитента эту задачу решает ACS (Access Control Server) — компонент 3-D Secure (протокол подтверждения держателя в CNP-операциях), выбирающий между сценарием *frictionless* (без действий держателя) и *challenge* (дополнительное подтверждение) по логике RBA (Risk-Based Authentication, аутентификация на основе оценки риска); см. гл. 11.

Управление токенами

После выпуска карты её реквизиты хранятся на пластике, в телефоне, в браузере и у продавца в виде сетевых токенов DPAN (Device PAN, токенизированный номер карты для устройства); см. раздел 9.3. Эмитент участвует в этом жизненном цикле с самого начала: получает от провайдера токенизации TSP (Token Service Provider, провайдер услуг токенизации) запрос на токенизацию, принимает решение об одобрении после процедуры ID&V (Identification & Verification, идентификация и верификация) держателя, а затем управляет состоянием токена — активирует, приостанавливает или удаляет [35—37].

Токен остаётся связанным с исходной картой. Если держатель блокирует карту, эмитент обязан приостановить и связанные с ней токены. Если карта перевыпущена, нужно обновить привязку токенов к новому PAN (Primary Account Number, основной номер счёта; см. гл. 9), иначе держатель увидит в приложении банка новую карту, а у кошелька или продавца останется старая привязка [35, 36].

Работа с диспутами

С претензией держатель карты обращается к эмитенту — своему банку, минуя карточную сеть и эквайера: «я не совершал эту покупку» или «товар не получен». Эмитент проверяет обоснованность жалобы и при наличии оснований инициирует chargeback (принудительный возврат средств держателю по правилам карточной сети с переносом ответственности на эквайера и ТСП) через карточную сеть, направляя его эквайеру; жизненный цикл диспута разобран в разделе 32.1 [13, 38, 39].

Приняв обращение и отнеся его к подходящему классу, эмитент сопоставляет ситуацию с правилами сети: есть ли подходящий код причины, не пропущены ли сроки, достаточно ли документов и соблюдены ли обязательные условия для chargeback. После этого эмитент формирует сообщение chargeback, а если эквайер присылает повторное представление с *compelling evidence* (компенсирующие свидетельства — набор документов, подтверждающих легитимность операции), эмитент решает, принять объяснение или идти дальше, к *pre-arbitration* (досудебная стадия спора между эмитентом и эквайером перед арбитражем сети) [13, 38, 39].

3.2 Эквайер

Эквайер (acquirer) подключает терминал или платёжный шлюз, доставляет авторизационный запрос в карточную сеть, формирует и отправляет клиринговый файл, принимает расчёт от эмитентов и перечисляет деньги продавцу за вычетом комиссий. Если эмитент несёт кредитный риск держателя, то эквайер — риск ТСП: расчётный, репутационный, правовой.

ПРАКТИКА

Расчётный риск — риск того, что расчёт в системе перевода средств не состоится в ожидаемое время; включает кредитную и ликвидную компоненты [40].

Правовой риск — риск убытков из-за нарушения договоров банком, его клиентами и контрагентами, допущенных правовых ошибок, несовершенства правовой системы или различия юрисдикций у филиалов и контрагентов (п. 2.1 Письма Банка России от 30.06.2005 № 92-Т «Об организации управления правовым риском и риском потери деловой репутации» [41]).

Репутационный риск (риск потери деловой репутации) — риск убытков от ухудшения восприятия банка клиентами, контрагентами, регулятором и участниками рынка (Письмо 92-Т) [41].

Система управления терминалами (TMS)

В офлайн-эквайринге первое физическое звено — терминал. У крупного эквайера TMS управляет десятками и сотнями тысяч устройств. Главная задача — держать на каждом устройстве актуальную конфигурацию: обновлённые таблицы BIN (Bank Identification Number, банковский идентификационный номер; см. гл. 4), свежие ключи, корректные параметры EMV.

Криптографические ключи терминала — ими он шифрует вводимый держателем PIN и подписывает сообщения, отправляемые эквайеру; устройство и иерархия этих ключей разобраны в разделе 10.4. Исторически загрузка ключей на терминал шла очной процедурой с двумя участниками в защищённой зоне эквайера; на парке в тысячи устройств она уже не справлялась. Удалённая инъекция ключей (Remote Key Injection, RKI) устраняет это ограничение: терминалы разворачиваются и обновляются без физического доступа [42]. Церемония при этом сдвигается

на уровень корневых ключей RKI и мастер-ключей HSM (см. раздел 10.8); из них через защищённый канал производятся ключи отдельных терминалов.

Конфигурация ТСП и параметры маршрутизации

Интернет-эквайринг и омниканальные сценарии требуют надстройки над терминалами. В ней хранятся профили ТСП, конфигурация MID/TID (Merchant ID / Terminal ID, идентификаторы ТСП и терминала в учётных системах эквайера и карточной сети), правила дескрипторов, маршрутизация по процессорам, параметры 3-D Secure, лимиты на возвраты и выплаты, а также связка с платёжным шлюзом из гл. 34.

Эта надстройка определяет, какой MCC и какой дескриптор увидит эмитент, через какой BIN эквайера пойдёт транзакция и в какую программу мониторинга попадёт ТСП. Если такие решения разбросаны по разрозненным таблицам, тикетам и ручным настройкам в кабинете процессора, эквайер теряет управляемость: одна и та же конфигурация ТСП по-разному выглядит для сети, риск-менеджмента и финансовой сверки [43].

У крупных эквайеров в этой надстройке сходятся подключение ТСП, маршрутизация между несколькими процессорами и правила работы с ТСП: кому дать прямой маршрут на конкретного процессора, кому оставить один канал, а кому включить усиленный фиксированный резерв (*holdback*) или ручную проверку выплат.

Подключение ТСП

Прежде чем дать ТСП доступ к карточной сети, эквайер должен установить, кто перед ним, какой бизнес он ведёт и какой риск несёт. Подключение ТСП — набор проверок и настроек, которые задают допуск и экономику отношений.

При идентификации ТСП (KYB, Know Your Business) проверяют юридическое лицо, бенефициаров и санкционные списки. При классификации MCC ТСП присваивают код категории, от которого зависят ставки interchange, правила 3DS и допустимость операции. При андеррайтинге (*underwriting*) оценивают финансовый риск и задают ставку комиссии, размер фиксированного резерва (*holdback*) и плавающего резерва (*rolling reserve*). Разбор каждого шага — в разделе 26.3.

Мониторинг ТСП

Эквайер непрерывно наблюдает за долей chargeback, долей фрода, долей возвратов и аномалиями частоты (*velocity* — всплески числа операций по карте или ТСП относительно ожидаемого профиля). Превышение порогов карточных сетей ведёт к штрафам и усиленному контролю; пропущенный *bust-out* (схема, при которой ТСП за короткий срок собирает большой объём авторизаций и выводит средства до истечения срока, в течение которого допустим chargeback) обходится эквайеру в миллионы. Ответственность за ТСП несёт эквайер: если ТСП оказался мошенником или нарушил правила карточной сети, штрафы и финансовые потери остаются у эквайера. Метрики мониторинга и обмен с ФинЦЕРТ (Центр взаимодействия и реагирования Департамента информационной безопасности Банка России) [44] разобраны в разделе 26.4, мониторинговые программы сетей — VAMP (Visa Acquirer Monitoring Program) и MC ECP (Mastercard Excessive Chargeback Program) — в разделе 32.6 [45, 46].

Ответственность за расчёт

Для продавца эквайринг заканчивается в момент поступления денег. Эквайер собирает клиринг, удерживает комиссии, применяет плавающий резерв (*rolling reserve*) и перечисляет средства продавцу.

Эквайер обязан показать состав каждой выплаты: какая сумма удержана как комиссия, какая отправлена в резерв, какая зачтена против возвратов и в какой валюте считается обязательство. Кроме того, на нём остаётся риск *late presentment* (просрочки представления операции в клиринг сверх установленного сетью срока; подробнее см. раздел 5.2), временных разрывов по chargeback и кассовых разрывов между получением денег от сети и выплатой продавцу. Эквайер же задаёт политику выплат в нотации T+N: T — день совершения операции (*trade date*), N — сдвиг в рабочих банковских днях до зачисления на счёт ТСП. T+0 — в тот же день, T+1 — на следующий рабочий день, T+2 — через два; еженедельные выплаты и отложенный расчёт для высокорисковых MCC — варианты той же шкалы. Сутки от T отсекаются по *cut-off* эквайера: операция после отсечки относится к следующему T.

На счёт ТСП приходит нетто после удержаний на стадиях жизненного цикла операции (авторизация, клиринг, межбанковский расчёт — разбор в гл. 5): торговая уступка (*merchant discount rate*, MDR, синоним *merchant service charge*, MSC; разложение в разделе 2.3), отчисления в плавающий и фиксированный резервы (разбор — в следующем абзаце), зачёты против возвратов и chargeback. Расчёт между сетью и банком-эквайером (см. раздел 5.3) идёт по своему графику. Когда эквайер выплачивает ТСП быстрее, чем сеть рассчитывается с ним (мгновенные выплаты, T+0 на рынках, где сетевой расчёт T+1), разницу эквайер покрывает собственными средствами — короткий кредит ТСП на несколько дней. Стоимость такого кредитования заложена в наценку эквайера в составе MSC и повышает тариф для быстрых выплат.

Фиксированный и плавающий резервы нужны из-за промежутка между авторизацией и истечением срока, в течение которого держатель ещё вправе оспорить операцию; от авторизации до этого момента может пройти несколько месяцев. Если продавец за это время прекратил деятельность или не может покрыть возвраты, потери несёт эквайер. Резерв — буфер для таких потерь. Его размер отражает оценку риска ТСП: для продавца с высокой долей chargeback, сезонным бизнесом или без истории эквайер устанавливает более высокий процент удержания.[1]

Завершение работы с ТСП

После расторжения договора риск эквайера сохраняется на те же месяцы, ради которых создан резерв. ТСП расторгает договор сам или эквайер отключает его из-за превышения порогов мониторинга, нарушения правил сети или подозрения на *bust-out*; в обоих случаях операции последних месяцев ещё можно оспаривать, и за них отвечает эквайер.

Резерв поэтому возвращают не в день расторжения, а по мере того, как истекает срок оспаривания накопленных операций; высвобождение растягивается до полугода после последней транзакции (привязка резерва к сроку оспаривания разобрана в гл. 32). Перед возвратом эквайер зачитывает против резерва незакрытые chargeback, штрафы сети и неоплаченные комиссии — продавец получает остаток.

[1] Эти резервы эквайера — *holdback* и *rolling reserve* — удерживаются на стороне эквайера. Не путать с резервами в продуктовом реестре платформы (*refund reserve*, *minimum balance*, *holdback* — см. раздел 35.6): там та же терминология описывает удержание у продавца на стороне маркетплейса/PSP, отдельным механизмом и по собственным правилам.

Ответственность сохраняется и в процедурах сети: представление возражений (*representment*) и арбитраж по операциям, совершённым до расторжения, проходят по срокам сети уже после отключения ТСП. Эквайер откладывает финальный расчёт с продавцом до закрытия этих диспутов. Само отключение затрагивает и учётные системы эквайера: MID и TID закрывают в CMS, терминалы выводят из эксплуатации в TMS, маршруты и дескрипторы исключают из конфигурации.

Если договор расторгнут из-за риска, эквайер вносит продавца в реестр расторгнутых ТСП своей сети — исторически такой реестр называли Terminated Merchant File (TMF). У Mastercard это теперь MATCH (Mastercard Alert to Control High-risk Merchants): запись содержит код причины — компрометация данных, отмывание, избыточные chargeback, избыточный фрод, осуждение за фрод — и хранится пять лет [47]. Правила Visa предписывают эквайеру участие в Visa Merchant Screening Service (VMSS) [48]. Реестры сетей раздельны: MATCH стал отраслевым стандартом де-факто, и эквайеры сверяются с ним и по картам Visa, хотя обязывает к нему только Mastercard. Следующий эквайер видит запись при андеррайтинге (см. раздел 26.3) и учитывает расторжение у предыдущего эквайера как риск.

В России отдельного публичного реестра расторгнутых ТСП у платёжной системы «Мир» нет: программа безопасности НСПК требует от эквайера подтверждать соответствие ТСП требованиям защиты данных и предусматривает штрафы за нарушения, но общего списка недобросовестных продавцов НСПК не ведёт [49]. Допуск и отключение ТСП опираются здесь на договор эквайера с ТСП и на инструменты Банка России — платформу «Знай своего клиента» (ЗСК), которая присваивает юрлицам и ИП уровень риска по 115-ФЗ (см. раздел 26.5).

3.3 Платёжный фасилитатор (PayFac) и модель субмерчантов

Классическая модель эквайринга работает, пока ТСП немного и каждое подключено как отдельный клиент банка. Для маркетплейса или SaaS-платформы с тысячами контрагентов банковское подключение становится узким местом: оформление каждого продавца занимает дни или недели, а бизнес-модель предполагает подключение за минуты.

В модели PayFac платформа регистрируется спонсирующим эквайером в карточной сети как PayFac и получает право подключать спонсируемых субмерчантов (*sponsored merchants*) по ускоренной схеме. У субмерчанта может быть собственный идентификатор, но договор и расчёты идут через PayFac и его эквайера. Эквайер перечисляет средства PayFac, а тот уже рассчитывается с субмерчантами. Нового продавца подключают за минуты вместо недель: PayFac автоматизирует идентификацию субмерчанта, присваивает MCC и начинает приём платежей, не дожидаясь полного банковского цикла [50, 51].

Ответственность за субмерчантов несёт PayFac. Перед карточной сетью и эквайером он отвечает за их действия как за свои: фрод субмерчанта, рост chargeback, нарушение правил сети — всё это штрафы и потери PayFac. Поэтому он строит собственные процессы идентификации, мониторинга ТСП и работы с диспутами, по строгости мало отличающиеся от банковских [50, 51].

Карточная сеть видит PayFac как единый субъект; внутренний портфель субмерчантов от неё скрыт. Нарушение правил субмерчантом сеть замечает только через отклонения в агрегированных показателях PayFac.

ВАЖНО

PayFac и ISO (Independent Sales Organization) — разные роли. ISO привлекает и обслуживает ТСП для банка-эквайера, получая агентское вознаграждение без прямого участия в расчёте. PayFac находится в денежном потоке: эквайер перечисляет средства ему, а он затем рассчитывается с субмерчантами [42, 50].

Когда выбирать PayFac

Платформа, выводящая на приём множество мелких продавцов, выбирает одну из трёх моделей. **PayFac** (Payment Facilitator) — платформа регистрируется в сети через спонсирующего эквайера, ведёт идентификацию субмерчантов, несёт ответственность за их chargeback и контролирует выплаты; оправдан при сотнях субмерчантов и потребности в быстром подключении. **MoR** (Merchant of Record) — платформа выступает единственным ТСП в глазах сети, а субмерчанты остаются её внутренней абстракцией; проще регуляторно, но налоговые обязательства, chargeback и возвраты замыкаются на платформу; подходит для SaaS с единым продуктом. **pass-through**, прямой эквайринг, — каждое ТСП заключает договор с эквайером напрямую, а платформа только маршрутизирует трафик; ответственность платформы минимальна, выплатами она не управляет, подключение каждого ТСП занимает недели [50].

Быстрое подключение в модели PayFac возлагает на платформу обязанности перед сетью и эквайером:

- ответственность за фрод и chargeback субмерчантов перед карточной сетью и спонсирующим эквайером;
- регистрация через эквайера как Third-Party Agent в Visa (Program Request Management) и аналогичные процедуры Mastercard [51];
- для платежей в CEMEA — сертификация Visa Ready Acceptance и подписание Payment Facilitator Agreement с Visa [51];
- собственный процесс идентификации субмерчантов и ПОД/ФТ (противодействие отмыванию доходов и финансированию терроризма) — эквайер требует от PayFac выполнять KYB и санкционную проверку по Visa Acceptance Risk Standards (VARS).

ПРАКТИКА

Если вы строите платформу и выбираете между PayFac и прямым эквайрингом для каждого ТСП, оцените, сколько ТСП планируете подключить в первый год. На десятках прямой эквайринг обычно проще и дешевле. На сотнях и тысячах PayFac часто окупает себя скоростью подключения, но требует серьёзных инвестиций в управление рисками, соблюдение требований и повседневное обслуживание.

Параллель в России — банковский платёжный агент

Модель PayFac родилась внутри правил карточных сетей и применяется там же. Российское право опирается на другую конструкцию — институт банковского платёжного агента (БПА) и банковского платёжного субагента, закреплённый статьями 14 и 14.2 161-ФЗ [1]; для БПА, осуществляющих операции платёжного агрегатора, дополнительно применяется Указание Банка России от 06.04.2020 № 5429-У «О ведении перечня БПА-агрегаторов» [52]. Кредитная организация вправе привлекать БПА для приёма наличных, переводов, идентификации и иных операций в случаях и в пределах, установленных законом.

Для платформы, подключающей субмерчантов и работающей с местным эквайрингом, БПА — отдельная правовая конструкция со своими обязанностями; прямой заменой PayFac из правил Visa/Mastercard она не служит. Для БПА-операторов платёжного агрегатора предусмотрено включение в перечень, который ведёт Банк России; общего публичного реестра всех БПА не существует. К обязанностям БПА относятся выполнение требований 115-ФЗ по идентификации и контролю операций (см. гл. 26 и 27), ведение специального банковского счёта, на который зачисляются принимаемые средства и с которого они перечисляются, и соблюдение ограничений по перечню операций, которые БПА имеет право выполнять от имени банка. Банковский платёжный субагент находится на следующем уровне договорных отношений и привлекается уже самим БПА с дополнительными ограничениями.

Вместо *Stripe Connect* и *Adyen for Platforms* платформа на местном рынке выбирает между вариантами: договор БПА с одним или несколькими банками; интеграция через PSP, который сам уже имеет статус БПА и предлагает решение для маркетплейсов как собственный продукт; роль спонсируемого PayFac у эквайера — участника платёжной системы «Мир». Архитектуру выплат и сверки проектируют под выбранную модель; ссылка на универсальные правила PayFac без оговорки о БПА неточна.

Прямой договор БПА с банком даёт контроль над приёмом и клиентским путём, но обязывает платформу самостоятельно вести специальный банковский счёт, поддерживать включение в перечень БПА-агрегаторов Банка России и выполнять требования 115-ФЗ по идентификации субмерчантов (юридических лиц и ИП). Идентификация клиентов-физлиц к функциям БПА не относится: Федеральный закон от 20.02.2026 № 44-ФЗ «Об ограничении идентификации физических лиц банковскими платёжными агентами» [53] изъял у банковских платёжных агентов право проводить идентификацию (в том числе упрощённую) и обновление сведений о физических лицах[1]. Интеграция через PSP-БПА (PSP в статусе банковского платёжного агента) освобождает платформу от прямых обязательств перед регулятором: специальный счёт, перечень и процедуры идентификации остаются на PSP. Цена этого варианта — маржа и меньшая гибкость: параметры приёма, тарифы и сценарии возврата определены продуктом PSP, и собственный сценарий маркетплейса чаще приходится укладывать в его API. Спонсируемый PayFac у эквайера «Мира» ближе всего к привычной международной модели и даёт быструю регистрацию субмерчантов внутри карточной сети, но работает только для карточных операций; приём через СБП и переводы по номеру счёта остаются за пределами этого договора и подключаются отдельно. Сверка и казначейство платформы поэтому делятся на карточный и некарточный потоки с самого старта проекта.

[1] Вступил в силу 03.03.2026; существующие договоры подлежат приведению в соответствие в течение 180 дней.

4 Что записано на карте

Платёжная карта содержит данные с разными функциями. PAN (Primary Account Number, основной номер карты) направляет транзакцию к нужному счёту, CVV (Card Verification Value, код верификации карты) и динамическая криптограмма EMV (см. гл. 7) подтверждают подлинность карты, часть данных нужна только в момент авторизации и после неё подлежит уничтожению. Путаница между этими группами ведёт к нарушению PCI DSS (Payment Card Industry Data Security Standard, стандарт безопасности данных индустрии платёжных карт) и эксплуатируемым уязвимостям.

4.1 Структура PAN

Цифры, выбитые или напечатанные на лицевой стороне карты, образуют PAN, главный идентификатор карты во всей платёжной инфраструктуре. PAN встречается повсюду: в авторизационном сообщении (DE 2 — Data Element 2, элемент данных 2, по ISO 8583; см. гл. 6), в клиринговом файле, в маскированном виде на чеке, на экране мобильного банка, в базе данных эмитента. Структура PAN определяет маршрут транзакции и то, какого эмитента увидит карточная сеть.

Длина PAN переменная. Современные спецификации платёжных сетей требуют поддерживать значения вплоть до 19 цифр [54, 55]. У подавляющего большинства карт Visa, Mastercard и Мир шестнадцать цифр; у American Express пятнадцать; ряд старых карт Visa — тринадцать. Поле ввода, жёстко фиксирующее длину в шестнадцать цифр, отвергает действительные карты Amex и часть Visa.

Первые шесть или восемь цифр PAN — IIN (Issuer Identification Number), идентификатор эмитента и карточной сети. Дальше идёт номер счёта, уникальный для держателя у конкретного эмитента. Последняя цифра контрольная: она вычисляется по алгоритму Луна и ловит случайную ошибку при вводе или передаче номера.

IIN и маршрутизация

По первым цифрам PAN платёжная инфраструктура определяет эмитента и карточную сеть и маршрутизирует транзакцию по её правилам. Исторически этот префикс назывался BIN (Bank Identification Number). Стандарт ISO 7812 закрепил более точное название IIN, потому что карты выпускают и банки, и небанковские эмитенты [54, 56]. В разговорной речи и в документации процессингов по-прежнему используется «BIN»; оба термина здесь синонимы.

Самая первая цифра PAN называется MII (Major Industry Identifier) и указывает на крупную отраслевую группу [57]; остальные цифры префикса уточняют эмитента и сеть по диапазонам из регистра ANSI/ISO и правил карточной сети [56, 58]. Эта цифра кодирует отрасль, под которую блок номеров выделили десятилетия назад; принадлежность к конкретной сети и эмитенту несёт весь IIN. Разработчик работает с актуальными таблицами BIN/IIN конкретных сетей и эмитентов; выводить принадлежность из MII в рабочей системе нельзя.

Долгое время IIN состоял из шести цифр, и миллион комбинаций удовлетворял потребности эмитентов. Рост числа компаний финтеха, выпускающих карты, и развитие токенизации, где каждому токену нужен свой диапазон, исчерпали свободные диапазоны BIN. Ревизия ISO 7812 2017 года запустила переход на восьмизначный

IIN, и сегодня отрасль использует этот формат [54, 57]. Шестизначные BIN из обращения не выведены: процессинги и интеграции обязаны поддерживать оба формата одновременно ещё много лет.

Процессинг, который продолжает обрезать IIN до шести цифр, рискует неверно определить эмитента. Два разных эмитента или даже две разные сети могут совпасть по первым шести цифрам, но различаться на седьмой и восьмой. Неверно определённый эмитент даёт неверный маршрут или отказ без объяснения причины. Поддержка восьмизначных IIN устраняет дефект маршрутизации; системы определения сети и маршрутизации должны учитывать её с самого начала.

Между IIN и последней цифрой PAN расположены цифры, идентифицирующие конкретный счёт держателя у конкретного эмитента. Эмитент назначает их по внутренним правилам: последовательно, случайно или с учётом продуктовой линейки. Стандарт способ назначения не регламентирует, поэтому средняя часть PAN внешнему наблюдателю непрозрачна.

Разновидности PAN

Когда на маршруте появляются сетевые токены и локальные суррогаты, у PAN возникают однокоренные термины с разной семантикой, и разные источники называют один и тот же объект по-разному.

FPAN (Funding PAN) — реальный номер карты, выпущенный эмитентом и используемый как источник для токена; в правилах ПС Мир тот же объект называется «Номер Карты (FPAN)». **DPAN** (Device PAN) — сетевой токен EMVCo для одного устройства; в правилах НСПК термин пишется как «Токен (DPAN)» и остаётся вторым именем «Токена», а не его подтипом для устройства. **MPAN** (Merchant PAN) — сетевой токен для одного ТСП; канон карточных сетей — MDES for Merchants (M4M) у Mastercard и функциональность для ТСП в Visa Token Service плюс Token Management Service от Visa Acceptance Solutions у Visa. Российскому банку с марта 2022 эти сервисы недоступны, а у НСПК аналога нет: Mir Pay SDK app2app реализует сценарий привязки к устройству (*provisioning* и *In-Application e-commerce* поверх DPAN), а токена для одного ТСП под именем MPAN в правилах ПС Мир не определено. **Pseudo PAN** — неформальный термин индустрии для суррогатов *vault* или результатов *format-preserving encryption* (FPE); в официальных документах PCI SSC используется «surrogate value», в стандартах сетей и у НСПК термин «pseudo PAN» не встречается.

Один и тот же знак «DPAN», «MPAN», «pseudo PAN» у EMVCo, PCI SSC и у российских правил расшифровывается по-разному: смысл термина задаёт источник, универсального определения нет. Разбор противоречий, матрица «термин × источник» и канон употребления в этой книге — в разделах 9.2 и 9.4 гл. 9.

Алгоритм Луна

Последняя цифра PAN контрольная и вычисляется по алгоритму Луна, который предложил Ханс Петер Лун (Hans Peter Luhn), инженер International Business Machines [59]. Алгоритм не требует секретной информации: любой, кто знает номер карты, проверит контрольную цифру самостоятельно. Поэтому проверка Луна находит случайные опечатки; злонамеренный подбор номера закрывают другие механизмы.

Алгоритм Луна проверяет PAN так:

1. Начиная со второй цифры справа и двигаясь влево, удвой каждую вторую цифру. Если результат удвоения больше 9, вычти 9 — это эквивалентно сложению цифр результата, $14 \to 1 + 4 = 5$.
2. Сложи все цифры, как удвоенные, так и неудвоенные.
3. Если сумма кратна десяти, номер проходит проверку Луна.
4. Если нет, номер содержит ошибку.

Пример — номер `4561 2612 3456 0892`: на рис. 3 все четыре шага разложены поразрядно. Сумма результатов — 67, не кратна десяти, поэтому этот номер не прошёл бы проверку: он вымышлен для примера. В реальном PAN эмитент подбирает контрольную цифру так, чтобы итоговая сумма оказалась кратна десяти.

Позиция	16	15	14	13	12	11	10	9
Цифра	4	5	6	1	2	6	1	2
Удвоение	8		12-9=3		4		2	
Результат	8	5	3	1	4	6	2	2

Позиция	8	7	6	5	4	3	2	1
Цифра	3	4	5	6	0	8	9	2
Удвоение	6		10-9=1		0		18-9=9	
Результат	6	4	1	6	0	8	9	2

Сумма	8+5+3+1+4+6+2+2+6+4+1+6+0+8+9+2 = 67, не кратна 10

Рис. 3 — Проверка Луна для PAN `4561 2612 3456 0892`.

Платёжной форме достаточно проверить введённый номер; вычислять правильную контрольную цифру не требуется. Компактная проверка на Python:

```
def luhn_valid(pan: str) → bool:
  total = 0
  double = False
  for ch in reversed(pan):
    digit = int(ch)
    if double:
      digit *= 2
      if digit > 9:
        digit -= 9
    total += digit
    double = not double
  return total % 10 == 0
```

Алгоритм Луна отсеивает опечатки и часть типичных перестановок соседних цифр, но криптографической защиты не даёт: он не защищает от злонамеренного подбора номера, не подтверждает существование карты и не заменяет аутентификацию.

PAN работает как адрес: по нему система находит эмитента и счёт. Подлинность карты и право держателя инициировать операцию PAN не доказывает. Для этого нужны другие данные; исторически первыми появились данные магнитной полосы. CVV, CVV2, iCVV, dCVV закрывают каждый свой канал атаки на карту и разбираются в разделе 4.3.

4.2 Магнитная полоса

На обратной стороне карты находится тёмная магнитная полоса (*magnetic stripe*, *magstripe*), стандартизованная в 1970-х годах; её минимальная ширина по ГОСТ Р ИСО/МЭК 7811-6 — 11,89 мм для дорожек 1 и 2 и 15,95 мм при использовании трёх дорожек [60]. Полоса сохранилась на большинстве карт мира, но чип и бесконтактное ядро вытеснили магнитное чтение из приёма. Требования к самой записи задаёт ISO/IEC 7811–2, а структуру финансовых карт и данных на дорожках описывает ISO/IEC 7813 [61, 62].

Магнитная полоса содержит три дорожки (*tracks*) с разным форматом и плотностью записи. В массовых карточных платежах работают первая и вторая, третья осталась факультативной.

Track 1 (IATA)

Первая дорожка, стандартизованная IATA, единственная из трёх, в которой допустимы буквенно-цифровые данные. Для финансовых карт ISO/IEC 7813 задаёт структуру и состав полей Track 1 и Track 2, по которым инициируется транзакция [55, 62]. Структура записи на Track 1:

```
%B4561261234560892^IVANOV/IVAN^2612...
```

Здесь `%` — маркер начала, `B` — код формата; для финансовых карт он всегда B. Далее идёт PAN, разделитель `^`, имя держателя в порядке фамилия-имя, ещё один разделитель, срок действия в формате две цифры года и две цифры месяца, сервисный код, данные для верификации CVV и дискреционные данные эмитента (поле, в которое эмитент при персонализации записывает собственные служебные значения); `?` — маркер конца. Track 1 — единственная дорожка с именем держателя, которое прямо указывает на человека; PAN на любой дорожке тоже относится к персональным данным, если по нему определяется держатель [63].

Track 2 (ABA)

Вторая дорожка, разработанная Американской банковской ассоциацией (ABA), хранит только цифровые данные: до 40 символов, из которых используются цифры 0–9 и несколько служебных символов. Track 2 остаётся основной рабочей дорожкой для карточных платежей. Когда карта проходит через считыватель или терминал читает магнитную полосу, в авторизационном сообщении в DE 35 отправляются данные второй дорожки [55].

Структура Track 2 компактнее:

```
;4561261234560892=2612...
```

Маркер начала `;`, далее PAN, разделитель `=`, срок действия в формате две цифры года и две цифры месяца, затем сервисный код из трёх цифр, определяющих условия использования карты (требуется ли PIN, разрешены ли международные транзакции и так далее), CVV, дискреционные данные эмитента и маркер конца `?`. Имя держателя на Track 2 *отсутствует*: только цифровой идентификатор.

Каждое поле Track 2 выросло из задач банковских операций 1960-х–70-х годов. PAN заменил ручную запись номера на слип, и терминал читал цифры с полосы без кассира. Срок действия ограничил «вечно действующие» карты и упростил перевыпуск: эмитент автоматически закрывал операции по истёкшим картам. Сервисный

код закодировал политику эмитента для терминала: три цифры задают «карта только для PIN», «международный приём запрещён» или «только онлайн». CVV добавил машинный признак верификации поверх тиснёных цифр; данные на полосе можно сверить с вычислением эмитента и поймать клон с пустой полосой.

ПРАКТИКА

В шестнадцатеричном дампе авторизационного сообщения поле DE 35 (Track 2 Data) совпадает с содержимым второй дорожки, прочитанным с магнитной полосы, либо с эквивалентными данными, сгенерированными чипом. В одной строке оказываются PAN, срок действия и CVV. Полные данные Track 2 PCI DSS относит к чувствительным аутентификационным данным (*sensitive authentication data*, SAD): их *запрещено* хранить после авторизации, даже в зашифрованном виде [64].

Track 3: редкое наследие

Третью дорожку разработала ассоциация Thrift Industry под приложения с перезаписью данных прямо на карте — баланс хранился на полосе, без обращения к эмитенту за каждой операцией. В эпоху дорогих телекоммуникаций идея казалась разумной. Карточные сети предпочли онлайн-авторизацию через центральную инфраструктуру: запись баланса на карту открывала держателю возможность перемагнитить полосу и увеличить себе остаток.

В современных карточных платежах Track 3 не участвует. Сетевые правила оставляют её как факультативную историческую возможность, но массовая приёмная инфраструктура опирается на Track 1 и Track 2 [62, 65].

Сервисный код

Три цифры сервисного кода на Track 1 и Track 2 задают условия приёма карты и потому влияют на маршрутизацию и проверки безопасности. Каждая позиция действует независимо. Первая описывает interchange и наличие чипа, вторая — требования эмитента к авторизации, третья — допустимые услуги и требования к PIN. Полный набор значений по позициям задан в ISO/IEC 7813:2006, Table 3 [62]. На рис. 4 разобран код `201` из дампа MTI 0100 в гл. 6: международная карта с чипом, обычная авторизация, без ограничений по услугам и без обязательного PIN.

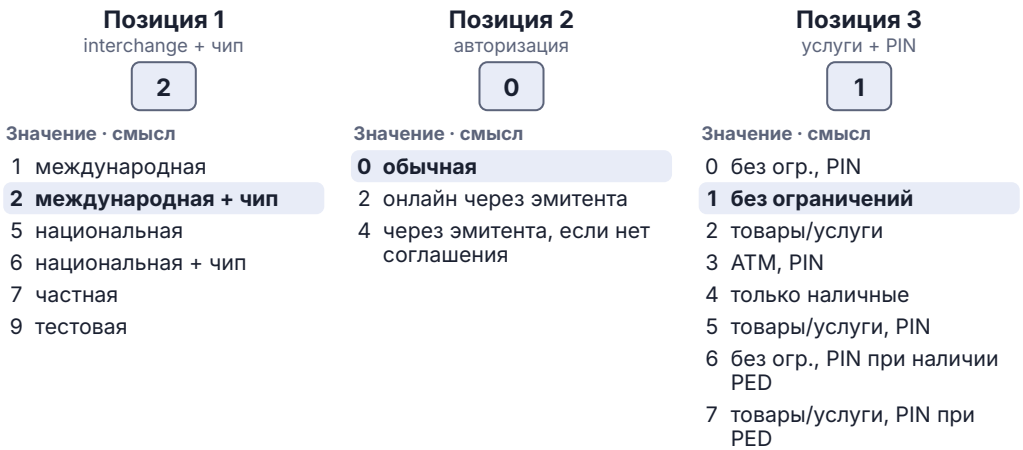


Рис. 4 — Сервисный код на Track 2: три независимые позиции; выделены значения примера `201`.

В реализациях платёжных сетей эмитент различает данные магнитной полосы и данные чипа в том числе по сервисному коду; в чиповом приложении он передаётся как тег `5F30` словаря данных EMV [31]. Поэтому эмитент проверяет магнитное CVV/CVC1 и чиповое iCVV как разные коды [65, 66].

4.3 Коды верификации

Подлинность карты подтверждают коды верификации: CVV/CVC1 на магнитной полосе, CVV2 на пластике для CNP-операций, iCVV в чипе. Каждый код проверяется в своём канале по своему входному набору, поэтому компрометация одного канала не открывает остальные.

CVV на магнитной полосе

CVV у Visa и CVC1 у Mastercard — трёхзначное значение, записанное в дискреционных данных на Track 1 и Track 2 магнитной полосы. Эмитент вычисляет его из данных карты и собственных секретных ключей; в расчёт входят PAN, срок действия и сервисный код [65]. CVV на карте не печатается: его получает только считыватель магнитной полосы.

Терминал считывает полосу и отправляет данные Track 2 в авторизационном сообщении. Эмитент извлекает CVV из полученных данных, сам пересчитывает ожидаемое значение по тем же входным параметрам и своему ключу и сравнивает. Совпадение означает, что полоса не подменена; расхождение означает, что данные скопированы или подделаны, и транзакция отклоняется.

CVV2: код для операций без физического предъявления карты

Три цифры, напечатанные на обратной стороне карты (у American Express это четыре цифры на лицевой), образуют CVV2, или CVC2 у Mastercard. Это код для операций без физического присутствия карты (*card-not-present*, CNP): покупок в интернете, заказов по телефону. CVV2 вычисляется отдельно от магнитного CVV/CVC1 и намеренно отличается от него, хотя оба значения привязаны к одной и той же карте [65].

Если злоумышленник перехватил PAN и срок действия из чека, утёкшей базы или фишинга, ТСП с проверкой CVV2 не примет интернет-покупку без трёх цифр с обратной стороны карты. Защита не абсолютна: CVV2 можно подсмотреть, сфотографировать или выманить, но атакующему придётся компрометировать отдельно ещё один фактор.

Магнитное CVV защищает от подделки полосы: без ключей эмитента злоумышленник, знающий PAN и срок действия, не вычислит CVV и не запишет его на чистую полосу. CVV2 защищает канал CNP — даже владея Track 2, злоумышленник не узнает три цифры с обратной стороны, они вычисляются отдельно и на полосе не записаны.

Покупатель оплачивает заказ в интернете, вводит PAN и срок действия, но ошибается в CVV2. Эмитент видит несовпадение и возвращает код N (CVV2 Not Matched) в DE 44.[1] Если шлюз или ТСП поддерживает 3-D Secure (протокол аутентификации держателя для CNP-операций, см. гл. 11), транзакция переводится в *challenge* (этап интерактивной проверки), и держатель подтверждает личность через ACS (Access

[1] Точное расположение результата проверки CVV2 в DE 44 различается между карточными сетями; здесь и далее ссылка на DE 44 указывает на поле в целом.

Control Server, сервер аутентификации на стороне эмитента). После успешной аутентификации эмитент может одобрить операцию даже с неверным CVV2: 3DS даёт более сильное подтверждение подлинности, чем три цифры на пластике, и ответственность за фрод смещается к эмитенту по правилам переноса ответственности (*liability shift*, см. раздел 11.6) [13]. CVV2 и 3DS работают как две проверки с разным весом; логика «CVV2 не совпал, отказать» верна при недоступном 3DS.

iCVV: защита от клонирования

Когда карточные сети начали внедрять чипы EMV и потребовали отличать чиповые транзакции от магнитных, появился риск: данные Track 2 из чипа можно было скопировать на магнитную полосу поддельной карты. Ответом стал iCVV (integrated circuit card verification value; у Mastercard этот механизм называется Chip CVC), альтернативное *статическое* значение кода верификации, прошитое в чип на этапе персонализации и используемое для *chip-initiated transactions*, то есть транзакций, инициированных чтением чипа [65, 66]. Оно отличается от значения магнитной полосы, и по нему эмитент отделяет данные чипа от данных полосы. От динамического CVC3, о котором речь дальше, iCVV/Chip CVC отличается тем, что не пересчитывается от транзакции к транзакции.

Чип хранит Track 2 Equivalent в теге 57: это эквивалент второй дорожки для передачи в авторизационном сообщении. Если скопированные из чипа данные Track 2 Equivalent предъявить как магнитную полосу, эмитент отклонит операцию: значение относится к чиповому профилю, а для магнитной полосы эмитент ожидает другой проверочный код. Криптография EMV остаётся отдельной защитой; iCVV решает узкую задачу — не дать *chip-derived data*, то есть данным, полученным с чипа, работать как данным обычной магнитной полосы.

Один алгоритм, разные сервисные коды

CVV/CVC1, CVV2 и iCVV эмитент вычисляет одним алгоритмом: входом служат PAN, срок действия и сервисный код, а секретом — ключ верификации. Различается только сервисный код, подставляемый в расчёт (табл. 2): для CVV/CVC1 используется настоящий код полосы, для CVV2 — фиктивный `000`, для iCVV — `999` [67]. Значение, верное для одного канала, не проходит проверку в другом.

Таблица 2 — Статические коды верификации: один алгоритм, разная подстановка сервисного кода.

Код	Где хранится	Сервисный код в расчёте	Канал приёма
CVV/CVC1	дискреционные данные Track 1 и Track 2 полосы	настоящий код полосы	магнитная полоса
CVV2/CVC2	напечатан на пластике, на полосу не пишется	`000`	CNP: интернет, заказ по телефону
iCVV/Chip CVC	Track 2 Equivalent чипа, тег 57	`999`	чиповые транзакции

Сервисные коды `000` и `999` на магнитной полосе недопустимы: они служат константами расчёта CVV2 и iCVV и не обозначают условий приёма карты. Visa запрещает записывать их на полосу и рекомендует эмитентам отклонять операции

с сервисным кодом `000` или `999` [68]. Перенос чиповых данных на полосу отсекает сверка кода: скопированный Track 2 Equivalent несёт iCVV, рассчитанный с кодом `999`, а в операции со считыванием полосы эмитент сверяет значение с CVV, рассчитанным по сервисному коду из дорожки, и при несовпадении отклоняет операцию [67, 68].

dCVV и CVC3: отличие от криптограммы EMV

В обычной транзакции EMV карта генерирует криптограмму, связанную с конкретной суммой, терминалом и параметрами операции. Криптограмма — центральный механизм аутентификации в EMV [31]; динамические коды семейства dCVV/CVC3 (dynamic CVV, динамический CVV) применяются точечно. В *contactless mag-stripe profile* у Mastercard, где бесконтактное ядро эмулирует данные магнитной полосы для приёма устаревшими терминалами, используется CVC3, меняющийся от транзакции к транзакции [69]. Сводить любую чиповую проверку к «dCVV» ошибочно: для контактного и бесконтактного EMV основным доказательством подлинности остаётся криптограмма, а CVC3 — частный механизм в отдельных профилях сетей. Криптограмма EMV подробно разбирается в разделе 7.8.

4.4 Что нельзя хранить после авторизации

PCI DSS жёстко разделяет данные карты на те, что допустимо сохранить после авторизации, и те, что должны исчезнуть сразу. Ошибка здесь может стоить компании права принимать карты [70].

Данные держателя карты

Первая категория, данные держателя карты (CHD, *cardholder data*): PAN, имя держателя, срок действия и сервисный код [64]. Эти данные *можно* хранить после авторизации, но только при соблюдении требований PCI DSS. PAN защищается шифрованием, токенизацией или маскированием, доступ к нему жёстко ограничен и протоколируется. PCI DSS отдельно требует делать PAN нечитаемым при электронном хранении; имя, срок действия и сервисный код сами по себе в это требование *unreadable* не входят, но при хранении рядом с PAN остаются частью данных держателя карты в том же контролируемом периметре [70, 71].

Чувствительные данные аутентификации

Вторая категория, SAD (*sensitive authentication data*): полные данные магнитной полосы или их эквивалент на чипе, коды верификации карты и PIN/PIN-блок [64]. Эти данные **запрещено** хранить после авторизации в любом виде: ни в открытом, ни в зашифрованном, ни в хешированном, ни на бумаге, ни в логах. Запрет закреплён требованием 3.3.1 PCI DSS [70, 72].

PAN нужен ТСП для возвратов, разрешения диспутов и отчётности, поэтому его хранят хотя бы в токенизированном виде. SAD нужны только в момент авторизации, чтобы подтвердить подлинность карты или держателя. После авторизации их ценность для бизнеса падает почти до нуля, а ценность для злоумышленника максимальна. Получив один PAN, злоумышленник попытается провести CNP-покупку; у ТСП и эмитента остаются CVV2, 3DS и проверки риска фрода. Получив полные

данные Track 2 с CVV, он изготовит клон карты для физического терминала. Получив PIN, снимет наличные в банкомате.

ВАЖНО

Частая инженерная причина утечки CHD и SAD — журналы. Разработчик включает подробное логирование авторизационных сообщений при отладке, и полные данные Track 2 вместе с CVV оказываются в текстовом файле на сервере, который команда не считает частью платёжного периметра и не защищает по требованиям PCI DSS. PCI DSS требует, чтобы при обычном отображении PAN сводился к BIN и последним четырём цифрам, если нет документированной деловой необходимости показывать больше, а CHD и SAD не попадали в логи [70, 73].

4.5 Карта как идентификатор и как инструмент аутентификации

Платёжная карта совмещает идентификатор счёта и средство доказательства, что операцию инициирует законный держатель; в инженерной практике эти роли нужно держать врозь.

Карта как идентификатор. PAN — номер, по которому платёжная система определяет, к какому счёту в каком банке относится транзакция. В этом смысле PAN аналогичен номеру банковского счёта или IBAN (International Bank Account Number, международный номер банковского счёта) и отвечает на вопросы «куда направить запрос?» и «с какого счёта списать деньги?». PAN напечатан на карте, виден невооружённым глазом, попадает в чеки в маскированном виде, фигурирует в выписках и отчётах. Идентификатор открыт по своей функции: чтобы направить платёж на нужный счёт, номер должен быть известен системе.

Карта как инструмент аутентификации. CVV, CVV2, данные чипа с криптограммой, PIN — всё это отвечает на другой вопрос, можно ли доверять именно этой операции. Задача — подтвердить, что транзакцию инициировал законный держатель карты или, как минимум, тот, кто физически владеет картой. В отличие от идентификации, аутентификация работает только пока секретные данные остаются секретными: утёк PIN — атакующий аутентифицируется вместо держателя.

Карточная индустрия долго смешивала эти две роли. В эпоху импринтеров (механических устройств, переносивших оттиск рельефных цифр карты на бумажный слип) 1950–1980-х годов для совершения платежа достаточно было предъявить карту: оттиск на слипе одновременно идентифицировал счёт и «аутентифицировал» держателя — физическое присутствие карты считалось достаточным доказательством. Магнитная полоса добавила CVV, но проблему не решила, потому что данные полосы статичны и копируются. Чип с динамической криптограммой впервые разделил идентификацию и аутентификацию на уровне технологии. PAN по-прежнему идентифицирует счёт, а криптограмма, уникальная для каждой транзакции, доказывает, что чип физически присутствовал в момент операции.

Токенизация (см. гл. 9) закрепляет это разделение. Идентификатор-токен становится бесполезным за пределами конкретного контекста использования, а аутентификация выполняется криптографическими средствами, не зависящими от знания номера карты.

Когда кто-то предлагает «просто проверить номер карты» для подтверждения платежа, отделите открытый идентификатор от аутентификационного фактора, который должен быть секретным, одноразовым и привязанным к контексту.

5 Жизненный цикл транзакции

Покупатель прикладывает карту в кофейне, терминал показывает «одобрено». Деньги продавец увидит на счёте позже, иногда через несколько суток. Карточная транзакция проходит фазы — авторизацию, клиринг, расчёт — и сумма в них не обязана совпадать. Между записями фаз и банковской выпиской возникают *расхождения*, на которых построена ежедневная сверка (см. раздел 31.1).

5.1 Авторизация

Авторизация — единственная фаза карточного платежа, которая идёт в реальном времени и видна покупателю. Для покупателя контакт с платёжной системой заканчивается на ответе терминала; клиринг, расчёт и возможный диспут проходят позже без его участия. В эти несколько секунд фиксируются реквизиты, по которым затем пойдут клиринг и спор.

Путь авторизационного запроса

Когда держатель прикладывает карту к терминалу, вставляет её или проводит магнитной полосой, терминал считывает данные карты и формирует авторизационный запрос. Это структурированное сообщение в формате ISO 8583, формат разобран в гл. 6. Внутри собраны как минимум PAN в DE 2 (Data Element, элемент данных) и данные Track 2 в DE 35 или их чиповый эквивалент в DE 55, сумма и валюта операции в DE 4 и DE 49, идентификаторы терминала и ТСП в DE 41 и DE 42, категория ТСП — MCC (Merchant Category Code) — в DE 18, а также тип операции, который задают MTI (Message Type Indicator, тип сообщения) и код обработки (*processing code*) в DE 3.

Сообщение уходит эквайеру — банку или процессору, обслуживающему этот терминал. Эквайер выполняет первичные проверки: валидность терминала, соответствие MCC, базовые правила антифрода на своей стороне. Затем он маршрутизирует запрос в карточную сеть [13]. Сеть по IIN/BIN определяет эмитента или его процессор и передаёт запрос адресату.

Весь путь от терминала к эквайеру, в сеть, эмитенту и обратно должен уложиться в жёсткие сроки. У Visa публичные правила задают верхние пределы ожидания для авторизаций с POS-терминалов (POS, Point-of-Sale, точка продажи) порядка нескольких секунд, с более коротким пределом в Европе. Таймауты для снятия наличных в банкомате (ATM, Automated Teller Machine) задаются отдельной строкой в таблице «Maximum Time Limits for Authorization Request Response» актуальной редакции Visa Core Rules [13]. Если ответ не пришёл вовремя, за эмитента может ответить сама Visa через механизм Stand-In Processing (STIP). STIP одобряет операции с низким профилем риска: сумма в пределах нормы для карты и ТСП, знакомая география, отсутствие признаков фрода. Неясная операция чаще отклоняется: STIP решает по параметрам, заданным эмитентом, а ответственность за одобренную или отклонённую в STIP операцию остаётся на эмитенте [13]; поэтому эмитент открывает STIP только для низкорисковой части потока. У Mastercard пределы ожидания и показатели доступности задаются в спецификациях сообщений и контролируются через нормативы доступности авторизации [13, 46].

Решение эмитента

Получив авторизационный запрос, эмитент или его процессор решает одобрить или отклонить операцию по группам проверок, которые укладываются в доли секунды:

- **проверка карты** — существует ли карта с таким PAN? Не заблокирована ли она? Не истёк ли срок действия? Совпадает ли CVV или криптограмма?
- **проверка баланса** — достаточно ли средств на счёте дебетовой карты или доступного кредитного лимита у кредитной?
- **лимиты и ограничения** — не превышен ли дневной лимит на операции? Не заблокирована ли карта для этого типа операций, например запрет на интернет-покупки? Не ограничена ли география использования?
- **антифрод** — соответствует ли операция типичному поведению держателя? Нет ли признаков компрометации карты? Не входит ли ТСП в списки повышенного риска?
- **аутентификация держателя** — для чиповых транзакций верификация криптограммы ARQC (Authorization Request Cryptogram, см. гл. 7); для CNP (Card-Not-Present, без физического предъявления карты) — результат 3-D Secure, если он был; для магнитной полосы — CVV.

По результатам этих проверок эмитент формирует ответ с кодом ответа в DE 39. Значение `00` означает, что операция одобрена; `05` — общий отказ без детализации; `51` — недостаточно средств; `14` — неверный номер карты. Полный список кодов зависит от профиля ISO 8583 и правил конкретной сети; базовая модель стандартизована, но сети дополняют её собственными значениями и уточнениями [15, 55, 74]. Классификация кодов по следующему действию (жёсткий, мягкий финансовый, аутентификационный, технический, непрозрачный) и правила повторов разобраны в разделе 33.2.

Если транзакция одобрена, эмитент присваивает ей код авторизации в DE 38 — шестисимвольный идентификатор, привязывающий одобрение к конкретному запросу. На этапе клиринга именно по нему сопоставят авторизацию с финансовой записью. Одновременно эмитент блокирует запрошенную сумму на счёте держателя — холд (*hold*). Деньги ещё не списаны, но уже недоступны для других операций.

Срок жизни холда

Правила карточных сетей задают окно между авторизацией и моментом, когда транзакцию нужно либо представить в клиринг, либо отменить сообщением *reversal*. У Visa для большинства транзакций с физическим предъявлением карты это окно составляет 5 календарных дней; для операций без предъявления — 10 дней; для оценочной авторизации в гостиницах, круизах и аренде автомобилей — до 30 дней. У Mastercard клиринговое окно зависит от типа авторизации (*final*, *undefined*, *preauthorization*) и находится в диапазоне 7–30 календарных дней — пункт 3.15.1 «Transaction Presentment Time Frames» Mastercard Transaction Processing Rules. Эти окна и задают, как долго эмитент держит неиспользованный резерв; точный момент снятия холда зависит ещё и от внутренних правил эмитента [13, 46].

Числа 5, 7 и 30 дней отражают минимальный цикл обработки: время доставки или оказания услуги, передачу клирингового файла от эквайера в сеть и буфер на задержки между участниками. Длинные сроки для гостиниц и аренды автомобилей соответствуют реальному промежутку между авторизацией при заселении (*check-in*) и финальной суммой при выезде. Эти сроки исторически сложились как компромисс сетей; их изменение требует согласования со всеми участниками расчёта.

В системе эмитента холд — это запись в таблице, синхронизация которой с доступным остатком держится на корректной последовательности коммитов авторизации и отката. Любой сбой в этой последовательности оставляет клиенту видимое расхождение даже без участия продавца.

ПРАКТИКА

Если клиент жалуется, что «деньги списали, но покупка не прошла», чаще всего речь идёт о холде. Авторизация была одобрена и средства заблокированы, но продавец не завершил операцию: например, отменил заказ на своей стороне, не отправив *reversal*. Деньги вернутся автоматически по истечении холда, а в мобильном банке клиент до этого видит уменьшенный доступный баланс.

Сложнее, когда расхождение возникает внутри хоста эмитента. Частичный отказ обработки рассинхронизирует холд и счёт: запрос одобрен, обновление таблицы холдов не сохранилось — резерв остаётся без нормального срока снятия при видимом клиенту отказе. Обратный случай: холд снят при откате незафиксированной транзакции, и клиент тратит средства, которые ещё `pending`. Защита — отдельный журнал холдов с меткой времени авторизации и признаком сверки с клирингом.

5.2 Клиринг

Авторизация — обещание заплатить, клиринг — предъявление счёта, формальное требование эквайера к эмитенту исполнить это обещание. Клиринг инициирует эквайер: он формирует у себя пакет финансовых записей и отправляет его в сеть, а эмитент получает пакет как адресат. Клиринг идёт пакетами (*batches*) и не ждёт ответа в секундах.

Формирование клирингового файла

В конце операционного дня — а у некоторых процессоров и несколько раз за день — эквайер формирует клиринговый файл (*clearing file*): пакет записей обо всех транзакциях, прошедших авторизацию за период. Каждая запись содержит реквизиты транзакции: PAN, сумму, которая может отличаться от авторизованной, валюту, дату и время, идентификатор ТСП, MCC, код авторизации и другие данные, нужные для расчёта [15]. Отправку такого файла с итоговыми суммами называют финансовым представлением (*financial presentment*, *capture*); в этот момент эквайер фиксирует финальную сумму обязательства [46, 55].

Формат клирингового файла зависит от карточной сети. Visa использует BASE II, в котором каждый тип записи обозначается *Transaction Code* (TC); Mastercard — формат IPM (Integrated Product Messages) с MTI 1240 для первого представления (*first presentment*); НСПК для внутрироссийских операций по картам «Мир» и по картам международных сетей — собственный профиль ISO 8583 с расширениями НСПК. Состав полей и коды причин относятся к закрытой части документации, доставка идёт пакетным файлом через систему электронного документооборота НСПК [75]. Во всех трёх форматах сеть получает набор записей с реквизитами транзакций, по которым нужно провести расчёт [13, 15].

Сопоставление с авторизацией

Получив клиринговый файл, сеть сопоставляет каждую запись с соответствующей авторизацией по комбинации PAN, суммы, кода авторизации и даты. Сумма в клиринге не обязательно равна авторизованной — возможны исходы:

- **auth = clearing** (штатный сценарий, большинство покупок) — покупка по POS в рознице: терминал формирует авторизационный запрос на финальную сумму, она же и приходит в клиринг.
- **auth > clearing** — авторизация была больше итогового чека. Классические случаи — предавторизация отеля или АЗС на ориентировочную сумму, фактический счёт меньше. Эквайер выпускает частичный *reversal* (*partial reversal*) до клиринга, либо клиринговая запись приходит сразу на финальную сумму; разница освобождается у держателя при снятии холда.
- **auth < clearing** — клиринговая сумма выше авторизованной. Типичный пример — ресторан, где авторизация проходит на сумму заказа, а в клиринг попадает сумма с чаевыми. Правила сетей допускают такое превышение для чаевых и категорий путешествий и развлечений (*travel&entertainment*), но ограничивают его процентом или фиксированным лимитом; точные пределы зависят от MCC, программы и текущей редакции правил [13, 15].

Если представление в клиринг приходит позже применимого окна или данные в нём не совпадают с исходной авторизацией, сеть всё равно может доставить это представление эмитенту. Но для эквайера это позднее представление (*late presentment*): риск диспута повышается, и эквайер теряет часть защитного срока по спору [13, 38, 46].

Более опасный сбой: клиринговый файл теряется или не принимается сетью из-за ошибки формата. Эквайер узнаёт об этом, когда сеть возвращает отчёт с перечнем отклонённых записей — *rejected transactions*. Эквайер исправляет записи и повторно отправляет файл в следующем пакете клиринга. Правила сетей ограничивают срок повторной подачи. У Visa *financial presentment* должен попасть в сеть в пределах авторизационного окна (5 дней для *card-present* и MIT, 10 — для CNP, до 30 — для оценочных авторизаций, в зависимости от типа операции), иначе авторизация аннулируется [13]. У Mastercard клиринг должен прийти в пределах 7–30 календарных дней [46]. Если эквайер не уложился, эмитент автоматически снимает холд, и деньги возвращаются в доступный баланс держателя. Для продавца это значит, что операция прошла в терминале, товар отдан, но через карточную сеть деньги уже не получить, и взыскивать придётся иначе.

Если авторизации не было вовсе, эмитент списывает средства по полученной клиринговой записи без предварительного холда; клиринг, как и в штатном сценарии, инициирует эквайер. Основанием списания служит сама клиринговая запись, в штатном сценарии ему предшествует авторизация. Риск переходит к эквайеру и продавцу; именно этот сценарий описывает принудительная отправка (*force post*) в разделе 5.6 [46].

Расчёт interchange и комиссий

На этапе клиринга сеть рассчитывает interchange для каждой транзакции — межбанковскую комиссию, которую эквайер платит эмитенту; см. раздел 2.3. Ставка interchange зависит от параметров, зафиксированных в клиринговой записи: типа карты, MCC, способа приёма, географии операции и ряда дополнительных признаков. Тип карты бывает дебетовый, кредитный или корпоративный; способ приёма — чип, магнитная полоса или CNP; география — внутренняя или международная.

Параллельно сеть начисляет собственные комиссии: плату за обработку, за международную маршрутизацию, за использование специальных сервисов. В документах самих сетей эту составляющую называют *scheme fees* и *assessments*. По итогам обработки всех клиринговых записей за период сеть формирует чистые расчётные

позиции (*net settlement positions*) для каждого банка-участника — итоговые суммы, которые один банк должен другому с учётом взаимозачёта встречных потоков.

5.3 Межбанковский расчёт (*settlement*)

Расчёт завершает жизненный цикл транзакции — именно здесь деньги переходят между банками. До этого момента средства оставались на счёте держателя; авторизация лишь заблокировала сумму, клиринг сформировал требование. На этапе расчёта требование исполняется в расчётной инфраструктуре платёжной системы [1, 13, 46].

Нетто-расчёт

Карточные сети используют нетто-расчёт. Вместо отдельной межбанковской операции на каждую транзакцию сеть суммирует все встречные обязательства между парами банков за расчётный период и переводит только разницу. Если за день банк А как эквайер должен банку Б как эмитенту миллион рублей interchange, а банк Б как эквайер должен банку А как эмитенту восемьсот тысяч, фактически переводятся только двести тысяч от А к Б. Этот механизм многократно сокращает количество и объём межбанковских проводок.

Сеть проводит расчёт через назначенный расчётный банк или иной расчётный сервис, предусмотренный её правилами. У Visa локальные операции, если в стране доступен соответствующий сервис, проходят через National Net Settlement Service (NNSS), остальные — через International Settlement Service; правила отдельно определяют расчётный банк и расчётный счёт участника. У Mastercard итоговый документ дня — ежедневное уведомление по нетто-расчётам, и оно считается окончательной записью о движении средств между участниками [13, 46].

Когда продавец получает деньги

Расчёт (*settlement*) — движение средств между банками внутри платёжной системы; этим завершается жизнь транзакции в сети. *Выплата по договору эквайринга* (*payout*) — отдельный шаг: эквайер, уже получив средства от сети, перечисляет их продавцу по условиям договора, ежедневно, через день или по иному графику, за вычетом MSC. Сроки фаз и выплаты сведены в табл. 3. В продуктовом реестре эти два события соответствуют разным переходам и собственному графику выплат (см. раздел 35.6).

Срок выплаты задаёт договор: после расчёта в сети эквайер перечисляет деньги продавцу по его графику — например, на следующий рабочий день или по SLA (Service Level Agreement, договор об уровне обслуживания) конкретного провайдера. Для продавца с большим оборотом или низкой маржой каждый дополнительный день задержки замораживает оборотные средства.

Таблица 3 — Сроки фаз карточной транзакции и выплаты продавцу

Фаза	Срок	Акторы	Протокол	Состояние
Авторизация	T0 .. T+ несколько с	терминал ↔ эквайер ↔ сеть ↔ эмитент	ISO 8583 (0100/0110)	холд на счёте держателя, сумма заблокирована
Клиринг	T0 .. T+1 раб. дня	эквайер → сеть → эмитент (batch конца дня)	файлы клиринга	сумма зафиксирована
Расчёт	T+1 .. T+2 раб. дня	сеть ↔ корсчета банков	нетто-расчёт	деньги между банками
Выплата (по договору)	T+1 .. T+5 раб. дней	эквайер → ТСП по графику договора	банковский перевод	зачисление на счёт ТСП

5.4 Одностадийная и двухстадийная схема

Описанная выше схема двухстадийна, *dual message system* (DMS): авторизация и клиринг идут разными сообщениями в разное время. Сначала терминал спрашивает «можно?», потом эквайер предъявляет финансовую запись. Это стандарт для большинства карточных покупок [13, 46].

Одностадийная архитектура, *single message system* (SMS), совмещает авторизацию и финансовую запись в одном сообщении. Такой запрос одновременно спрашивает разрешение *и* фиксирует финансовое обязательство. Ответ эмитента означает сразу «одобрено» и «деньги можно считать списанными», а отдельного клирингового шага не требуется.

Где используется каждая схема

Двухстадийная схема доминирует в обычных карточных покупках: в магазинах, ресторанах, во многих интернет-операциях. Она допускает расхождение между авторизованной и финальной суммой — это нужно там, где возможны чаевые, довзвешивание товара или частичная отмена. При этом эквайер группирует транзакции в пакеты и обрабатывает их сериями.

Одностадийная схема — стандартная модель для банкоматов (ATM). Когда держатель снимает наличные, разделять авторизацию и финансовую запись нет смысла: деньги уже выданы физически, и задним числом операцию не отменить. По той же логике одностадийная схема используется в некоторых дебетовых сетях, где транзакция проходит на точную сумму и считается окончательной [13, 46].

На уровне ISO 8583 различие выражается в MTI. Авторизационный запрос в двухстадийной схеме имеет MTI 0100, финансовый запрос в одностадийной — MTI 0200; соответствующие ответы — MTI 0110 и MTI 0210. Структура MTI подробно разбирается в разделе 6.2.

ВАЖНО

Двухстадийная или одностадийная схема — свойство канала приёма, его не выбирают ни продавец, ни разработчик. POS-терминал по протоколу Visa или Mastercard отправляет двухстадийный поток; банкомат в сети ATM — одностадийный.

Гибридные варианты

Различие между двухстадийной и одностадийной схемой размывается. Visa, Mastercard и процессоры поверх них поддерживают гибридные сценарии, в которых одобренная авторизация при определённых условиях автоматически доводится до финансовой записи или обслуживается общей инфраструктурой авторизации и клиринга. Гибриды снижают трудозатраты на стороне эквайера, но добавляют сложности процессинговым системам, которым приходится поддерживать оба сценария в одной кодовой базе.

5.5 Отмена платежа

Карточная транзакция в каждый момент находится в одной из фаз, и способ отмены определяется фазой. Этим карточная отмена отличается от банковского перевода, который либо прошёл, либо нет.

Отмена авторизации (*reversal*)

Reversal, отмена авторизации, аннулирует авторизацию *до того*, как транзакция ушла в клиринг. В терминах ISO 8583 это отдельный тип сообщения. MTI 0400, *Reversal Request*, требует ответа от эмитента; MTI 0420, *Reversal Advice*, односторонне уведомляет о состоявшемся *reversal*. Эквайер отправляет одно из них в сеть с просьбой аннулировать ранее одобренную авторизацию.

В сообщениях *reversal* DE 39 несёт код причины отмены, а не код ответа; конкретные значения — таймаут на стороне эмитента, ошибка разбора ответной криптограммы ARPC (Authorization Response Cryptogram), обрыв связи и прочие — задаются спецификацией сети или процессора.

Reversal возникает в нескольких типовых сценариях. Покупатель передумал у кассы; терминал не получил ответ на авторизацию по таймауту и отправляет *reversal*, чтобы закрыть возможное одобрение; кассир ошибся с суммой и отменяет операцию. При успешном *reversal* эмитент снимает холд со счёта держателя, и средства возвращаются в доступный баланс обычно мгновенно или за несколько минут. Правила Mastercard требуют от эквайера обеспечить отправку *Reversal Request*/0400 в течение 24 часов после отмены ранее авторизованной операции или её завершения на меньшую сумму; у Visa *reversal* также обязателен, если одобрение пришло уже после таймаута [13, 46, 55].

Reversal работает в реальном времени, без финансовой записи и без возвратной транзакции: деньги ещё не перемещались. Возможность *reversal* исчезает с уходом транзакции в клиринг: попавшую в клиринговый файл авторизацию *reversal* уже не отменит [15].

Аннулирование до расчёта (*void*)

void, или аннулирование, — термин эквайринга и кассового ПО: он означает отмену операции до окончательного клиринга, а в карточной сети реализуется через сообщения *reversal*. В двухстадийной схеме (*dual-message*) отмена (*cancellation*) должна произойти до того, как эквайер отправит транзакцию в клиринг; если отмена случилась уже после отправки онлайн-авторизации, устройство или продавец обязаны сформировать *reversal*, а саму транзакцию убрать из пакета клиринга или пометить как *void* [55].

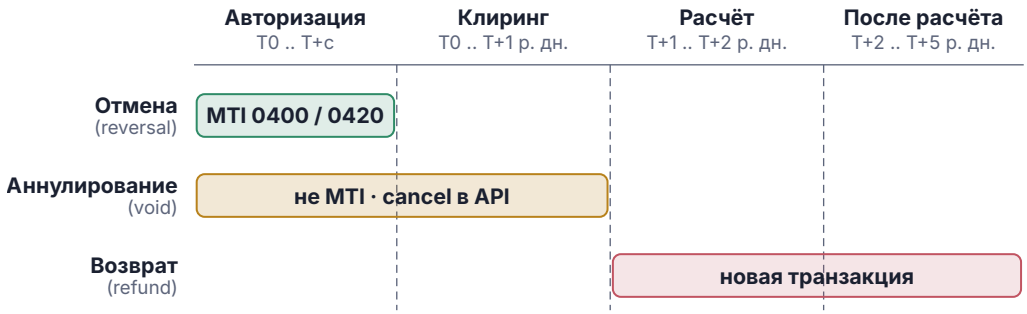


Рис. 5 — *Reversal*, *void* и возврат на временной шкале транзакции.

Для держателя карты *void* и *reversal* выглядят одинаково — холд снимается, деньги возвращаются на счёт. Технически *void* обрабатывается медленнее, потому что он привязан к циклу клиринга, и если файл уже отправлен, исправленная запись попадёт только в следующий пакет клиринга.

ПРАКТИКА

В API большинства PSP и платёжных шлюзов вы встретите метод `cancel` или `void`, абстрагирующий оба механизма. Если транзакция ещё не ушла в клиринг, PSP отправляет *reversal*; если ушла, но расчёт не произошёл, применяется *void*. Для разработчика, интегрирующего платежи, это удобная абстракция, но за ней стоят разные процессы с разной скоростью возврата средств клиенту.

Возврат после расчёта (*refund*)

Возврат — единственный способ вернуть деньги после того, как расчёт завершён и средства фактически перемещены между банками. В отличие от *reversal* и *void*, которые аннулируют исходную транзакцию, возврат — *новая* транзакция в обратном направлении: эквайер инициирует перевод от продавца к держателю через ту же карточную сеть.

Возврат проходит собственный цикл авторизации, клиринга и расчёта, только в обратную сторону. В Visa TADG (Transaction Acceptance Device Guide) возврат описан как онлайн-авторизационное сообщение с последующим клирингом; Mastercard допускает возврат в двухстадийной (*dual-message*) и одностадийной (*single-message*) схемах, а для двухстадийной требует онлайн-авторизацию [46, 55].

Для держателя карты средства по возврату поступают на счёт через несколько рабочих дней: возврат проходит полный цикл клиринга и расчёта. Для продавца возврат обычно дороже *reversal*: часть расходов исходной покупки автоматически не компенсируется; эквайер нередко берёт отдельную комиссию за саму операцию возврата. Все три механизма — *reversal*, *void* и возврат — расположены относительно фаз транзакции на рис. 5.

ВАЖНО

Распространённая ошибка при проектировании платёжной интеграции — использовать возврат там, где достаточно *reversal* или *void*. Если клиент отменяет заказ через минуту после оплаты, а система продавца отправляет возврат вместо *reversal*, клиент будет ждать возврата несколько дней вместо нескольких минут, продавец не вернёт уплаченную эквайеру комиссию, а эквайер зафиксирует лишнюю транзакцию. Практическое правило: отменять как можно раньше. *Reversal* лучше *void*, *void* лучше возврата.

5.6 Граничные случаи

Схема «авторизация на точную сумму, клиринг на ту же сумму, расчёт через день» покрывает основную массу розничных покупок. Остальные сценарии — предавторизация, инкрементальная и частичная авторизация, отложенная авторизация и принудительная отправка — отличаются своими сроками и распределением риска.

Предавторизация (*pre-authorization*)

Предавторизация, *pre-auth*, — авторизация, при которой финальная сумма заранее неизвестна. Типовые примеры — гостиница и аренда автомобиля. В момент заселения или получения машины продавец авторизует оценочную сумму — ожидаемую стоимость проживания или депозит за автомобиль, — а итоговая определяется при выезде или возврате и может оказаться как меньше, так и больше авторизованной.

В сетевых правилах *pre-auth* — самостоятельный тип запроса. Visa различает *Estimated Authorization* и *Incremental Authorization*, а Mastercard рекомендует кодировать запрос как *preauthorization*, если сумма оценочная или если операция может вообще не завершиться. Эмитент ставит холд, заранее зная, что финальный клиринг может отличаться от исходной оценки. Допустимые пределы расхождения зависят от MCC, типа ТСП и конкретного сценария, поэтому точные пороги берут из актуальных правил сети [13, 46, 55].

Инкрементальная авторизация (*incremental authorization*)

Инкрементальная авторизация увеличивает сумму ранее одобренной авторизации без отмены исходной. Продавец отправляет дополнительный авторизационный запрос, ссылающийся на исходный через код авторизации или специальный идентификатор, и эмитент увеличивает холд на запрошенную сумму [13, 46, 55].

Типичный сценарий — гостиница, где гость продлевает пребывание или заказывает дополнительные услуги. Вместо повторного цикла «авторизовать — отменить» продавец наращивает сумму инкрементально. Поддержка такого потока зависит от сети, региона, MCC и настроек эмитента или эквайера, поэтому при проектировании интеграции нужно закладывать запасной сценарий — например, новую авторизацию на дополнительную сумму.

Частичная авторизация (*partial authorization*)

Частичная авторизация — сценарий, в котором эмитент одобряет транзакцию только на часть запрошенной суммы. Держатель пытается оплатить покупку на тысячу рублей, но на карте доступно только семьсот. Вместо полного отказа с кодом `51` эмитент одобряет операцию на семьсот рублей; продавец предлагает клиенту доплатить оставшиеся триста наличными или другой картой [46, 55].

Частичная авторизация требует поддержки на всех уровнях. Терминал обрабатывает частичное одобрение и предлагает доплату, POS-система корректирует чек, кассир должен понимать, что происходит. Чаще всего схема встречается с предоплаченными и подарочными картами, где остаток заранее известен и ограничен.

ВАЖНО

Если ваша система не поддерживает частичную авторизацию, убедитесь, что терминал или платёжный шлюз не заявляет такую поддержку в сетевом индикаторе частичного одобрения. Например, у Mastercard для этого используется *Partial Approval Terminal Support Indicator* в DE 48, подэлемент 61. Необработанное частичное одобрение ведёт к расхождению в учёте: продавец отпускает товар на полную сумму, а списывается только часть [46].

Отложенная авторизация (*deferred authorization*)

Отложенная авторизация — механизм, при котором транзакция совершается без онлайн-авторизации, а авторизационный запрос отправляется позже, по восстановлении связи. Классические сценарии — оплата на борту самолёта, где терминал работает офлайн и авторизации уходят после посадки; паркинг, где сумма определяется по времени стоянки; платные дороги и общественный транспорт.

При отложенной авторизации терминал собирает данные карты, фиксирует операцию локально и позже формирует авторизационный запрос с соответствующим флагом. Эмитент может одобрить или отклонить этот запрос, но товар или услуга уже предоставлены, и кредитный риск несут эквайер и продавец. Поэтому сети ограничивают отложенную авторизацию сроком: у Mastercard она допустима для операций с физическим предъявлением карты при сбое связи, запрос уходит по восстановлении связи, по возможности в течение 24 часов; у Visa такие авторизации нужно запросить в течение 24 часов с момента исходной операции, а для ряда наземных транспортных MCC — 4111, 4112, 4131 — допускается до 4 суток. В авторизационном сообщении передаётся *Deferred Authorization Indicator* со значением `5206` в поле 63.3; индикатор обязателен для сценариев с физическим предъявлением карты (*card-present*) и без него (*card-absent*) [13, 55].

Принудительная отправка (*force post*)

Принудительная отправка — механизм, при котором продавец отправляет транзакцию в клиринг без предварительной онлайн-авторизации, используя код авторизации, полученный по телефону через голосовую авторизацию (*voice authorization*).

Такой сценарий возникает, когда онлайн-авторизация невозможна: терминал не работает или пропала связь, но провести платёж нужно. Продавец получает голосовую авторизацию у эмитента или через эквайера и затем использует этот код при обработке транзакции. Mastercard оговаривает: код, полученный голосовой авторизацией, не защищает от *chargeback* по авторизационным основаниям [46].

Онлайн-проверки криптограммы здесь нет, часть контроля переносится на человека и процедуры эквайера, ответственность за последствия несёт продавец. Принудительная отправка остаётся резервным сценарием: устойчивые каналы связи и офлайн-режимы терминалов закрывают большую часть случаев, где раньше требовалась голосовая авторизация.

Покупка с выдачей наличных (POS-кешбэк)

С термином «cashback» в обиходе путаница. Чаще всего так называют маркетинговый бонус, который эмитент возвращает на счёт держателя по итогам периода; физические наличные при этом не выдаются. POS-кешбэк устроен иначе: продавец выдаёт держателю карты часть запрошенной суммы наличными вместе с розничной покупкой. У Visa это «Cash at POS» или «Visa Cashback», у Mastercard «Purchase

Таблица 4 — Граничные случаи карточной авторизации.

Механизм	Когда сумма известна	Онлайн-авторизация	Кто несёт риск	Типичный MCC
pre-auth	позже	да	эквайер/ТСП	7011 (гостиницы), 7512 (аренда авто)
incremental auth	постепенно	да (несколько)	эквайер/ТСП	7011
partial auth	сразу, но покрытие неполное	да	ТСП	любой (чаще предоплаченные)
deferred auth	позже	нет (офлайн)	эквайер/ТСП	4511 (авиа), 7523 (паркинг)
force post	сразу	голосовая	ТСП	любой

with Cashback» (PWCB); в ПС Мир — «Выдача наличных при совершении покупки». На прикладном уровне POS-терминала действует максимальный лимит выдачи наличных за операцию: в ПС Мир — 5000 руб.; Visa задаёт лимит по странам, для многих рынков это 200 USD в национальном эквиваленте; у Mastercard для Debit Mastercard потолок — 100 USD в местной валюте, если правила рынка не задают иной [13, 46].

POS-кешбэк допустим только для контактных и бесконтактных чиповых карт; ввод по магнитной полосе и ручной ввод PAN запрещены. Кешбэк привязан к покупке; выдачу без покупки допускают правила отдельных рынков. Авторизация всегда онлайн — *floor limit* (порог суммы, ниже которого терминал вправе одобрить операцию офлайн) для операции принудительно равен нулю (раздел 7.7), а CVM (Cardholder Verification Method, метод верификации держателя карты) обязателен. Набор допустимых методов различается у сетей: Visa требует PIN или CDCVM (Consumer Device CVM, верификация на устройстве пользователя — например, отпечаток пальца или Face ID на смартфоне), подпись и No CVM запрещены; Mastercard требует CVM даже ниже бесконтактного лимита CVM, а региональные правила сужают набор до PIN. С 18.04.2026 Visa отменила требование проводить кешбэк только во внутренних операциях; Mastercard обязывает эмитентов поддерживать кешбэк и во внутренних, и в трансграничных операциях [13, 46, 55].

На уровне EMV покупка с выдачей наличных кодируется через два поля суммы. Теги передаются в формате TLV спецификации EMV [31]. `0x9F02` (*Authorized Amount*) содержит общую сумму операции — покупку плюс наличные, `0x9F03` (*Other Amount*) — отдельно сумму наличных. Тип операции несёт тег `0x9C`; конкретные значения, маркирующие наличие наличной части, задаются спецификациями сетей и различаются между ними. Сумма наличных ограничена прикладным лимитом терминала, не описанным в EMV-ядре, и задаётся правилами сети для конкретного рынка.

В ISO 8583 DE 4 несёт общую сумму. Отдельную сумму наличных Mastercard передаёт в DE 54 (*Amounts, Additional*), Visa — в поле 61.1 (*Other Amounts*); в DE 55 дублируются EMV-теги `0x9F02`, `0x9F03` и `0x9C`. Эмитент может одобрить операцию полностью или отказать только в наличной части, оставив покупку. На уровне ответа DE 39 для этого предусмотрены отдельные коды «наличная часть не одобрена, покупка проходит»; их конкретные значения различаются между Visa, Mastercard и ПС Мир, и эквайер обычно конвертирует фирменный код сети в универсальный для своего хоста ответ. *Reversal* аннулирует операцию целиком; отмена или возврат,

инициированные кассиром по требованию держателя, допустимы только для покупки — общей суммы за вычетом наличной части (`0x9F02` минус `0x9F03`; в ISO 8583 — DE 4 минус DE 54 или поле 61.1), но не для выданных наличных [46, 55].

Interchange по POS-кешбэку устроен иначе, чем по ATM-снятию. Тарифные сетки Visa и Mastercard относят покупку с выдачей наличных к розничной дебетовой программе, а не к *cash advance*: у Mastercard в американской публичной таблице ставок строка «Purchases, Purchases with Cash-back and Unique» объединяет покупку и покупку с кешбэком в единый тариф [76]; у Visa наличная часть в *Consumer Debit Acceptance Fee* исключается из объёма продаж и не относится к отдельной ставке *cash advance*. ПС Мир в межхостовых правилах задаёт свою ставку для розничной выдачи; конкретные значения — в приложении 4 «Тарифы» к Правилам ПС Мир, которое публикует НСПК [75]. Для ТСП кешбэк сокращает выручку наличными, которую иначе пришлось бы инкассировать. В Великобритании услугу поддерживает государственная программа защиты доступа к наличным: Закон «Financial Services and Markets Act 2023» наделил FCA полномочиями обеспечивать разумную доступность услуг внесения и снятия наличных (*cash deposit and withdrawal services*), а оператор крупнейшей банкоматной сети LINK ведёт реестр точек выдачи наличных без покупки (*cashback without purchase*) [77, 78]. В Канаде POS-кешбэк действует с 1990-х как штатная функция дебетовой сети Interac и принимается крупными продуктовыми сетями [79].

Для держателя сумма наличных суммируется с дневным лимитом снятия наличных по карте, если эмитент объединяет лимиты ATM и POS; часть банков ведёт их раздельно. Когда общего лимита не хватает на весь запрос, эмитент вправе одобрить только покупочную часть и отклонить наличную: правила Mastercard для этого определяют отдельный код ответа DE 39 87 «Purchase Amount Only, No Cash Back Allowed» [46]. Эмитент не обязан принимать такой исход: он может отказать в операции целиком кодом 51 «insufficient funds» или 61 «exceeds withdrawal amount limit»; тогда продавцу остаётся предложить держателю повторить операцию без кешбэка. Структура суммы, по которой эмитент принимает это решение, передаётся в авторизационном запросе в DE 4, поле суммы наличных и DE 55.

В учёте POS-кешбэк проходит как гибрид покупки и выдачи наличных, поэтому суммы нужно разделять по лимитам, interchange, отменам и последующей сверке.

6 ISO 8583: формат сообщений

В процессинге авторизационный запрос на покупку 1 250 рублей 50 копеек занимает 153 байта. Дамп читается как рассказ о транзакции, когда известна грамматика ISO 8583: где заканчивается тип сообщения, где начинаются значения, как найти конкретное поле. Разберём её на одном MTI 0100 и его ответе MTI 0110 — том же жизненном цикле, что в гл. 5, только в байтах.

6.1 Структура сообщения

Сообщение целиком — на рис. 6: байты в hex-виде с подсветкой по полям. Содержимое каждого поля, его начало и декодированный смысл — в табл. 5. Поля переменной длины (LLVAR) выделены другим цветом; префикс длины LL в первых двух байтах каждого LLVAR отмечен тёмной кромкой.

Грамматика ISO 8583 одинакова для всех сообщений и состоит из частей в строгом порядке:

- **MTI** (Message Type Indicator) — четыре первых байта (`0x30 31 30 30`, в ASCII даёт `0100`). Отвечают на вопрос, *что это за сообщение*: авторизация, финансовое сообщение, *reversal*, сетевое управление.
- **bitmap** — следующие восемь байт (`0x72 3C 04 81 20 C0 80 00`). Битовая карта отвечает на вопрос, *какие поля присутствуют дальше*.
- **элементы данных** (data elements, DE) — сами значения; в нашем сообщении их пятнадцать: PAN (Primary Account Number), сумма, STAN (Systems Trace Audit Number, номер трассировки), код обработки, идентификаторы терминала и ТСП, временные метки и ещё несколько признаков транзакции.

Offset	Hex bytes												ASCII
0000	30	31	30	30	72	3C	04	81	20	C0	80	00	0100r<.. ...
000C	31	36	32	32	30	30	31	32	31	32	33	34	162200121234
0018	35	36	30	38	39	32	30	30	30	30	30	30	560892000000
0024	30	30	30	30	30	30	31	32	35	30	35	30	000000125050
0030	30	33	31	37	31	37	33	30	34	35	34	38	031717304548
003C	32	37	33	31	31	37	33	30	34	35	30	33	273117304503
0048	31	37	32	36	31	32	30	37	31	30	30	30	172612071000
0054	36	31	32	33	34	35	36	33	34	32	32	30	612345634220
0060	30	31	32	31	32	33	34	35	36	30	38	39	012123456089
006C	32	3D	32	36	31	32	32	30	31	31	32	33	2=2612201123
0078	34	35	36	37	38	39	30	54	45	52	4D	30	4567890TERM0
0084	30	30	31	4D	45	52	43	48	41	4E	54	30	001MERCHANT0
0090	30	30	30	30	30	31	36	34	33				000001643

MTI · Bitmap · fixed · LLVAR · кромка: префикс LL

Рис. 6 — Hex-дамп MTI 0100 с подсветкой полей по типу.

Таблица 5 — Поля MTI 0100: тип, смещение, длина и значение

Поле	Тип	Смещение	Длина, байт	Значение
MTI	MTI	`0x00`	4	`0100`
Bitmap	Bitmap	`0x04`	8	DE 2, 3, 4, 7, 11, 12, 13, 14, 22, 25, 32, 35, 41, 42, 49
DE 2 (PAN)	LLVAR	`0x0c`	18	LL=16, `2200121234560892`
DE 3 (Proc Code)	fixed	`0x1e`	6	`000000`
DE 4 (Amount)	fixed	`0x24`	12	`000000125050`
DE 7 (Trans DT)	fixed	`0x30`	10	`0317173045`
DE 11 (STAN)	fixed	`0x3a`	6	`482731`
DE 12 (Local Time)	fixed	`0x40`	6	`173045`
DE 13 (Local Date)	fixed	`0x46`	4	`0317`
DE 14 (Expiry)	fixed	`0x4a`	4	`2612`
DE 22 (POS Entry)	fixed	`0x4e`	3	`071`
DE 25 (POS Cond)	fixed	`0x51`	2	`00`
DE 32 (Acq Inst)	LLVAR	`0x53`	8	LL=06, `123456`
DE 35 (Track 2)	LLVAR	`0x5b`	36	LL=34, `2200121234560892=26122011234567890`
DE 41 (Terminal)	fixed	`0x7f`	8	`TERM0001`
DE 42 (Merchant)	fixed	`0x87`	15	`MERCHANT0000001`
DE 49 (Currency)	fixed	`0x96`	3	`643`

ISO 8583 устроен иначе, чем самоописывающиеся форматы вроде JSON или XML. Сначала идёт тип операции, затем bitmap с картой присутствия, затем значения подряд в порядке возрастания номеров. Тег и длина внутри каждого поля не передаются.

В примере все числовые поля закодированы в ASCII — каждая цифра занимает один байт. Промышленные IFS могут паковать числа в BCD (Binary Coded Decimal) и вдвое сокращать числовые поля; подробности кодировки, ответ эмитента MTI 0110 и *reversal* — в разделе 6.5.

6.2 MTI и стадия транзакции

MTI — первые четыре цифры сообщения; каждая цифра кодирует свой признак: версию стандарта, класс операции, функцию в потоке и инициатора пары. Раскладка для MTI 0100 — на рис. 7.

В паре запрос/ответ меняется только третья цифра — функция; класс, версия и инициатор постоянны. Массовые карточные интеграции работают на версии `0` (ISO 8583:1987) [34]; редакция 1993 года работает в клиринге Mastercard IPM [14], редакция 2003 года широкого распространения не получила. 4-я цифра фиксирует инициатора обмена; в ответе это значение сохраняется, хотя отправитель сообщения меняется.

Запрос идёт сквозным маршрутом (*end-to-end*), advice и notification — от узла к узлу (*point-to-point*). Эквайер отправляет запрос и ждёт решения эмитента; advice и notification на уровне приложения не отвергаются, поэтому доставку гарантируют повторы с теми же ссылочными полями. Повтор кодируют заменой 4-й цифры

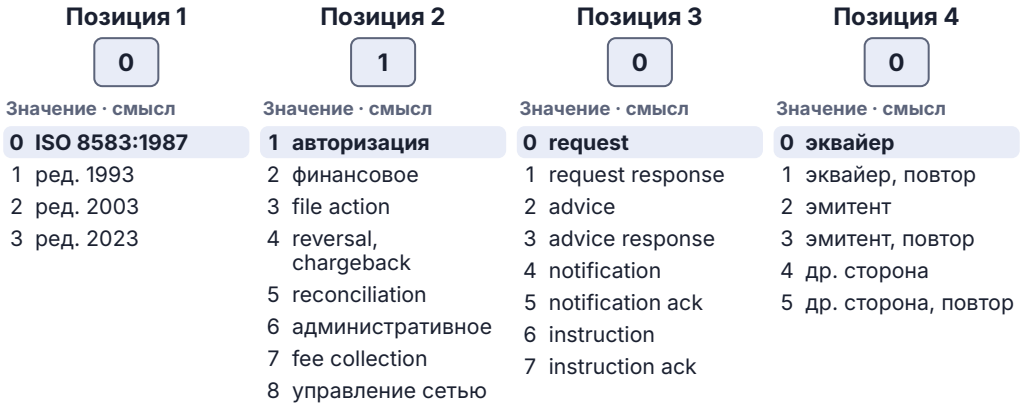


Рис. 7 — MTI 0100 по четырём позициям; выделены значения примера.

на нечётную: MTI `0121` — та же advice, что MTI `0120`, но переотправленная после недоставки.

Из 10 000 теоретических комбинаций большая часть нерабочая. MTI `1102` формально означал бы запрос на авторизацию от эмитента, чего в карточной модели не бывает: запрос на авторизацию всегда инициирует эквайер. Учебные обзоры раскладывают MTI по разрядам, но реальный список MTI задаёт IFS партнёра (Interface Specification, подробно — в разделе 6.6): стандарт фиксирует общую схему, а конкретный процессинг или сеть оставляют от неё узкий рабочий набор [34, 74].

Канонические пары запрос/ответ для ISO 8583:1987:

- MTI 0100 / MTI 0110 — authorization request / response: авторизация без списания;
- MTI 0120 / MTI 0130 — authorization advice / advice response: уведомление об операции, прошедшей через *stand-in* или офлайн;
- MTI 0200 / MTI 0210 — financial request / response: авторизация и финансовое представление одним сообщением;
- MTI 0220 / MTI 0230 — financial advice / advice response: офлайновая операция или *force post*;
- MTI 0320 / MTI 0330 — file action advice / response: обновление справочников и BIN-таблиц;
- MTI 0400 / MTI 0410 — reversal request / response: *reversal* в реальном времени;
- MTI 0420 / MTI 0430 — reversal advice / response: отложенный *reversal*;
- MTI 0500 / MTI 0510 — reconciliation request / response: сверка итогов;
- MTI 0600 / MTI 0610 — административные сообщения;
- MTI 0800 / MTI 0810 — network management: echo test, обмен ключами, sign-on/off.

В паре MTI 0100/MTI 0110 эмитент принял решение об авторизации, а деньги в расчётном смысле ещё не двинулись; в клиринг операцию отправит эквайер, не эмитент, отдельным сообщением в клиринговом файле (BASE II TC у Visa, IPM MTI 1240 у Mastercard, собственный профиль ISO 8583 у НСПК для карт «Мир» [80] — разбор в гл. 14, 15 и 16).

MTI 0120 — advice: парный 0130 определён спецификацией, но многие IFS его не поддерживают: для них доставка самой advice закрывает диалог. Отложенная авторизация (*deferred authorization*) — сценарий для операций с лимитом времени короче онлайн-запроса к эмитенту: часть транспортных турникетов пропускает

пассажира по локальным правилам, а запрос авторизации уходит эмитенту уже после прохода [81]; другие держат пассажира до онлайн-ответа эмитента (раздел 13.5). Обработка в режиме *stand-in* (STIP, stand-in processing) включается, когда эмитент или его процессинг недоступны: карточная сеть отвечает на запрос авторизации от его имени по заранее заданным правилам и досылает advice эмитенту после восстановления связи [82, 83].

Пара MTI 0200/MTI 0210 — финансовое сообщение; в карточных диалектах именно она даёт одностадийный сценарий с авторизацией и финансовым представлением в одной транзакции.

Reversal идёт через MTI 0400/MTI 0410 в одних интерфейсах и через MTI 0420/MTI 0430 в других. Разница повторяет деление на запрос и advice: 0400 — запрос *reversal* в реальном времени, на который эмитент отвечает; 0420 — одностороннее уведомление о *reversal*. Пару выбирает спецификация интерфейса [34].

Служебная пара MTI 0800/MTI 0810 обслуживает *сетевой диалог*: «sign-on» — логический вход в сеть с началом сессии и обновлением ключей; «echo» («echo-test») — периодическая проверка живости канала; «cutover» — переключение на новый набор ключей или новую версию профиля без разрыва связи.

6.3 Bitmap

После MTI идёт bitmap — восемь или шестнадцать байт, в которых каждый бит отвечает за присутствие одного элемента данных. Значения идут после него: bitmap указывает только, какие поля искать дальше в теле сообщения [34].

Поздние форматы вроде TLV (Tag-Length-Value), как в DE 55 для EMV, делают сообщение самоописывающимся: каждое поле несёт собственный тег и длину. Bitmap проектировался в 1970–80-х, когда каждый байт в телекоммуникационном канале был на счету, и проверить бит маской было дешевле, чем пройти по тегам.

В нашем примере основная bitmap — `0x72 3C 04 81 20 C0 80 00`. Бит N в bitmap — флаг присутствия DE N. Биты внутри байта нумеруются слева направо, от старшего (MSB, Most Significant Bit — бит с наибольшим весом, $2^7 = 128$ в восьмибитном байте) к младшему (LSB, Least Significant Bit — бит с наименьшим весом, $2^0 = 1$). В нашей таблице бит 1 каждого байта — его MSB; разворот по ячейкам — на рис. 8.

Первый бит первого байта (`0x72` = `0111 0010`) равен 0 — значит, дополнительной (secondary) битовой карты нет и сообщение укладывается в первые 64 DE. Остальные единицы дают: DE 2, 3, 4, 7, 11, 12, 13, 14, 22, 25, 32, 35, 41, 42, 49 — правдоподобный набор для обычной авторизации, в котором есть идентификация карты, сумма, временной контекст, ТСП и способ ввода.

Если бы старший бит `0x72` стоял в единице, после первой bitmap шли бы ещё восемь байт — дополнительная (secondary) bitmap для DE 65…128. Старший бит уже её первого байта аналогично включает третью (tertiary) bitmap на DE 129…192. Получаются три яруса присутствия — основная (primary), дополнительная (secondary), третьего уровня (tertiary). Secondary в реальных сообщениях обычна, её используют и Visa BASE I, и Mastercard CIS; tertiary публично описана только в Visa BASE I и встречается редко, для специализированных служебных полей.

Декодер принимает байты сообщения и возвращает MTI и список номеров присутствующих DE; сами значения он читает по длине и формату каждого поля из IFS партнёра.

Hex	1	2	3	4	5	6	7	8
0x72		DE 2	DE 3	DE 4			DE 7	
0x3C			DE 11	DE 12	DE 13	DE 14		
0x04						DE 22		
0x81	DE 25							DE 32
0x20			DE 35					
0xC0	DE 41	DE 42						
0x80	DE 49							
0x00								

Рис. 8 — Bitmap MTI 0100, развёрнутая в 64 ячейки: заполненная — DE присутствует.

```
from collections.abc import Iterable

MTI_SIZE = 4
BITMAP_SIZE = 8
PRIMARY_START = MTI_SIZE
SECONDARY_START = PRIMARY_START + BITMAP_SIZE


def parse_mti(message: bytes) → str:
  if len(message) < MTI_SIZE:
    raise ValueError("сообщение короче 4 байт -- MTI не извлечь")
  return message[:MTI_SIZE].decode("ascii")


def parse_bitmap(message: bytes) → list[int]:
  primary = message[PRIMARY_START:SECONDARY_START]
  if len(primary) < BITMAP_SIZE:
    raise ValueError("primary bitmap должен занимать 8 байт")

  # Старший бит primary -- флаг расширения, а не DE 1.
  has_secondary = bool(primary[0] & 0b1000_0000)
  # Развёртка primary даёт кандидаты на DE 1..64; отбрасываем DE 1 -- это флаг.
  present = [de for de in _bits_to_de_numbers(primary, offset=0) if de ≠ 1]

  if has_secondary:
    secondary = message[SECONDARY_START : SECONDARY_START + BITMAP_SIZE]
    if len(secondary) < BITMAP_SIZE:
      raise ValueError("secondary bitmap ожидается, но не помещается")
    present.extend(_bits_to_de_numbers(secondary, offset=64))
  return present


def _bits_to_de_numbers(block: bytes, offset: int) → Iterable[int]:
  for byte_index, byte in enumerate(block):
    # f"{byte:08b}" -- строка из 8 битов, от старшего к младшему: "01110010".
    # Позиция в строке = номер бита в байте, бит "1" -- DE присутствует.
    for bit_index, bit in enumerate(f"{byte:08b}"):
      if bit == "1":
        yield offset + byte_index * 8 + bit_index + 1
```

ПРАКТИКА

При разборе инцидента начинайте с bitmap: по нему сразу видно, есть ли в сообщении DE 35 (Track 2), DE 38 (код авторизации), DE 39 (код ответа) и DE 55 (чиповые данные EMV). Этого хватает, чтобы снять половину вопросов ещё до полного чтения дампа.

Декодер выше намеренно ограничивается primary и secondary bitmap и возвращает только список номеров полей: MTI — шаг первый, bitmap — второй. Полный разбор сообщения добавляет третий шаг: для каждого номера DE из списка взять формат и длину из IFS партнёра, отрезать заданное количество байт от тела сообщения и декодировать значение.

Для полей фиксированной длины спецификация задаёт длину; у LLVAR и LLLVAR префикс длины идёт первым внутри самого поля. `LL` — двузначный префикс длины, `LLL` — трёхзначный; размер префикса в байтах зависит от кодировки: в ASCII LL занимает 2 байта, LLL — 3 байта; в BCD те же цифры пакуются вдвое плотнее, LL умещается в 1 байте, LLL — в 2 (со старшим нулём для выравнивания по границе байта). Кодировка длины может не совпадать с кодировкой значения и оговаривается отдельной строкой IFS; эту строку читают до разбора поля.

6.4 DE — элементы данных

Для MTI 0100/MTI 0110 рабочие поля распадаются на пять смысловых групп; полный каталог DE с форматами и длинами задают сетевая спецификация и IFS партнёра [34].

Идентификация и маршрутизация

DE 2 (PAN) идентифицирует карту. DE 35 (Track 2 Data) укладывает в одну строку тот же PAN вместе со сроком действия, сервисным кодом и дискреционными данными. DE 32 — идентификатор эквайера или банка-инициатора. DE 37 (RRN, Retrieval Reference Number — сквозной ссылочный номер операции) проходит через запрос, ответ и все последующие сообщения; по нему операцию ищут в отчётах, диспутах и операторских инструментах [34].

Деньги и время

DE 3 (Processing Code) кодирует тип операции: покупка, возврат, снятие наличных, запрос баланса. DE 4 хранит сумму с фиксированным масштабом; масштаб задаёт код валюты из DE 49 по таблице экспонентов ISO 4217 [84]. DE 7 фиксирует сетевое время передачи сообщения. DE 11 — STAN (Systems Trace Audit Number), шестизначный номер трассировки, по которому процессинг связывает запрос с ответом. DE 12 и DE 13 — локальное время и дата терминала.

Шесть цифр STAN — счётчик. Диапазон от `000000` до `999999` инициатор исчерпывает и запускает заново: тот же STAN повторяется в более поздних сообщениях, а у нагруженного процессора счётчик делает полный оборот и в пределах суток. Поэтому операцию однозначно находит только STAN вместе с идентификатором инициатора (DE 32) и сетевым временем отправки (DE 7): один и тот же STAN с разным DE 7 обозначает разные операции. Локальные время и дата терминала (DE 12, DE 13) на эту роль не годятся: они идут в часовом поясе точки приёма и зависят

от настройки её часов, а эмитент и эквайер сверяют спор по единому сетевому времени из DE 7.

Контекст точки приёма

DE 22 (POS Entry Mode) показывает, как терминал получил данные карты: вручную, с магнитной полосы, с чипа, бесконтактно, в интернет-операции. DE 25 (POS Condition Code) добавляет условия операции. DE 41 и DE 42 — идентификаторы терминала и ТСП — привязывают транзакцию к точке приёма.

Одни и те же PAN и сумма получают у эмитента разную оценку — чиповая покупка в супермаркете и ручной ввод реквизитов на сайте идут по разным шкалам риска.

Результат авторизации

DE 39 (Response Code) — поле решения: одобрена операция или нет. При одобрении эмитент добавляет DE 38 (идентификатор авторизации), который связывает авторизацию с последующим клирингом.

В запросе этой группы нет: решение ещё не принято. Чтение MTI 0110 начинается с DE 39.

Слух о «премиальном коде одобрения»

Отдельного кода успешной авторизации для премиальной карты в DE 39 нет. Слух обычно приписывают Visa, иногда Mastercard: обычная карта якобы получает один код одобрения, привилегированная — другой, а знают об этом только посвящённые. Слух держится на реальных деталях: нескольких кодах успеха в ISO 8583, слове «VIP» в одном из них и идентификаторе продукта в BIN-данных Visa; ни одна из них не связывает код ответа с тарифом карты.

В DE 39 действительно несколько кодов одобрения. Базовый ISO 8583 задаёт `00` (approved), `08` (honour with identification), `10` (approved for partial amount) и `11`, помеченное в стандарте дословно «approved (VIP)». В трёхзначной редакции обычное одобрение и «approved (VIP)» кодируются как `000` и `003`; в четырёхзначной таблице ISO 8583:2023 это `0003` «approved (VIP)» [74]. Несколько кодов успеха прописаны в опубликованном стандарте; скрытой сетевой тайны здесь нет.

«VIP» в этом коде не означает премиального держателя. В ISO это вариант одобрения, семантику которого эмитент задаёт сам. У Visa V.I.P. — название авторизационной системы (VisaNet Integrated Payment), ядра VisaNet, которое обрабатывает авторизации и замещает недоступного эмитента в режиме *stand-in* [82, 83]; устройство этой системы разбирает гл. 14. Омоним превращает техническое имя системы в мнимый признак статуса держателя.

Тип продукта Visa действительно передаёт открыто, только не в коде ответа. Для этого в BIN-данных запроса есть идентификатор продукта (*product ID*): `F` — Classic, `C` — Signature, `N` — Platinum, `I` — Infinite [85]. Это поле описывает продукт карты и передаётся в запросе; решение эмитента в DE 39 оно не заменяет.

Код `11` «approved (VIP)», идентификатор продукта и V.I.P. существуют на самом деле и принадлежат разным механизмам. Слух о секретном коде возникает там, где идентификатор продукта принимают за код ответа, а «VIP» — за тарифную ступень.

Чиповые данные

DE 55 — TLV-контейнер EMV: он несёт криптограммы, TVR (Terminal Verification Results, результаты проверок терминала), AID (Application Identifier, идентификатор платёжного приложения карты), ATC (Application Transaction Counter, счётчик операций приложения) и другие теги. Криптограмму вычисляет карта, терминал её только передаёт, и по ней эмитент проверяет, что операция пришла с подлинного чипа. Подробный разбор тегов — в гл. 7 [86].

DE 55 в примере умышленно опущен: чиповый хвост в реальной авторизации увеличивает сообщение, а без него легче разделить грамматику ISO 8583 и детали EMV.

6.5 Ответ, отмена и нюансы кодирования

В запросе на рис. 6 эквайер просит одобрить бесконтактную покупку на сумму 1 250 рублей 50 копеек по карте `2200121234560892` в терминале `TERM0001` у ТСП `MERCHANT0000001`.

MTI 0110 — ответ эмитента

MTI 0110 короче запроса: ответ обходится без PAN и Track 2, зато несёт DE 39 (response code) и, при одобрении, DE 38 (authorization ID response). STAN, сумму, дату и идентификатор терминала эмитент повторяет, чтобы процессинг сопоставил ответ с запросом [34].

Ответный bitmap в примере — `0x32 38 00 00 0E C0 80 00`: DE 3, DE 4, DE 7, DE 11, DE 12, DE 13, DE 37, DE 38, DE 39, DE 41, DE 42, DE 49. DE 37 несёт RRN — сквозной ссылочный номер для сопоставления в клиринге; DE 38 — код авторизации (в нашем примере `A1B2C3`); DE 39 фиксирует решение эмитента: `00` — одобрение, `51` — недостаток средств [34].

Отмена авторизации (*reversal*) — MTI 0400 и MTI 0420

Одни интерфейсы оформляют *reversal* как MTI 0400/MTI 0410, другие как MTI 0420/MTI 0430. FIS/Worldpay разделяет варианты request и advice [34]. Смысл общий — «считать предыдущее сообщение несостоявшимся» или «скорректировать его последствия». Возврат денег клиенту — отдельная операция; различия *reversal*, *void* и *refund* подробно разбирает раздел 5.5.

Сообщение *reversal* однозначно ссылается на исходную операцию, хотя DE 7 у него собственное (время создания самого сообщения): локальные время и дата (DE 12, DE 13) копируются из исходного сообщения, а исходные MTI, STAN и DE 7 эмитент получает в «original data elements» DE 90 [34]. DE 90 идентифицирует отменяемую операцию составным ключом — исходные MTI, STAN, дата и время, идентификаторы эквайера и направляющего института, — а не стабильным сетевым идентификатором [74, 87, 88]. Стандарт описывает *reversal* как отмену авторизации или финансового сообщения, поэтому DE 90 указывает ровно на одно исходное сообщение; многошаговое наслоение правок ведут клиринг и внешние реестры (гл. 31, раздел 31.4).

Скрытая структура: подполя и битовые поля

Один и тот же байт значит разное в разных профилях, а внутри одного поля прячутся собственные подполя со своей структурой.

POS Entry Mode (DE 22). В нашем сообщении DE 22=`071`. В этом профиле код описывает бесконтактный чиповый сценарий с терминалом, который умеет принять PIN: третий разряд кодирует способность терминала принимать PIN (*PIN entry capability*), а факт верификации PIN через DE 22 не передаётся. Для бесконтактного чипа FIS/Worldpay предусматривает два значения DE 22, `07` и `08`, а другой IFS может назначить свой код [34]. Код, написанный под один процессинг, у другого партнёра молча падает; такие диалектные расхождения ловят на тестовых транзакциях, до промышленной эксплуатации (*production*).

Сумма с неявным масштабом (DE 4 и DE 49). DE 4 хранит сумму без десятичной точки. Масштаб задаёт код валюты из DE 49 по таблице экспонентов ISO 4217: для рубля и евро — две минорные единицы, для иены — ноль. В нашем сообщении DE 4=`000000125050` и DE 49=`643` (рубль), что и даёт 1 250 рублей 50 копеек.

Внутренняя структура Track 2 (DE 35). Track 2 несёт несколько подполей в одной строке: PAN, разделитель `=`, срок действия `YYMM`, трёхзначный сервисный код, далее дискреционные данные. В примере: `2200121234560892=26122011234567890` — PAN `2200121234560892`, срок `2612` (декабрь 2026), сервисный код `201`, дальше идут дискреционные данные.

Кодировка чисел: ASCII или BCD. В разобранном примере все числовые поля закодированы в ASCII — каждая цифра занимает один байт. В реальных IFS цифры могут идти в упакованном числовом формате BCD: две цифры в одном байте, числовые поля вдвое короче. ASCII удобнее при отладке в логах, BCD типичен для промышленной эксплуатации, где каждый лишний байт стоил денег на телеком-канале и времени обработки на железе 1980-х. Перед ручным чтением дампа выясните кодировку из IFS — иначе ошибка на этом этапе делает бессмысленным весь дальнейший разбор [34].

6.6 IFS поверх ISO 8583

ISO 8583 не описывает сетевой протокол целиком. Стандарт определяет *грамматику сообщения*; официальная аннотация ISO исключает способ доставки сообщений и метод расчёта из предмета стандарта [74].

Транспорт и фрейминг. Способ доставки — по TCP, через VPN, с каким заголовком и префиксом длины — стандарт не предписывает. Двух- или четырёхбайтовый префикс длины, отдельный application header, выбор между ASCII и EBCDIC (Extended Binary Coded Decimal Interchange Code — 8-битная кодировка IBM, исторически используемая на мейнфреймах процессингов) — всё это задаёт соглашение конкретного процессинга. Одни и те же сообщения передаются поверх X.25, SNA и TCP/IP [89], поэтому каждый IFS фиксирует транспорт сам, и при смене партнёра транспортную обвязку интеграции делают заново.

Криптография и ключи. PIN-блок (зашифрованный блок с PIN-кодом фиксированной длины; форматы — в разделе 10.7) передаётся в DE 52, MAC (Message Authentication Code, код аутентификации сообщения; алгоритмы CBC-MAC и CMAC, ключи и состав строки — в разделе 10.1) — в DE 64 или DE 128. Алгоритмы, формат PIN-блока, схему ключей и порядок их обмена задаёт сеть или спецификация конкретного коммутатора; сам ISO 8583 их не описывает. MAC в DE 64 или DE 128

проверяется только вместе с обвязкой вокруг ISO 8583: ключами, алгоритмом, дополнением (*padding*), составом строки и транспортной спецификацией, которые находятся вне базовой грамматики стандарта.

Состояние сессии. Sign-on, echo test, cutover, управление ключами и повторная отправка опираются на MTI 0800/MTI 0810 и на то, как конкретная система трактует таймауты, идемпотентность (гарантию, что повторная отправка того же сообщения не приведёт к двойному списанию или двойному *reversal*) и повтор.

Правила обработки. Что считать дубликатом, когда отправлять сообщение *reversal*, как долго ждать ответ, какие поля обязательны для чиповой или интернет-операции — всё это прикладные правила интерфейса, вне синтаксиса сообщения.

Одна система кодирует всё в ASCII, другая смешивает ASCII, BCD и бинарные поля. Один партнёр считает DE 32 обязательным, другой не принимает его вовсе; одному хватает DE 35, другому нужен ещё DE 2, третьему — набор частных полей под конкретный сценарий. Один профиль раскрывает дополнительные данные через DE 48, DE 60, DE 61, DE 63 или DE 124, другой собирает их в собственные подполя. Аналогично расходятся коды ответа, жизненный цикл сообщений *reversal*, cutover, транспортный заголовок, sign-on и обмен ключами. Какие поля требует конкретный канал, как профиль кодирует сумму, где размещает частные подполя и какой ответ ждёт на MTI 0800 — описывает только IFS партнёра [34].

Детали диалектов Visa, Mastercard и НСПК — в их сетевых спецификациях, как и полный справочник элементов данных и дампы MTI 0200, MTI 0420 и сетевых служебных сообщений.

Часть II

Безопасность и протоколы

Базовая модель платежа называет, кто несёт денежное обязательство, кто посылает сообщение и кто меняет запись в своём учёте. Провести операцию одного этого знания мало. Покупатель прикладывает карту к терминалу, на экране загорается сумма, авторизационный запрос уходит к эмитенту, и за доли секунды участники должны убедиться, что карта подлинная, данные не подменены, а согласие дал сам держатель. Почему такому решению можно доверять — предмет части II.

Часть I описала внешний поток между банками, сетями и продавцом; часть II разбирает внутренние проверки системы: как терминал и карта договариваются о правилах операции, как эмитент получает основания сказать «да» или «нет», как токен заменяет PAN, не нарушая жизненный цикл транзакции, как криптография заменяет статический идентификатор динамическими доказательствами подлинности и как защита данных в платеже распределяется между несколькими устройствами и стандартами.

В основе этой части — инварианты, которые повторяются в разных формах независимо от конкретной сети. EMV задаёт, как карта доказывает свою подлинность эмитенту. Бесконтактные платежи показывают, как проверка подлинности подстраивается под удобство пользователя, не ослабляя доверия к операции. Токенизация позволяет участникам обрабатывать платёж, не превращая PAN в универсальный ключ к счёту. Криптография даёт этим сюжетам общий язык секретов, ключей и криптограмм. 3-D Secure переносит проверку в электронную коммерцию, где карта и терминал не встречаются физически. PCI DSS определяет, какие данные допустимо хранить внутри системы и во что обходится их присутствие.

Часть II отвечает на вопрос, как платёж совмещает удобство и проверяемость — два требования, которые конкурируют между собой. Чип не должен замедлять оплату, токенизация — ломать регулярные списания, 3-D Secure — превращать страницу оплаты в испытание, PCI DSS — оставаться внешним аудитом, отделённым от архитектуры продукта.

Часть остаётся на уровне общих механизмов: офлайн- и онлайн-проверка, криптографическое доказательство, замена чувствительного идентификатора, удалённое подтверждение держателя, сокращение зоны хранения данных. Конкретные правила *fallback* и пороги сертификации каждой сети разбирает часть III: там те же механизмы работают в конкретных системах — Visa, Mastercard, СБП, открытом банкинге, и один принцип безопасности влечёт разные технические и коммерческие последствия в зависимости от свода правил и расчётной модели.

7 EMV

7.1 Магнитная полоса и чип

Магнитная полоса из раздела 4.2 хранит статические данные. PAN, срок действия, CVV (раскрыты в разделах 4.2 и 4.3) и сервисный код записаны на дорожке раз и навсегда при выпуске карты. Каждый считыватель получает одну и ту же последовательность байтов, и каждая считанная копия неотличима от оригинала. Это свойство сделало магнитную полосу удобной мишенью для мошенников. Достаточно один раз пропустить карту через скиммер, накладку на терминал или банкомат, незаметно считывающую дорожку, и полученные данные можно записать на чистую карту-болванку и создать клон.

В 1990-х платёжная отрасль искала способ снизить ущерб от поддельных карт: нужен был микрочип, который труднее скопировать, чем магнитную полосу. Спецификация EMV (исходно аббревиатура от Europay, Mastercard, Visa; сегодня — имя стандарта, поддерживаемого EMVCo) версии 96 стала общей платформой для такого перехода. В 1999 году появилась EMVCo, отвечающая за развитие и сопровождение набора спецификаций. Сегодня EMVCo принадлежит шести глобальным карточным сетям — American Express, Discover, JCB, Mastercard, UnionPay и Visa [90]; актуальная редакция базовых контактных книг (Books 1–3) — v4.4 от октября 2022 года, Book 4 остаётся в v4.3 от ноября 2011 года [32, 91].

В EMV подлинность карты подтверждает криптограмма, вычисленная для конкретной операции. Вместо статических данных, которые терминал транслирует дальше как есть, чиповая карта вычисляет криптограмму. Это значение зависит от суммы транзакции, валюты, даты, случайного числа терминала (*unpredictable number*, UN, свежее в каждой транзакции) и секретного ключа, который никогда не покидает чип. Скопировать криптограмму бесполезно: она валидна только для одной транзакции, а для следующей нужна новая, вычислить которую без ключа невозможно [91].

Карточные сети дополнили спецификацию экономическим стимулом — переносом ответственности (*liability shift*; подробно — раздел 11.6): риск фрода смещается на ту сторону, которая не поддержала более защищённый сценарий по правилам конкретной сети. Visa для США привязывает этот перенос к 1 октября 2015 года. Если чиповая карта используется в магазине, а терминал не поддерживает чтение чипа, ответственность несёт сторона, оставшаяся на менее защищённой технологии [92].

Из-за угрозы немедленного *chargeback* и отсроченных штрафов парк терминалов обновлялся быстрее, чем при прямом предписании регулятора.

EMV закрывает один класс фрода — клонирование статических карточных данных в операциях с физическим предъявлением карты. По данным Visa, к декабрю 2018 фрод с поддельными картами (*counterfeit fraud*) в канале с физическим предъявлением у ТСП США, перешедших на чиповый приём, упал на 80 % по сравнению с уровнем 2015 года до миграции на EMV; к марту 2019 — на 87 % у модернизированных POS и на 62 % по стране, считая и ТСП без EMV [93, 94]. Параллельно фрод сместился в канал без предъявления карты (CNP, *card-not-present*), где статическая защита остаётся прежней — отсюда экономическая мотивация для 3-D Secure.

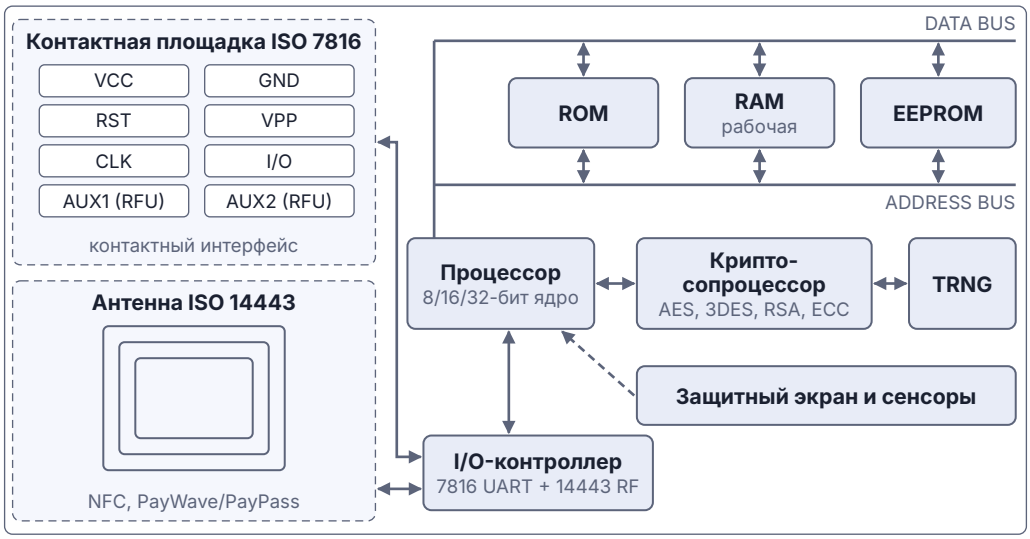


Рис. 9 — Архитектура чипа платёжной карты.

7.2 Архитектура чиповой транзакции

Чиповая карта, ICC (Integrated Circuit Card) — небольшая вычислительная система со своим процессором, криптографическим сопроцессором, оперативной памятью, постоянной памятью и перезаписываемой памятью; в последней записаны данные эмитента, счётчики транзакций и ключи [91].

Внутри чипа: апплет и аттестация

В ROM чипа записана операционная система; для платёжных карт это Java Card Classic. Платёжное приложение реализовано как *апплет* (applet), загружаемый в перезаписываемую память при персонализации и выбираемый командой `SELECT` (см. раздел 7.3).

GlobalPlatform — отраслевой консорциум (прежде Visa OpenPlatform) и его одноимённая спецификация управления содержимым смарт-карты: какие приложения на ней установлены, как они загружаются, блокируются и удаляются и какими ключами разделены [95]. Java Card исполняет апплет, GlobalPlatform управляет его жизненным циклом. Эмитент загружает, активирует, блокирует и обновляет апплеты по защищённым каналам SCP02/SCP03 (Secure Channel Protocol, шифрованный и аутентифицированный канал поверх APDU); по ним же он доставляет *issuer scripts* (команды эмитента к чипу).

В GlobalPlatform ключи разделены по доменам безопасности (*security domain*). Issuer Security Domain (ISD) принадлежит эмитенту и управляет содержимым карты, Supplementary Security Domain (SSD) — отдельному провайдеру приложения; ключи одного домена недоступны другому. Через защищённый канал апплет проходит установку (`INSTALLED`), активацию (`SELECTABLE`) и персонализацию, а эмитент позже может заблокировать (`LOCKED`) или удалить его — управление содержимым доступно и после выпуска карты.

Аппаратная база сертифицируется отдельно от апплета. EMVCo ведёт реестры одобренных интегральных микросхем (ICCN, Integrated Circuit Certificate Number)

и платформ (PCN, Platform Certificate Number); в декабре 2024 года процесс Chip & Platform Approval получил аккредитацию по ISO/IEC 17065 [96, 97].

Уровень безопасности самого чипа задаётся профилем защиты Security IC Platform Protection Profile (BSI-CC-PP-0084) по схеме Common Criteria — международной системе оценки безопасности ИТ-продуктов согласно ISO/IEC 15408 [98]. CC использует две связанные шкалы — EAL (Evaluation Assurance Level, глубина проверки) и AVA_VAN (Vulnerability ANalysis, стойкость к атакам, шкала 1–5). Базовый уровень для платёжного чипа — EAL 4+ с AVA_VAN.5 (атакующий с неограниченным временем и лабораторией); промышленные NXP JCOP, Infineon SLE и ST31 проходят на EAL 6+ с тем же AVA_VAN.5 [99]. Российский аналог — ГОСТ Р ИСО/МЭК 15408 с оценочными уровнями доверия ОУД (ОУД4 соответствует EAL 4).

Сертификация задаёт требуемый уровень стойкости: чип должен выдержать атаки без раскрытия ключа. Механизмы защиты на рис. 9:

- TRNG (true random number generator, истинный ГСЧ — генератор случайных чисел) даёт свежие nonce;
- защитный экран поверх кристалла препятствует зондированию;
- сенсоры напряжения и температуры регистрируют попытки внешнего воздействия;
- счётчики неудачных попыток необратимо стирают секреты при срабатывании сенсоров.

Эти механизмы противостоят SPA/DPA (simple/differential power analysis, анализ потребления тока микросхемой под нагрузкой), *fault injection* (*glitch* — кратковременный провал напряжения, лазерный импульс, перегрев) и физическому препарированию чипа.

Стойкость проверяема: при оценке по AVA_VAN.5 лаборатория моделирует нарушителя с оборудованием и неограниченным временем, а сертификат фиксирует достигнутый уровень. Физическая безопасность кремния — отдельная инженерная дисциплина; в протокольном разборе EMV чип выступает сертифицированным по Common Criteria чёрным ящиком, доверие к которому опирается на этот сертификат [98].

Терминал общается с чипом по правилам ISO 7816. Расположение контактов C1–C8 на площадке задаёт часть ISO/IEC 7816-2 [100], электрический интерфейс и полудуплексный протокол передачи данных (посимвольный T=0 или блочный T=1) — ISO/IEC 7816-3 [101], формат команд APDU (Application Protocol Data Unit) — ISO/IEC 7816-4 [102]. Через APDU терминал читает карту, выбирает приложение и запрашивает обработку транзакции. Команда APDU состоит из заголовка с классом, кодом инструкции и двумя параметрами и необязательных данных; в ответ карта возвращает данные и двухбайтовый код статуса SW1 SW2 (Status Word 1/2). Например, `0x9000` означает успех, `0x6A82` — файл не найден, `0x6985` — условия использования не выполнены. Первоисточник этих кодов — ISO/IEC 7816-4, а EMV Book 3 наследует их и уточняет применение для платёжных приложений [31, 102].

Чиповая карта хранит несколько независимых платёжных приложений. На одной физической карте могут сосуществовать, например, приложение Мир и приложение UnionPay (кобейдж, выпускаемый в России с 2017 года; маршрутизация и правила — в гл. 16) [103], каждое в отдельном домене безопасности с собственным набором ключей, сертификатов и параметров: ключи одного приложения недоступны другому. Приложение для операции определяется на первом шаге сценария EMV — выборе приложения.

Контактный сценарий EMV проходит фазы в следующем порядке:

- **выбор приложения** — терминал и карта согласовывают, какое платёжное приложение будет использовано;
- **аутентификация данных** — терминал проверяет, что данные на карте подлинны и не были подменены;
- **верификация держателя** — карта или терминал проверяют, что операцию инициировал законный держатель, через PIN, подпись или иной метод;
- **управление рисками** — терминал и карта выбирают между офлайн-одобрением и онлайн-авторизацией у эмитента;
- **генерация криптограммы** — карта вычисляет криптографическое значение, подтверждающее результат всех предыдущих проверок.

К моменту генерации криптограммы карте доступны данные о том, какое приложение выбрано, прошла ли аутентификация данных, как завершилась проверка держателя и нужно ли обращаться к эмитенту онлайн — криптограмма фиксирует весь этот путь.

7.3 Выбор приложения

Перед транзакцией терминал определяет, какое платёжное приложение на карте использовать. Каждое такое приложение хранится в отдельном ADF (Application Definition File) и идентифицируется *AID* (Application Identifier) — по нему терминал выбирает нужное ядро, набор правил и сценарий обработки. AID состоит из RID (Registered Application Provider Identifier) карточной сети и PIX (Proprietary Application Identifier Extension) конкретного продукта. EMV Book 1 описывает выбор по шагам: сначала терминал запрашивает у карты каталог приложений, затем согласовывает приложение из списка кандидатов [91].

Терминал начинает с обращения к каталогу PSE (Payment System Environment), а в бесконтактном сценарии — к PPSE (Proximity Payment System Environment), описанному в разделе 8.2. В ответ карта возвращает список записей с установленными приложениями, каждая содержит AID. Из этих записей терминал собирает *список кандидатов* — приложения, которые поддерживают и карта, и терминал.

На уровне протокола терминал посылает команду `SELECT` к файлу `1PAY.SYS.DDF01` или `2PAY.SYS.DDF01`, получает список записей с короткими идентификаторами файлов и номерами записей и извлекает из них идентификаторы приложений.

Если PSE на карте отсутствует — так бывает у старых карт или в конфигурациях некоторых эмитентов, — терминал использует прямой перебор. Он последовательно вызывает SELECT для каждого AID из своего списка поддерживаемых и проверяет, на какой карта ответит положительно.

Когда в списке кандидатов оказывается несколько приложений, терминал сортирует их по приоритету — тег `0x87`, Application Priority Indicator — и либо автоматически выбирает приложение с наивысшим приоритетом, либо предлагает выбор держателю. У большинства ТСП выбор происходит автоматически: на экране терминала отображается название выбранного приложения или запрос подтвердить выбор, если того требует сценарий. У Visa Debit/Credit (Classic, бренд EMV-приложений Visa — VSDC, Visa Smart Debit/Credit) в актуальном TADG (Visa Technology Asset Documentation for Global Card Acceptance, публичный технический справочник Visa) указан RID `0xA000000003`, PIX `0x1010` и полный AID `0xA0000000031010` [55].

После успешного выбора приложения терминал отправляет команду GPO (Get Processing Options). Она объявляет начало транзакции и передаёт первичные данные — сумму, валюту, дату и другие параметры. В ответ карта возвращает AIP

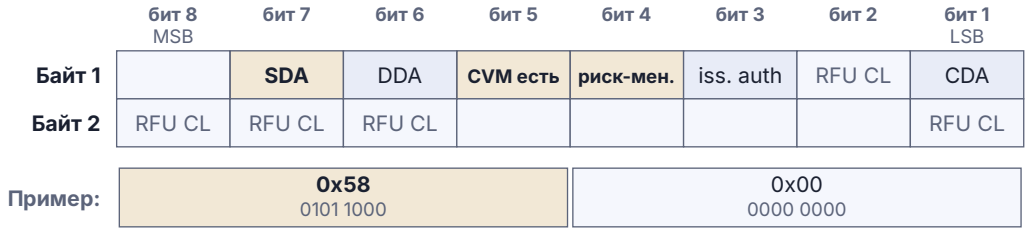


Рис. 10 — Раскладка AIP: 2 байта, MSB слева; жёлтым — биты примера `AIP = 0x5800`.

и AFL. AIP (Application Interchange Profile, тег `0x82`) — битовое поле о поддержке функций SDA, DDA, CDA (статической, динамической и комбинированной аутентификации данных), управления рисками и верификации эмитента. AFL (Application File Locator) — список файлов (по SFI, Short File Identifier) и диапазонов записей, которые терминал должен прочитать для продолжения транзакции [31]. На этом этапе терминал только выясняет, на что карта способна и какие данные читать дальше.

Раскладка AIP по битам приведена на рис. 10: перечисленные выше флаги уложены в байт 1, четыре бита байта 2 зарезервированы под бесконтактные расширения (RFU CL, reserved for EMV Contactless Specifications), остальные четыре — RFU. В разобранном примере `AIP = 0x5800` карта поддерживает SDA, CVM и требует управления рисками на терминале [31].

Набор параметров для GPO задаёт сама карта. В ответе на SELECT она объявляет PDOL (Processing Options Data Object List, тег `0x9F38`) — список тегов и их длин, которые терминал должен сложить и передать в поле данных GPO. Например, бесконтактная Visa объявляет PDOL вида

```
0x9F66049F02069F37045F2A029F1A02
```

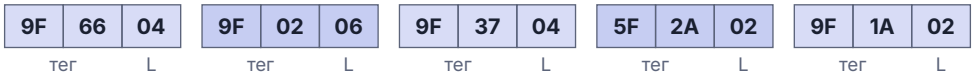
(см. рис. 11) — пять пар `(тег, длина)`: TTQ (Terminal Transaction Qualifiers — возможности и предпочтения бесконтактного терминала), сумма, случайное число, код валюты, код страны терминала. Терминал конкатенирует значения в указанном порядке и оборачивает их в тег `0x83` в теле GPO [31, 55].

Каждый тег здесь занимает 2 байта: у первого байта (`0x9F` или `0x5F`) младшие пять бит равны единице — признак BER-TLV, что номер тега продолжается во втором байте. Длина — 1 байт; на рисунке байт длины выделен более насыщенным оттенком.

Если PDOL у карты нет — так бывает у контактных Mastercard, — GPO отправляется с пустым телом `0x8300`. Реализации POS (Point of Sale, торговый терминал), ожидавшие PDOL у любой карты без исключений, на таких профилях завершали обработку с ошибкой.

BER-TLV в EMV: минимальный парсер

PDOL — усечённая TLV-структура (Tag-Length-Value): в нём нет значений, только пары `(тег, длина)`. Полный BER-TLV (Basic Encoding Rules TLV) — цепочки `(тег, длина, значение)` — встречается в ответах карты на SELECT, READ RECORD и в содержимом DE 55 (Data Element 55 ISO 8583, см. раздел 6.4). EMV использует подмножество ISO/IEC 8825-1 [104]: одно- и двухбайтовые теги, short и long form длины,



Hex	Тег	Len	Запрошенное значение
9F 66 04	0x9F66	4 B	TTQ (Terminal Transaction Qualifiers)
9F 02 06	0x9F02	6 B	сумма (Authorized Amount)
9F 37 04	0x9F37	4 B	непредсказуемое число (Unpredictable Number)
5F 2A 02	0x5F2A	2 B	код валюты (Transaction Currency Code)
9F 1A 02	0x9F1A	2 B	код страны (Terminal Country Code)

Рис. 11 — Побайтовый разбор 15-байтового PDOL бесконтактной Visa: пять пар `(тег, длина)`.

иногда вложенные *constructed*-теги (шаблоны/templates — конструктивные теги BER-TLV, содержащие вложенные TLV; у них бит 6 первого байта тега равен единице — например, FCI Template `0x6F`, File Control Information).

Номер тега формируется так: первый байт описывает объект, где старшие два бита — класс (платёжные теги EMV относятся к *context-specific*), бит 6 уже знаком — примитивный или конструктивный, младшие пять бит несут номер. Когда эти пять бит — все единицы, номер не умещается в одном байте, и тег занимает второй (там бит 8 значит «дальше есть ещё байт»). Поэтому `0x82` (AIP) и `0x94` (AFL) однобайтовые, а `0x9F26` (криптограмма) двухбайтовый. Какой номер что означает, задаёт словарь: платёжные теги — приложение A «Data Elements Dictionary» EMV Book 3 [31], межотраслевые шаблоны вроде `0x6F` — ISO/IEC 7816-4 [102].

Минимальный парсер этого подмножества:

```
from dataclasses import dataclass


@dataclass(frozen=True)
class TLV:
  tag: int
  value: bytes
  children: tuple[TLV, ...] = ()


def parse_tlv(data: bytes) → list[TLV]:
  result: list[TLV] = []
  cursor = 0
  while cursor < len(data):
    # Бит 6 первого байта тега = 1 у constructed-тегов (FCI, шаблоны).
    is_constructed = bool(data[cursor] & 0b0010_0000)
    tag, cursor = _read_tag(data, cursor)
    length, cursor = _read_length(data, cursor)
    if cursor + length > len(data):
      raise ValueError(f"тег {tag:X}: длина {length} больше остатка")
    value = data[cursor : cursor + length]
    cursor += length
    children = tuple(parse_tlv(value)) if is_constructed else ()
    result.append(TLV(tag, value, children))
  return result


def _read_tag(data: bytes, cursor: int) → tuple[int, int]:
  first = data[cursor]
  cursor += 1
  # Тег многобайтовый, если младшие 5 бит первого байта = 11111.
  if first & 0b0001_1111 ≠ 0b0001_1111:
    return first, cursor
  tag = first
  while cursor < len(data):
    b = data[cursor]
```

(продолжение)

```
    cursor += 1
    tag = (tag << 8) | b
    if not b & 0b1000_0000:  # старший бит = 0 в последнем байте тега
      return tag, cursor
  raise ValueError("неожиданный конец потока в многобайтовом теге")


def _read_length(data: bytes, cursor: int) → tuple[int, int]:
  first = data[cursor]
  cursor += 1
  # Short form: старший бит = 0, остальные 7 бит -- сама длина (0..127).
  if not first & 0b1000_0000:
    return first, cursor
  # Long form: первый байт = 0b1000_0000 | N, дальше N байт значения длины.
  n = first & 0b0111_1111
  if n == 0 or cursor + n > len(data):
    raise ValueError("некорректная long-form длина")
  length = int.from_bytes(data[cursor : cursor + n], "big")
  return length, cursor + n
```

7.4 Аутентификация данных

Получив AIP и AFL, терминал знает, какие файлы читать и какой метод аутентификации данных поддерживает карта. Аутентификация подтверждает, что данные, записанные эмитентом при персонализации (раздел 7.11), с тех пор не были подменены. Методы аутентификации данных EMV по возрастанию стойкости: SDA, DDA и CDA [30].

SDA: статическая аутентификация данных

SDA (Static Data Authentication) — базовый метод. При выпуске карты эмитент формирует подпись RSA над статическими данными приложения — записями, которые AFL помечает для офлайн-аутентификации, — и эта подпись записывается на чип. При каждой транзакции терминал считывает подписанные данные и подпись, а затем проверяет цепочку: корневым ключом карточной сети — сертификат эмитента, а открытым ключом эмитента из сертификата (IPK, Issuer Public Key) — подпись данных карты.

SDA подтверждает только, что данные не менялись после персонализации. Подпись статична, и если скопировать все данные с чипа вместе с подписью на другой чип, терминал подмену не заметит — подпись по-прежнему валидна. От клонирования защищают динамические методы, вытеснившие SDA из современных профилей.

DDA: динамическая аутентификация данных

В DDA (Dynamic Data Authentication) карта в дополнение к статической подписи эмитента хранит собственную пару ключей RSA; SDA-профилю такие ключи не нужны, поэтому DDA поддерживают не все карты. Приватный ключ хранится в защищённой памяти чипа, а открытый ключ заверен сертификатом эмитента. Корень цепочки терминал выбирает по паре RID + *CA Public Key Index* (тег `0x9F22`): для каждой карточной сети на терминале хранится свой набор корневых ключей, и индекс указывает, какой именно ключ использовать при проверке сертификата эмитента [105]. При каждой транзакции терминал отправляет карте случайное число (*unpredictable number*, тег `0x9F37`) в составе данных по DDOL (Dynamic Data Authentication Data Object List, тег `0x9F49`) — списку тегов, значения которых карта

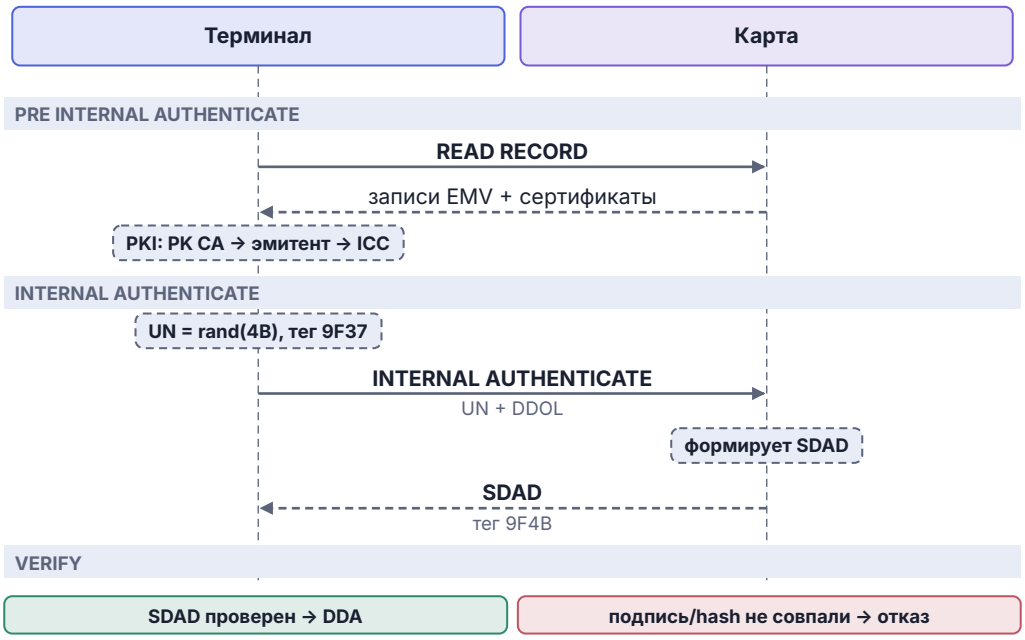


Рис. 12 — Контактный сценарий DDA с командой `INTERNAL AUTHENTICATE`.

ожидает в теле команды `INTERNAL AUTHENTICATE`. В ответ карта формирует *Signed Dynamic Application Data* (SDAD, тег `0x9F4B`) — подпись над Dynamic Application Data, куда входят *ICC Dynamic Number* (тег `0x9F4C`, вырабатываемый чипом для каждой транзакции) и значения тегов из DDOL [106]. Терминал проверяет эту подпись, используя открытый ключ карты из сертификата.

Рисунок 12 отражает контактный профиль с командой `INTERNAL AUTHENTICATE` (APDU-команда EMV для запроса динамической аутентификации карты). Бесконтактные ядра (kernel — реализация EMV-сценария на стороне терминала под конкретную карточную сеть) сжимают этот обмен, каждое по-своему. Kernel 3 (Visa) возвращает SDAD сразу в ответе на `GET PROCESSING OPTIONS`; вариант называется fDDA (fast DDA), отдельных команд `INTERNAL AUTHENTICATE` и `GENERATE AC` в этом сценарии нет [107]. Kernel 2 (Mastercard) совмещает подпись с выработкой финальной криптограммы (*application cryptogram*) в команде `GENERATE AC` — это CDA, следующий подраздел [108].

Скопировать читаемые данные с чипа по-прежнему можно, но приватный ключ используется только внутри криптосопроцессора и не покидает микросхему: копия не подпишет случайное число, которое терминал предъявит в следующей транзакции. Криптографические примитивы RSA разбираются в разделе 10.2 [30].

CDA: комбинированная аутентификация

CDA (Combined DDA / Application Cryptogram Generation) объединяет динамическую аутентификацию данных и генерацию криптограммы в один шаг: карта подписывает своим приватным ключом случайное число терминала и криптограмму транзакции — ARQC (Authorization Request Cryptogram), TC (Transaction Certificate)

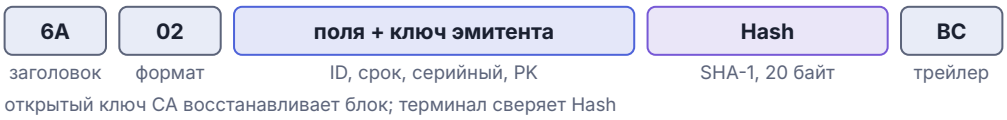


Рис. 13 — Восстановление Issuer Public Key Certificate: маркеры `0x6A` и `0xBC`, хеш внутри.

или AAC (Application Authentication Cryptogram); подробно эти три типа криптограмм разобраны в разделе 7.8. Криптограмма тем самым привязана к конкретному чипу и не может быть подменена при передаче [30].

Уязвимости DDA на стороне терминала

Стойкость DDA зависит от внешнего условия: UN формирует терминал, и формировать его он должен непредсказуемо. В работе «Chip and Skim» (IEEE S&P, 2014) группа из Кембриджа показала, почему это условие нарушалось [109]. Первая причина — реализация: часть обследованных банкоматов и POS, включая машины крупных производителей, формировала UN счётчиком, временной меткой или самописным PRNG (pseudorandom number generator, программный псевдослучайный генератор). Предсказав будущий UN, атакующий заранее запрашивает у карты криптограммы под нужные значения и проигрывает их позже — для эмитента это неотличимо от клонирования. Вторая — протокол: UN генерируется на терминале, а проверяется у эмитента, поэтому вредоносное ПО в POS или MITM (man-in-the-middle, посредник на канале) на участке «терминал — эквайер» подменяет легитимный UN на тот, под который криптограмма у атакующего уже есть. Аппаратный TRNG чипа от этого не спасает: он отвечает за карточную сторону обмена, качество UN карта проверить не может.

Подпись с восстановлением: что внутри сертификата

SDA, DDA и CDA опираются на один примитив — цифровую подпись RSA с восстановлением сообщения по ISO/IEC 9796-2 (EMV Book 2, Annex A2.1) [30]. В этой схеме проверяющий восстанавливает подписанные данные из самой подписи открытым ключом: подпись одновременно служит контейнером данных.

Сертификат — это число; терминал возводит его в степень открытой экспоненты ключа удостоверяющего центра (CA) по модулю ключа и получает восстановленные данные. Первый байт этих данных — `0x6A`, последний — `0xBC`; между ними расположены поля сертификата и хеш (рис. 13). Несовпадение трейлера `0xBC` останавливает восстановление: аутентификация провалена ещё до разбора содержимого.

Внутри Issuer Public Key Certificate терминал находит (табл. 6) формат сертификата, идентификатор эмитента, срок действия, серийный номер, индикаторы алгоритмов, длину и экспоненту открытого ключа эмитента, сам ключ и хеш SHA-1 поверх всего перечисленного. Терминал пересчитывает этот хеш и сверяет с восстановленным; заодно проверяет, что идентификатор эмитента совпадает со старшими цифрами PAN, что сертификат не просрочен и не отозван по списку CRL.

Если открытый ключ эмитента длиннее $N_{CA} - 36$ байт, в сертификате помещается только его старшая часть (Leftmost Digits), а остаток (Issuer Public Key Remainder) карта отдаёт отдельным тегом; терминал склеивает их перед проверкой. Подписанные статические данные SDA дополняются паттерном `0xBB` до длины модуля эмитента —

Таблица 6 — Восстановленные данные Issuer Public Key Certificate [30].

Поле	Длина, байт
Recovered Data Header (`0x6A`)	1
Certificate Format (`0x02`)	1
идентификатор эмитента	4
срок действия сертификата	2
серийный номер сертификата	3
индикатор алгоритма хеширования	1
индикатор алгоритма ключа эмитента	1
длина открытого ключа эмитента	1
длина экспоненты ключа эмитента	1
открытый ключ эмитента (или старшие байты)	$N_{CA} - 36$
Hash Result (SHA-1)	20
Recovered Data Trailer (`0xBC`)	1

тем же байтом-заполнителем, по которому в дампе видно неиспользованное место структуры.

7.5 Верификация держателя

Аутентификация данных подтверждает подлинность карты, но подлинная карта может оказаться в чужих руках — украденная, найденная, забытая на прилавке. Верификация держателя (Cardholder Verification) проверяет, что транзакцию инициирует законный владелец карты.

EMV допускает несколько способов проверки. Список методов верификации держателя — CVM List (Cardholder Verification Method List; CVM — Cardholder Verification Method, метод верификации держателя) — записывает на карту эмитент при персонализации [31]. Порядок выражает его приоритеты: во время транзакции терминал просматривает список сверху вниз, для каждого метода проверяет применимость — есть ли клавиатура для PIN, превышена ли нужная сумма, допускает ли конфигурация подпись или локальную проверку на устройстве — и выбирает первый применимый. Наверх эмитент ставит метод, которому доверяет для данного продукта и региона, ниже — запасные варианты для терминалов без нужных возможностей. Состав списка ограничен правилами карточной сети: в банкоматах, например, обязателен online PIN; остальное определяет политика рисков эмитента.

Основные семейства методов верификации:

- **offline PIN, открытый текст** — держатель вводит PIN на клавиатуре терминала, терминал передаёт его чипу командой VERIFY, и чип сравнивает введённое значение с эталоном, хранящимся в защищённой памяти. PIN никогда не покидает периметр «терминал + чип». Open PIN — исторический вариант, который постепенно выводится из сценариев без участия кассира [55, 110].
- **offline PIN, зашифрованный** — аналогичен открытому, но PIN передаётся чипу в зашифрованном виде с использованием открытого ключа карты, что защищает от перехвата на интерфейсе терминал–чип.
- **online PIN** — PIN вводится на клавиатуре терминала, шифруется в PIN-блок (форматы PIN-блока — в разделе 10.7) и отправляется в авторизационном

Правило	Байт 1 (CVM Code)	Байт 2	Смысл
44 03	след. + код 04	усл. 03	Offline enc. PIN, если терминал поддерживает
42 03	след. + код 02	усл. 03	Online PIN, если терминал поддерживает
1F 00	стоп + код 1F	усл. 00	No CVM, всегда (fallback)

Рис. 14 — Анатомия CVM List `0x8E`: пороги X, Y и три правила с разбором.

сообщении эмитенту через DE 52. Чип в проверке не участвует; верификацию выполняет хост эмитента.

- **подпись** — кассир визуально сверяет подпись на чеке с образцом на обратной стороне карты. Метод устаревший и ненадёжный, но по-прежнему встречается в некоторых конфигурациях.
- **no CVM** — верификация не требуется; обычно это мелкие суммы или определённые категории ТСП, например вендинговые автоматы.
- **проверка на устройстве** — биометрия или пароль на мобильном устройстве вместо PIN на терминале; этот метод применяется при оплате телефоном и подробно разбирается в разделе 8.3.

Как читается CVM List

Список приходит в теге `0x8E` и имеет фиксированную структуру: два четырёхбайтовых порога X и Y в валюте приложения, заданные эмитентом, затем пары байт — Cardholder Verification Rules. Каждое правило — байт CVM Code и байт Condition Code (рис. 14).

В байте CVM Code бит 7 задаёт действие при неуспехе правила: `1` — перейти к следующему правилу, `0` — считать верификацию проваленной и остановиться. Младшие шесть бит — код метода (табл. 7). Байт Condition Code задаёт, когда правило применимо: всегда, только при снятии наличных, только если терминал поддерживает метод, или по сумме относительно X и Y (табл. 8).

Таблица 7 — CVM Code (младшие 6 бит байта 1 правила) [31].

Код	Метод
`000000`	завершить верификацию провалом
`000001`	Offline PIN, открытый текст (проверяет чип)
`000010`	Online PIN (шифруется в PIN-блок)
`000011`	Offline PIN, открытый текст, плюс подпись
`000100`	Offline PIN, зашифрованный (проверяет чип)
`000101`	Offline PIN, зашифрованный, плюс подпись
`011110`	подпись
`011111`	No CVM

Коды `10 xxxx` зарезервированы за платёжными системами, `11 xxxx` — за эмитентом; CDCVM на устройстве (раздел 8.3) кодируется именно в этих диапазонах.

Таблица 8 — Condition Code (байт 2 правила) [31].

Код	Правило применимо
00	всегда
01	снятие наличных в автомате без кассира
02	не наличные и не покупка с выдачей наличных
03	если терминал поддерживает метод
04	снятие наличных через кассира
05	покупка с выдачей наличных
06	в валюте приложения, сумма меньше X
07	в валюте приложения, сумма больше X
08	в валюте приложения, сумма меньше Y
09	в валюте приложения, сумма больше Y

Терминал идёт по правилам сверху вниз (EMV Book 3, §10.5.5) [31]. Для каждого проверяет условие из байта 2; если оно выполнено, пробует метод из байта 1. Успешный метод завершает верификацию. После неуспешного метода терминал смотрит бит 7: единица отправляет к следующему правилу, ноль завершает верификацию провалом. Правило, чьё условие не выполнено, пропускается без попытки.

Пример с рисунка — `44 03 42 03 1F 00`: сначала Offline PIN в зашифрованном виде, если у терминала есть PIN-клавиатура; не прошёл — Online PIN; недоступен и он — No CVM с условием «всегда». Так одна карта обслуживается и на POS с клавиатурой, и на вендинговом автомате без неё.

Если ни один метод из CVM List не применим — например, у терминала нет клавиатуры, а карта требует PIN, — верификация считается неуспешной (флаг «CV not successful»). Соответствующий бит попадает в TVR (Terminal Verification Results) и влияет на решение о типе криптограммы на последнем шаге сценария.

Исход верификации терминал записывает в тег `0x9F34` (CVM Results) — три байта: метод, условие применения, результат. `0x9F34` передаётся в DE 55 вместе с криптограммой. При отказе эмитента 55 (Incorrect PIN) тег — первый объект проверки: если он указывает на подпись или No CVM, дело не в PIN-блоке, а в рассогласовании конфигурации терминала с ожиданиями эмитента.

7.6 TVR и TSI: битовые поля результатов проверок

TVR (Terminal Verification Results) — пятибайтовое поле, в которое терминал записывает результаты проверок перед финальным решением. Оно передаётся в DE 55 под тегом `0x95` [31].

Каждый байт TVR отвечает за свою группу проверок; нумерация идёт от старшего бита к младшему внутри каждого байта (бит 8 — MSB).

Установленная единица для большинства битов означает «шаг не прошёл» или «сработало нештатно»; в логе отказанной транзакции по выставленным битам сразу видна причина отказа. Расшифровка по битам всех пяти байт — в табл. 9; жёлтая ячейка — бит 4 байта 3, установленный в разобранном ниже примере `TVR = 0x0000080000`.

Байт 1 — офлайн-аутентификация данных (ODA, *offline data authentication*, раздел 7.4): выполнялась ли ODA и какой из методов SDA/DDA/CDA не прошёл. **Байт 2** — ограничения обработки на терминале: совпадение версии с конфигурацией, срок

действия, активация, разрешённые услуги, признак «новая карта». **Байт 3** — итог CVM (раздел 7.5): выбранный из CVM List метод, доступность клавиатуры, счётчик попыток PIN, факт ввода PIN. **Байт 4** — управление рисками терминала (раздел 7.7): floor limit, нижний и верхний лимит офлайн-операций, идущих подряд, случайный отбор, принудительный онлайн от ТСП. **Байт 5** — состояние после ARQC и онлайн-ответа эмитента (раздел 7.8): сошёлся ли ARPC, выполнились ли issuer scripts до и после финальной криптограммы, использовался ли TDOL по умолчанию.

Имена флагов в таблице даны в сокращённой форме EMVCo; полные формулировки — в EMV Book 3, Annex C5 [31]. Маски бит 8–1 внутри байта — `0x80`, `0x40`, `0x20`, `0x10`, `0x08`, `0x04`, `0x02`, `0x01`.

Таблица 9 — TVR: расшифровка битов всех пяти байтов; жёлтым — бит 4 байта 3 примера `TVR = 0x0000080000`.

Бит	Б1: ODA	Б2: terminal	Б3: CVM	Б4: risk	Б5: issuer auth
8	ODA not performed	App version mismatch	CV not successful	Floor limit exceeded	Default TDOL used
7	SDA failed	Expired application	Unrecognised CVM	LCOL exceeded	Issuer auth failed
6	ICC data missing	Not yet effective	PIN Try Limit exceeded	UCOL exceeded	Script fail pre-GAC
5	Exception file	Service not allowed	No PIN pad	Random online	Script fail post-GAC
4	DDA failed	New card	PIN not entered	Merchant forced online	—
3	CDA failed	—	Online CVM captured	Biometric Try Limit exceeded	CA ECC key missing
2	SDA selected	Biometric successful	Biometric device not working	Biometric Type not supported	ECC key recovery failed
1	XDA selected	Biometric template not supported	Biometric entry bypassed	XDA signature failed	—

Диагностический разбор примера `TVR = 0x0000080000`: установленный бит 4 байта 3 означает, что карта потребовала PIN при работающей клавиатуре, но держатель нажал «Отмена» или кассир пропустил шаг. В сочетании с IAC Online, требующим онлайн-авторизацию при неуспешной верификации, транзакция отправляется онлайн и получает отказ эмитента `55` (Incorrect PIN) — хотя PIN физически не запрашивался. Готовые онлайн-разборщики EMV-тегов (например, emvdecoder.com [111]) декодируют TVR, AIP, TSI и CVM List на стороне клиента.

TSI: что было выполнено

Парный к TVR тег — TSI (Transaction Status Information, `0x9B`). Это тоже битовые флаги, два байта, но с противоположным смыслом: TVR фиксирует *провалы и факты* проверок («что не прошло»), TSI — *какие проверки выполнялись* в ходе транзакции [31]. Шесть определённых битов расположены в байте 1 (табл. 10); биты 2 и 1 байта 1 и весь байт 2 зарезервированы (RFU). На рис. 15 жёлтым отмечен пример `TSI = 0xE800` — офлайн-транзакция, в которой выполнены ODA, верификация держателя, управление рисками карты и терминала; аутентификация эмитента и обработка issuer scripts не запрашивались, потому что онлайн-обращения не было.

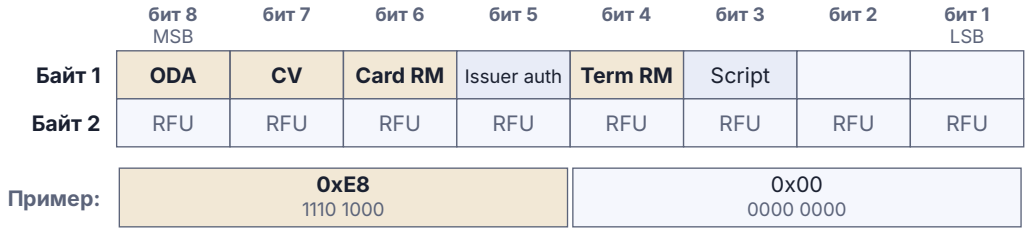


Рис. 15 — Раскладка TSI: 2 байта, MSB слева; жёлтым — биты примера `TSI = 0xE800`.

Таблица 10 — Биты TSI (байт 1) [31].

Бит	Маска	Назначение
8	`0x80`	Offline data authentication was performed
7	`0x40`	Cardholder verification was performed
6	`0x20`	Card risk management was performed
5	`0x10`	Issuer authentication was performed
4	`0x08`	Terminal risk management was performed
3	`0x04`	Script processing was performed

7.7 Управление рисками терминала и карты

После аутентификации данных и верификации держателя решается, одобрить транзакцию офлайн, без обращения к эмитенту, или отправить запрос онлайн. EMV разделяет это решение на два уровня управления рисками — на стороне терминала и на стороне карты. Оба уровня записывают свои результаты в битовое поле TVR, из которого затем складывается итоговое решение [31].

Лимиты терминала оценивают текущую операцию — пороги по сумме и правила случайного отбора; их выставляет эквайер по правилам карточной сети. **Прикладные лимиты карты** учитывают историю самой карты — сколько подряд операций прошло офлайн и на какую общую сумму; их записывает эмитент при персонализации. Для бесконтактного канала действует ещё третий набор — пороги CVM и DRL (Dynamic Reader Limits, динамические лимиты ридера).

Управление рисками терминала

Первый рубеж — **floor limit**, порог автономного одобрения по сумме. Эквайер выставляет его по правилам карточной сети; у сети и эмитента могут быть собственные значения, и терминал применяет минимум. Сумма ниже порога допускает офлайн-одобрение; выше — терминал обязан отправить операцию онлайн и поднимает в TVR флаг «Transaction exceeds floor limit» (байт 4, бит 8). Сегодня у большинства POS-терминалов floor limit равен нулю, и любая операция отправляется эмитенту (об исходах см. раздел 33.2).

Второй рубеж — **случайный отбор**. Эмитент получает часть операций, которые по сумме могли бы пройти офлайн. Ниже порога Threshold Value for Biased Random Selection терминал отправляет онлайн фиксированную долю Target Percentage for Random Selection; между этим порогом и floor limit вероятность линейно растёт

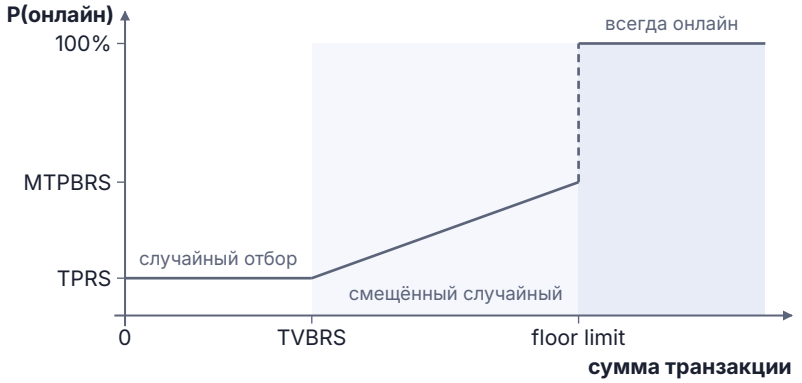


Рис. 16 — Вероятность отправки операции онлайн при случайном отборе.

до Maximum Target Percentage for Biased Random Selection по мере приближения суммы к floor limit (EMV Book 3, §10.6.2; рис. 16) [31].

Третий рубеж — контроль последовательных офлайн-операций по лимитам, записанным в данных карты: **Lower/Upper Consecutive Offline Limit**. Если карта давно не проходила онлайн-авторизацию, терминал больше не вправе одобрять операцию офлайн.

Управление рисками карты

Карта ведёт собственный учёт — счётчик транзакций ATC (Application Transaction Counter, тег `0x9F36`), кумулятивные суммы офлайн-транзакций, количество последовательных офлайн-операций. Текущие значения карта сравнивает с лимитами, установленными эмитентом при персонализации, и при исчерпании лимитов сама запрашивает онлайн-авторизацию или отклоняет операцию — независимо от того, что решил терминал.

TAC и IAC: матрица решений

Результаты всех проверок собираются в TVR. Чтобы превратить набор признаков в исход транзакции, терминал сопоставляет TVR с двумя наборами масок. TAC (Terminal Action Codes) настраивает эквайер — какие сочетания признаков ведут к онлайн-авторизации, отклонению или офлайн-допуску. IAC (Issuer Action Codes) записывает эмитент при персонализации; это его собственная политика на тот же набор ситуаций.

Терминал выполняет побитовое AND между TVR и соответствующими масками TAC/IAC. Ненулевой результат для маски *Denial* ведёт к отклонению и AAC. Ненулевой результат для маски *Online* направляет операцию онлайн и приводит к ARQC. Если ни одно условие не срабатывает, терминал запрашивает офлайн-одобрение — TC; последнее слово при этом остаётся за картой (раздел 7.8). Из-за нулевых офлайн-порогов у современных POS офлайн-ветвь срабатывает редко, но стандарт сохраняет её и отражает флагами TVR.

Сами маски повторяют раскладку TVR — те же пять байт, бит к биту; взведённый бит маски означает «эта проверка критична». Наборов шесть: IAC-Denial, IAC-Online и IAC-Default эмитент записывает на карту при персонализации (теги `0x9F0E`, `0x9F0F` и `0x9F0D`), три парных TAC эквайер настраивает в терминале; маски Default

применяются вместо Online, когда выйти онлайн не получилось [31]. Условный пример: в TVR взведён только флаг «Transaction exceeds floor limit»; в обеих масках Denial этот бит не взведён — офлайн-отказа нет, но эквайер включил его в TAC-Online, и операция уходит онлайн с ARQC.

7.8 Криптограмма: ARQC, TC, AAC

Криптограмма завершает транзакцию EMV. Восьмибайтовое значение, вычисленное чипом по секретному ключу, одновременно фиксирует решение карты и доказывает подлинность чипа. По итогам предыдущих фаз (аутентификации данных, верификации держателя и управления рисками) карта генерирует одну из трёх криптограмм [31].

ARQC (Authorization Request Cryptogram) — криптограмма, с которой карта запрашивает онлайн-авторизацию у эмитента; наиболее распространённый исход контактной транзакции EMV. По настройкам IAC, превышению лимитов или требованию терминала карта определяет, что одобрение офлайн невозможно, и формирует криптограмму для эмитента.

TC (Transaction Certificate) — «карта одобряет транзакцию офлайн». Эмитент в решении не участвует; TC передаётся в клиринг как доказательство, что транзакция была одобрена чипом.

AAC (Application Authentication Cryptogram) — «карта отклоняет транзакцию». Терминал должен остановиться.

В онлайн-сценарии команда `GENERATE AC` (разобрана ниже) выполняется дважды: первым вызовом терминал запрашивает у карты ARQC и отправляет его эмитенту, а после ответа вторым вызовом запрашивает финальную криптограмму — TC при одобрении, AAC при отказе. Выбор между ARQC, TC и AAC сведён в табл. 11.

Тип криптограммы кодируется в теге `0x9F27` — CID (Cryptogram Information Data) [31]. В публичном глоссарии Visa TADG ARQC, TC и AAC описаны как результат обработки данных карты, терминала и транзакции ключом TDEA или AES [55]; детали иерархии ключей и деривации — в разделе 10.4. В авторизационном сообщении криптограмма передаётся внутри DE 55 под тегом `0x9F26`; в том же DE 55 идут CID (`0x9F27`), ATC и IAD — порядок TLV-объектов внутри поля не закреплён, и парсер ищет их по тегам.

Таблица 11 — Принятие решения о типе криптограммы в EMV

Маска TVR ∩ TAC/IAC	Криптограмма	Поведение терминала
Denial $\neq 0$: любой бит маски Denial выставлен	**AAC**	отказ; дальнейшая обработка прекращается
Denial $= 0$, Online $\neq 0$: офлайн-отказ исключён, нужен онлайн	**ARQC**	уход в онлайн для авторизации эмитентом
Denial $= 0$, Online $= 0$: обе маски пусты	**TC**	офлайн-одобрение картой без обращения к эмитенту

Команда GENERATE AC и сборка криптограммы

Криптограмму терминал запрашивает командой `GENERATE AC` (`CLA = 0x80`, `INS = 0xAE`). В P1 закодирован желаемый тип — биты 8–7 (`00` AAC, `01` TC, `10` ARQC),

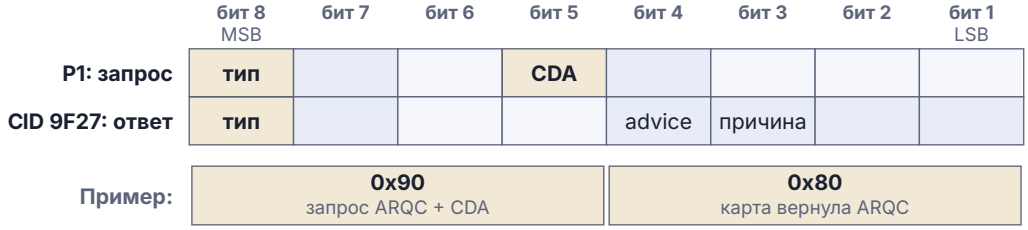


Рис. 17 — GENERATE AC: P1 запроса и CID ответа; жёлтым — биты примера.

а биты 5–4 со значением `10` запрашивают подпись CDA [31]; тело команды — значения по CDOL1 (рис. 17).

CDOL1 (а на втором, завершающем `GENERATE AC` — CDOL2) — это DOL: карта перечисляет в нём теги и длины, а терминал склеивает в том же порядке только *значения*, без тегов (механика DOL та же, что у PDOL, раздел 7.3). В типичный CDOL1 входят сумма, код страны терминала, TVR, код валюты, дата и тип операции, непредсказуемое число; карта знает раскладку и разбирает склейку позиционно. Эту склейку вместе с собственными данными карта прогоняет через MAC на сессионном ключе (раздел 10.4) и получает восьмибайтовую криптограмму. Подмена любого поля под криптограммой без ключа невозможна: MAC изменится.

В ответ карта возвращает криптограмму и CID. Старшие два бита CID — фактически выданный тип, и он может быть слабее запрошенного: терминал просил ARQC, а карта при исчерпанных лимитах вернула AAC. Бит 4 — признак advice, биты 3–1 — код причины: `000` — нет данных, `001` — услуга не разрешена, `010` — лимит попыток PIN исчерпан, `011` — аутентификация эмитента не прошла. По ним эмитент и процессинг видят, почему карта понизила решение.

Офлайн-одобрение карта может дополнительно заверить хешем: по необязательному TDOL терминал строит TC Hash Value (тег `0x98`) — SHA-1 от выбранных полей операции — и передаёт его карте в данных `GENERATE AC`; хеш фиксирует, что именно было одобрено [31].

CVN: какой именно вариант криптограммы

Чтобы хост эмитента воспроизвёл ARQC, ему нужен один параметр сверх данных транзакции — **CVN (Cryptogram Version Number)**. Он передаётся внутри IAD (Issuer Application Data, тег `0x9F10`) и указывает хосту, каким способом карта вывела ключи от мастер-ключа к ключу карты и далее к сессионному ключу (см. раздел 10.4) и какой формат MAC она применила. CVN 10 и 18 на одних и тех же данных карты, ATC, UN и IMK дают разные восьмибайтовые значения, и при расследовании расхождения криптограммы типичная причина — профиль персонализации карты под одну версию, а настройки хоста — под другую.

В семействе Visa VIS чаще других встречаются CVN 10, 18 и 22 [112]:

- **CVN 10** — ключ карты (UDK, Unique Derivation Key) выводится из IMK по PAN и PSN (PAN Sequence Number), и UDK используется как сессионный ключ напрямую, без диверсификации по ATC. MAC считается по CDOL1 (Card Risk Management Data Object List 1; список тегов, которые карта запрашивает у терминала при первом `GENERATE AC`), ARPC формируется методом 1 (8 байт, XOR криптограммы с ARC — Authorization Response Code, кодом ответа эмитента — и шифрование сессионным ключом).

- **CVN 18** — поверх UDK выводится сессионный ключ по ATC, как в разделе 10.4. ARPC формируется методом 2 (4 байта, MAC поверх ARQC и CSU — Card Status Update, инструкций эмитента к карте).
- **CVN 22** — та же схема, что у CVN 18 (деривация CSK на 3DES); отличие — в составе данных, входящих в криптограмму, а не в смене шифра [113]. Переход с 3DES на AES описан в разделе 10.1 и к номеру CVN не привязан.

Mastercard в профиле M/Chip использует собственные значения CVN: у M/Chip 4 и M/Chip Advance это `0x10`, `0x11`, `0x14` и `0x15`, они различаются алгоритмом сессионного ключа и включением счётчиков в данные криптограммы [112]; конкретные параметры криптограммы задают M/Chip Requirements, доступные только участникам сети.

ВАЖНО

«Номер CVN» — это один байт внутри IAD (тег `0x9F10`). Парсеры и логи показывают его шестнадцатерично, спецификации Visa и хосты — десятичным значением: `0x0A` — это CVN 10, `0x11` — CVN 17, `0x12` — CVN 18. Сверяйте систему счисления, иначе один и тот же байт читается как два разных номера. Для CVN 22 соответствие нарушается: сам байт равен `0x22`, его десятичное значение — 34 [112].

ARPC: ответ эмитента

Когда эмитент получает авторизационный запрос с ARQC, он повторяет вычисление на своей стороне: выводит те же ключи и считает криптограмму над данными операции. Совпадение подтверждает, что карта подлинная, а защищённые криптограммой данные карты и терминала не были подменены при передаче [55]. Затем эмитент одобряет или отклоняет операцию и формирует ARPC (Authorization Response Cryptogram) — ответную криптограмму аутентификации эмитента. Карта проверяет ARPC, чтобы убедиться, что ответ получен от легитимного эмитента и не был изменён при передаче [55].

Терминал передаёт ARPC чипу командой `EXTERNAL AUTHENTICATE` либо в данных второго `GENERATE AC` — по CDOL2, куда карта обычно включает и код ответа эмитента (тег `0x8A`). Если ARPC валиден и эмитент одобрил транзакцию, карта формирует финальную криптограмму TC, подтверждая итог. Если ARPC невалиден или эмитент отклонил операцию, карта генерирует AAC.

Сценарии эмитента (*issuer scripting*)

Вместе с ARPC эмитент может отправить чипу сценарии управления (*issuer scripts*). Они передаются в тегах EMV `0x71` (Script Template 1, выполняется до финальной криптограммы) или `0x72` (Script Template 2, выполняется после). Через них эмитент обновляет параметры карты — сбрасывает офлайн-счётчик попыток PIN (`PIN CHANGE/UNBLOCK`), меняет офлайн-лимиты (`PUT DATA`, `UPDATE RECORD`), блокирует приложение или всю карту (`APPLICATION BLOCK`, `CARD BLOCK`). Сценарий доходит до карты в ответе на любую онлайн-транзакцию держателя через любой терминал, и отдельный канал к карте эмитенту не нужен [31]. Подлинность этих команд карта проверяет через Secure Messaging (раздел 10.5).

CVR: результаты глазами карты

TVR фиксирует ход транзакции глазами терминала. Карта ведёт собственный отчёт о том же событии — CVR (Card Verification Results) и отправляет его эмитенту

	бит 8 MSB	бит 7	бит 6	бит 5	бит 4	бит 3	бит 2	бит 1 LSB
1: AC + аутент.	**AC 2-й**		**AC 1-й**		**CDA**	DDA офл	IA нет	IA пров
2: PIN	PTC				**офл PIN**	PIN ×	PTL	онл ×
3: лимиты	ниж N	вер N	ниж S	вер S				
4: сценарий	N сцен				сцен ×	ODA пр	онл сл	!онл
Пример:	**0xA8** 1010 1000		**0x38** 0011 1000		0x00 0000 0000		0x00 0000 0000	

Рис. 18 — CVR Format A: четыре значащих байта; жёлтым — поля примера `0xA8 38 00 00`.

внутри IAD (тег `0x9F10`) рядом с CVN. TVR показывает, что увидел терминал; CVR — что решила карта. При онлайн-авторизации эмитент читает оба: расхождение между ними указывает на подмену данных на участке терминал—эмитент или рассогласование профилей персонализации и хоста.

Раскладка CVR проприетарна для каждого приложения: VSDC, M/Chip и CPA укладывают результаты в разные форматы IAD, и их побитовые схемы доступны участникам сетей. Публично описан CVR Format A из Common Core Definitions (EMV Book 3, Part V), на котором строятся CCD-совместимые приложения [31]. Варианты VSDC и M/Chip кодируют те же по смыслу поля иначе. Format A занимает пять байт; четыре несут смысл, пятый зарезервирован.

Байт 1 кодирует решение карты и способ подтверждения. Старший нибл содержит тип криптограммы, выданной во втором и первом `GENERATE AC`, по два бита на команду; младший нибл — выполнялась ли CDA и прошла ли аутентификация эмитента. Коды первой команды совпадают с CID: 00 — AAC, 01 — TC, 10 — ARQC, 11 — RFU; у второй код 10 означает, что второй `GENERATE AC` не запрашивался. Байт 2 несёт остаток счётчика попыток PIN (PTC, PIN Try Counter) и результат офлайн-проверки PIN. Байт 3 — какие из четырёх офлайн-лимитов карты превышены (число и сумма офлайн-операций, нижний и верхний порог). Байт 4 — сколько команд сценария эмитента с Secure Messaging карта успешно обработала и не провалилась ли обработка.

Разобранный пример `CVR = 0xA8 38 00 00`: первый `GENERATE AC` вернул ARQC (байт 1, биты 6–5 `=10`), второй ещё не запрашивался (биты 8–7 `=10`), карта выполнила CDA (байт 1, бит 4), офлайн-проверка PIN прошла (байт 2, бит 4), в счётчике осталось три попытки (байт 2, биты 8–5 `=0011`), ни один офлайн-лимит не превышен. Эмитент видит успешную онлайн-операцию по подлинному чипу с локально проверенным держателем.

CVR дополняет авторизационный запрос: криптограмма доказывает подлинность чипа, ATC отсекает повтор, CVN задаёт способ деривации ключей, CVR сообщает решение и условия карты. Со стороны терминала те же факты описывают TVR и TSI.

CIAC и CSU: решение карты и ответ эмитента

Терминал сводит TVR с масками TAC и IAC; карта выполняет собственную проверку. Свой CVR она сопоставляет с тремя Card Issuer Action Codes — CIAC-Default,

Таблица 12 — CVR Format A: поля по байтам и битам [31].

Байт	Биты	Поле
1	8–7	тип AC во 2-м GENERATE AC: 00 AAC, 01 TC, 10 2-й не запрашивался
1	6–5	тип AC в 1-м GENERATE AC: 00 AAC, 01 TC, 10 ARQC
1	4	выполнена CDA
1	3	выполнена офлайн-DDA
1	2	аутентификация эмитента не выполнялась
1	1	аутентификация эмитента провалилась
2	8–5	остаток счётчика попыток PIN (PTC)
2	4	офлайн-проверка PIN выполнялась
2	3	офлайн-проверка PIN выполнялась и не сошлась
2	2	лимит попыток PIN исчерпан
2	1	последняя онлайн-операция не завершена
3	8	превышен нижний лимит числа офлайн-операций
3	7	превышен верхний лимит числа офлайн-операций
3	6	превышен нижний лимит суммы офлайн-операций
3	5	превышен верхний лимит суммы офлайн-операций
4	8–5	число успешно обработанных команд сценария с Secure Messaging
4	4	обработка сценария эмитента провалилась
4	3	ODA провалилась на прошлой операции
4	2	установлен признак «онлайн в следующий раз»
4	1	не удалось выйти онлайн

CIAC-Decline, CIAC-Online — и по совпадению битов решает, понизить ли криптограмму до AAC или потребовать онлайн, независимо от решения терминала. Так работает второй контроль: даже когда терминал готов одобрить офлайн, карта по своим CIAC может потребовать онлайн. CCD и CPA задают CIAC публично; M/Chip использует собственные коды.

В онлайн-ответе эмитент возвращает ARPC и может передать CSU (Card Status Update) — четыре байта инструкций карте внутри Issuer Authentication Data (тег 0x91, рис. 19).

Рис. 19 — CSU: байт 2 действий эмитента; жёлтым — биты примера 0x00 82 00 00.

Байт действий кодирует, одобрил ли эмитент операцию и что изменить в карте: заблокировать карту или приложение, обновить счётчик попыток PIN (новое

значение — в нибле байта 1), выставить признак «онлайн в следующий раз». Двухбитное поле *update counters* управляет офлайн-накопителями: `00` — оставить без изменений, `01` — выставить по верхним лимитам (UCOL по числу, UCOTA по сумме), `10` — обнулить, `11` — добавить операцию. Так эмитент управляет картой прямо в онлайн-ответе, обходясь без сценарных команд вроде `PIN CHANGE/UNBLOCK` и `CARD BLOCK`; команды, которых нет в CSU, эмитент передаёт сценариями.

Чтение DE 55 по логу

Терминал ведёт транзакцию последовательностью APDU; на хост эмитента её итог приходит одним полем ISO 8583 — DE 55. Таблица связывает команды с диагностическими данными в ответе карты:

Таблица 13 — APDU-цепочка контактной транзакции и ответы карты.

Команда	CLA INS	Что несёт ответ
`SELECT`	`00 A4`	FCI выбранного приложения, PDOL
`GET PROCESSING OPTIONS`	`80 A8`	AIP и AFL: профиль и карта файлов
`READ RECORD`	`00 B2`	записи по AFL: данные карты и сертификаты
`GENERATE AC`	`80 AE`	криптограмма и CID; P1 задаёт запрошенный тип

DE 55 содержит конкатенацию BER-TLV. Ниже поле, собранное из стандартных тегов EMV Book 3; TVR в нём взят из разбора выше [31]:

```
DE55 = bytes.fromhex(
  "82023D00"  # AIP 0x3D00: DDA, CDA, проверка держателя, риск-менеджмент, аутентификация эмитента
  "9505000080000"  # TVR = 0x0000080000 (пример из раздела про TVR)
  "9B02E800"  # TSI -- какие функции терминал выполнил
  "9A03260529"  # дата транзакции (YYMMDD) 2026-05-29
  "9C0100"  # тип транзакции -- покупка
  "9F0206000000010000"  # сумма авторизации 100.00
  "9F0306000000000000"  # Amount, Other -- наличные на кассе (cash-out); здесь 0.00; в CDOL1, в криптограмме
  "5F2A020840"  # код валюты 840 (USD)
  "9F1A020840"  # код страны терминала 840 (US)
  "9F3704A1B2C3D4"  # непредсказуемое число (UN)
  "9F350122"  # тип терминала (attended, online+offline, merchant)
  "9F3602007C"  # ATC   счётчик транзакций = 124
  "9F100706011203A48000"  # IAD   данные приложения эмитента (DKI, CVN, CVR)
  "9F260843C11460F9146400"  # ARQC -- настоящий, посчитан в emv_keys.py над полями ниже
  "9F270180"  # CID   тип криптограммы -- ARQC
  "9F34031F0002"  # результаты CVM
)
```

Тот же минимальный парсер разворачивает поле в дерево (`тег, длина, значение`):

```
# Короткие имена тегов DE 55 (EMV Book 3, раскладка тегов).
TAGS = {
  0x82: "AIP   профиль приложения",
  0x95: "TVR   результаты проверок терминала",
  0x9B: "TSI   статус транзакции",
  0x9A: "дата транзакции",
  0x9C: "тип транзакции",
```

(продолжение)

```
    0x9F02: "сумма авторизации",
    0x9F03: "сумма прочая: наличные на кассе",
    0x5F2A: "код валюты",
    0x9F1A: "код страны терминала",
    0x9F37: "непредсказуемое число (UN)",
    0x9F35: "тип терминала",
    0x9F36: "ATC   счётчик транзакций",
    0x9F10: "IAD   данные приложения эмитента",
    0x9F26: "криптограмма (ARQC/TC/AAC)",
    0x9F27: "CID   тип криптограммы",
    0x9F34: "результаты CVM",
}

def decode(field55: bytes) → list[tuple[str, str, str]]:
    """DE 55 → строки (тег, значение hex, имя) для разбора по логу."""
    return [
        (f"{t.tag:02X}", t.value.hex().upper(), TAGS.get(t.tag, ""))
        for t in parse_tlv(field55)
    ]

if __name__ == "__main__":
    for tag, value, name in decode(DE55):
        print(f"{tag:<6}{value:<18}{name}")
```

При разборе инцидента несколько тегов сразу указывают на место диагностики. `0x95` — TVR: значение `0x00 00 08 00 00` из примера означает, что карта потребовала PIN, держатель отказал, и операция получила отказ 55 (раздел 7.6). `0x9F10` — IAD: внутри него CVN и CVR; рассогласование криптограммы между профилем карты под CVN 10 и настройкой хоста под CVN 18 часто приводит к отказу; чтение CVR — в разделе 7.8. `0x9F26` — криптограмма: в примере это ARQC, посчитанный над полями этой транзакции в разделе 10.4. `0x9F36` — ATC, защита от повтора; `0x9F27` — CID с фактически выданным типом. Если `POS Entry Mode` в DE 22 указывает на возврат к магнитной полосе, причину ищут в разделе 7.9. Веб-разборщики тегов вроде `emvdecoder.com` делают тот же разбор в браузере [111].

7.9 Возврат к магнитной полосе (fallback)

Не каждая чиповая транзакция завершается на чипе. Контакт между терминалом и площадкой бывает нестабилен (карта изношена, загрязнена, терминал повреждён), приложение на чипе не отвечает, обмен APDU прерывается на полпути. В таких случаях терминал выполняет *fallback* — переключается на считывание магнитной полосы и проводит транзакцию как обычную операцию по полосе [32].

Fallback бывает технический и обходной. При техническом терминал не смог прочитать чип и после нескольких неудачных попыток сам перешёл на магнитную полосу. Авторизационное сообщение несёт специальное значение POS Entry Mode в DE 22, и эмитент получает признак: чип не прочитался, операция проводится по полосе. При обходном инициатива на стороне ТСП — кассир проводит карту через магнитный считыватель, минуя чип. Причиной бывает спешка, неисправный терминал или злонамеренное поведение; именно этот сценарий карточные сети ограничивают жёстче всего.

Fallback возвращает транзакцию к статическим данным магнитной полосы вместо динамической криптограммы чипа. Карточные сети рассматривают его как исключение — он повышает уровень риска и может перераспределять ответственность. По Visa TADG транзакции с *fallback* должны авторизовываться онлайн, и порог офлайн-авторизации к ним не применяется [55]. Пороги мониторинга, штрафы

Таблица 14 — Известные атаки на чиповую и бесконтактную транзакцию и их статус.

Вектор	Что закрывает	Статус
Клон магнитной полосы	EMV-чип, динамическая криптограмма	закрыт на чипе, остался в *fallback*
Клон по статической SDA	DDA/CDA (раздел 7.4)	вытеснен
Pre-play: предсказуемый или подменённый UN	непредсказуемый UN и его контроль на эмитенте (раздел 7.4)	остаточный риск
Шимминг, *EMV-bypass cloning*	проверка iCVV (раздел 4.3)	закрыт при корректной проверке
Fallback-фрод	онлайн-авторизация и мониторинг сетей (раздел 7.9)	ограничен правилами
Relay (бесконтакт)	*distance bounding*/RRP (раздел 8.5)	редок, защита дорогая

и конкретные условия правил привязаны к каждой карточной сети и разбираются в главах 14 и 15.

Дополнительным рубежом защиты в сценарии *fallback* остаётся iCVV (см. раздел 4.3). Он отсекает попытку выдать скопированные с чипа данные за магнитную полосу; обычный скимминг самой полосы закрывают отказ от полосы и сетевые правила. Конечная цель миграции на EMV — полный отказ от магнитной полосы [13].

Шимминг и *EMV-bypass cloning*

Скиммингу магнитной полосы родственна атака на сам чип — *шимминг* (shimming): тонкий *шиммер* в слоте между чипом и ридером считывает обмен. Такой перехват не позволяет клонировать чип: динамическую криптограмму не предсказать, но снятые с чипа данные эквивалента полосы (Track 2 Equivalent) злоумышленник выдаёт за магнитную полосу (*EMV-bypass cloning*). Подмену блокирует iCVV: на чипе и на полосе значения отличаются (табл. 2), и эмитент сверяет код с типом ввода. Атака работает лишь там, где эмитент iCVV не проверяет [114].

Векторы атаки на чиповый поток

Скоринг, правила и мониторинг фрода разобраны в гл. 29; здесь протокольная сторона: что именно ломает каждый вектор и какая защита ему противостоит сегодня.

7.10 Скорость обмена: EFA и Fast/Quick Chip

Заметная пауза на кассе при оплате контактным чипом складывается из длины последовательности APDU к карте и накладных расходов протоколов T=0/T=1.

Кроме APDU, ряд протоколов между POS и ПЦ эквайера требует второй сессии связи после онлайн-ответа эмитента. EMVCo описывает её как *online completion*, или `second GENERATE AC`: после ARPC терминал повторно вызывает `GENERATE AC`,

и карта генерирует финальную криптограмму TC или AAC. В процессорной практике за этим шагом закрепилось индустриальное название EMV Final Advice (EFA), и обычно он передаётся в ISO 8583 как пара MTI 0220 (advice от терминала) и 0230 (ответ хоста). В этом обмене терминал передаёт на хост результат обработки картой ARPC, финальную криптограмму TC или AAC и данные, нужные для формирования клиринговой записи [32]. POS дважды открывает соединение: сначала чтобы получить ответ эмитента, затем чтобы сообщить итог транзакции.

Чтобы сократить задержку, карточные сети выпустили облегчённые сценарии под общим именем «Fast» или «Quick»: Mastercard M/Chip Fast, Visa Quick Chip, AmEx Quick Chip. Общий принцип — завершить взаимодействие с картой сразу после первого GENERATE AC, не дожидаясь ответа эмитента и не запрашивая вторую криптограмму. Карта возвращает либо TC, либо ARQC; авторизационный обмен с ПЦ становится опциональным и асинхронным относительно держателя, который завершил оплату [46, 55].

В России Fast/Quick Chip не получил широкого внедрения: задержку при оплате сокращал бесконтактный приём. Эмиссия PayPass и payWave началась в 2010–2011 годах (Московский индустриальный банк стал первым в России эмитентом карт PayPass в 2010 [115], Альфа-банк и Visa начали выпуск первых в России карт payWave в 2011 [116]); первый в России массовый приём бесконтакта в транспорте запустил Петербургский метрополитен 27 января 2015 года — один турникет на каждой из 72 станций. Московский метрополитен прошёл тот же путь позже: первый турникет на станции «Котельники» в сентябре 2015 года, около десятка станций к концу пилота в феврале 2016, 20 станций к июлю 2016 и массовое внедрение в течение 2016 года [117—119].

Отдельная сертификация POS-парка под Quick Chip к этому времени уже не давала заметного выигрыша. Visa описывает Quick Chip как сценарий только онлайн (*online-only*) с подмножеством проверок ADVT (Acquirer Device Validation Toolkit), но обновление прошивок и повторная сертификация POS всё равно требовались [120]. Эмиссия бесконтактных карт Мир стартовала в 2017 году (Сбербанк — 22 сентября 2017 [121]), и к 2017–2018 годам НСПК закрепила бесконтактную эмиссию в собственном EMV-апплете карты MPA (Mir Payment Application; подробнее — в разделе 8.2). Для сравнения: тест UL Solutions 2016 на американских POS давал среднее время контактной EMV-транзакции около 11 секунд с разбросом от 4,4 до 22,6 секунды [122]. Бесконтактная транзакция на стороне карты укладывается в доли секунды: обмен по ISO 14443 после прикладывания обычно занимает менее 500 мс, часто 50–250 мс на современных картах и кошельках — быстрее, чем Fast/Quick Chip даёт в контактном сценарии. В России бесконтакт полностью заменил Fast/Quick Chip в приёме; в США Quick Chip по-прежнему используется из-за поздней EMV-миграции 2015 года и парка терминалов, работающих только онлайн. Устройство бесконтактного канала разбирается в гл. 8.

7.11 Персонализация и выпуск карты

Карта проводит транзакцию только после персонализации. С завода чип несёт операционную систему и незаполненный платёжный апплет; всё, чем карта подтверждает себя в операции — PAN, сертификаты эмитента и карты, ключ карты, счётчики, CVM List, коды действий, — эмитент загружает при выпуске.

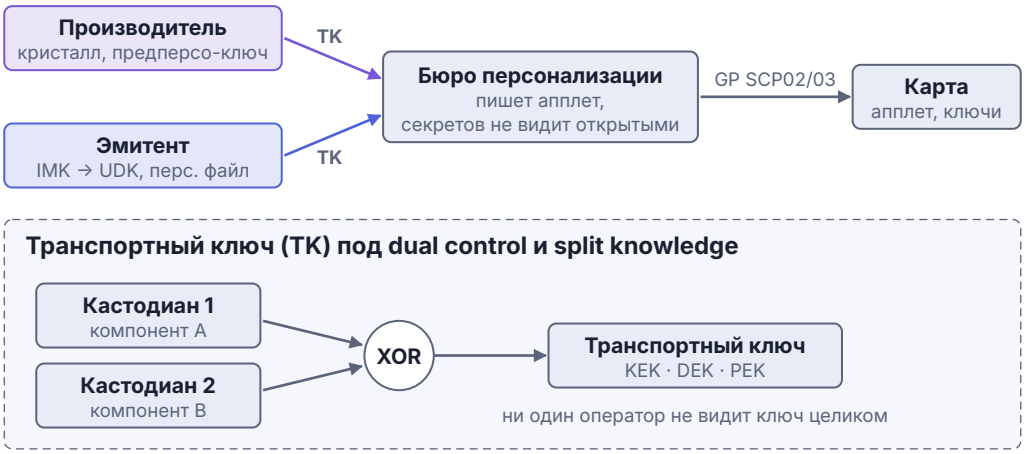


Рис. 20 — Межзональный обмен ключевым материалом под транспортным ключом, который собирают из компонентов под *dual control* и *split knowledge*.

Жизненный цикл чипа фиксирует CPLC (Card Production Life Cycle, тег `0x9F7F`, 42 байта): производство микросхемы, предперсонализация, персонализация, использование, блокировка. CPLC хранит производственную историю — изготовителя кристалла и даты этапов — и читается командой GET DATA для диагностики и учёта.

Данные для каждой карты готовит система подготовки данных эмитента. Она собирает файл персонализации: реквизиты (PAN, срок, Track 2 Equivalent), сертификаты EMV (раздел 7.4), ключ карты UDK из мастер-ключа IMK (раздел 10.4), CVM List, IAC, CDOL. Секреты в файле зашифрованы под транспортным ключом, чтобы бюро персонализации (площадка, которая физически персонализирует чипы, — своя у эмитента или внешний сертифицированный вендор) не видело их открытыми.

Бюро записывает файл в чип по защищённому каналу GlobalPlatform (SCP02/SCP03, раздел 7.2): апплет получает свои записи, разложенные по группам данных. Интерфейс между подготовкой данных и бюро стандартизует EMV Card Personalisation Specification [123]; загрузку и управление апплетом задаёт GlobalPlatform [95].

Ключи карты загружаются в чип иначе, чем ключи в терминал. UDK выводится из IMK эмитента и записывается при персонализации под транспортным ключом; терминальные ключи доставляет RKI или ручная загрузка (раздел 10.8). Транспортные ключи (Transport Key, ТК; рис. 20), которыми эмитент, бюро и производитель обмениваются ключевым материалом, по назначению делятся на ключи шифрования ключей, данных и ПИН-блоков (KEK, DEK, PEK) [123]. Сам транспортный ключ передаётся под *dual control* и *split knowledge*: его собирают из компонентов, и ни один оператор не видит ключ целиком [66]. Ошибка здесь дороже всего: скомпрометированный транспортный ключ открывает ключи всей партии карт.

Персонализация карт Мир следует той же модели — подготовка данных, бюро, загрузка по GlobalPlatform, — но на криптографии ГОСТ и по требованиям НСПК; детали профиля закрыты и доступны участникам (гл. 16).

8 Бесконтактные платежи

Карта, телефон и кольцо предъявляются к терминалу одним жестом и используют один радиоинтерфейс, но устройства, ключи и проверка держателя у них разные.

8.1 NFC и ISO 14443

Бесконтактная карта обменивается данными с терминалом через NFC (Near Field Communication). Это радиоинтерфейс ближнего поля на частоте 13,56 МГц, рассчитанный на короткую дистанцию. Физический и канальный уровни такого обмена определяет стандарт ISO 14443, который задаёт типы карт, антиколлизию (процедуру опознания одной карты, когда в поле сразу несколько) и транспортный уровень, поверх которого работает платёжное приложение [124—127].

ISO 14443 определяет два типа инициализации, Type A и Type B. Type A использует модуляцию ASK 100% (Amplitude-Shift Keying, амплитудная манипуляция) и модифицированное кодирование Миллера при передаче от терминала к карте, а Type B использует ASK 10% и кодирование NRZ (Non-Return-to-Zero, без возврата к нулю). Большинство платёжных карт работают по Type A, но терминал для сертификации EMVCo Level 1 (уровень радио- и низкоуровневого протокола; Level 2 — ядро, Level 3 — приложение) обязан поддерживать оба типа [125, 128].

Рис. 21 — Стек протоколов бесконтактного платежа и анатомия APDU-команд.

У бесконтактной карты нет собственного источника питания. Поле, которое создаёт антенна терминала, наводит ток в антенне карты, и этого тока достаточно, чтобы запустить чип и выполнить криптографические операции. По той же причине бесконтактный платёж возможен в кольце, брелоке или стикере, где антенна и чип внутри, а энергию даёт поле терминала.

Антенна терминала должна создавать поле достаточной силы в рабочей зоне до 4 см от поверхности. Металлический корпус, расположение антенны внутри устройства и толщина защитного стекла влияют на стабильность связи. Если карта получает недостаточно энергии, чип может не успеть завершить криптографическую операцию до выхода из поля, и транзакция сорвётся. ISO 14443-4 задаёт Frame Waiting Time (FWT) — время, в которое карта обязана начать ответ на команду; значение от 300 мкс до 5 с объявляет сама карта при активации. FWT ограничивает ожидание терминала и от срыва из-за недостатка энергии не защищает [127, 129].

8.2 Бесконтактный EMV: протокол и ядра

Бесконтактная транзакция EMV сокращает контактную схему до короткого обмена, чтобы терминал успел завершить его, пока карта в поле [128].

Поверх транспортного уровня T=CL (contactless transport protocol) по ISO 14443-4 работает APDU-уровень (Application Protocol Data Unit) ISO/IEC 7816-4, по которому передаются команды SELECT, GPO и другие сообщения платёжного приложения (см. раздел 7.3) [102].

Бесконтактный выбор приложения начинается с команды SELECT к PPSE `2PAY.SYS.DDF01`, бесконтактному аналогу PSE из контактной транзакции. На уровне байтов команда выглядит как `0x00 A4 04 00 0E 32 50 41 59 2E 53 59 53 2E 44 44 46 30 31 00`: CLA, INS, P1/P2, длина и ASCII-строка имени PPSE. PPSE возвращает список AID; терминал выбирает подходящее приложение, отправляет GET PROCESSING OPTIONS (GPO), получает AIP и AFL и считывает только нужные записи. После чтения записей карта формирует криптограмму по команде GENERATE AC: байт P1 задаёт тип запрашиваемой криптограммы — AAC, TC или ARQC, а бит b5 (маска `0x10`) запрашивает подпись CDA [128].

Ниже порога CVM limit (Cardholder Verification Method limit) сеть разрешает операцию без проверки держателя, а выше запрашивает PIN, биометрию или иной метод [55].

Концепция ядра (*kernel*)

EMVCo определяет несколько ядер бесконтактного протокола. У каждой сети свой набор правил аутентификации, допустимых сценариев и логики офлайн-одобрения, и EMVCo приводит эти различия к общему интерфейсу: команды обмена с картой одинаковы, а правила обработки остаются на стороне каждой сети [128].

После выбора приложения терминал сопоставляет AID с ядром этой сети и передаёт управление соответствующей реализации. Поддержка новой сети требует отдельного ядра, набора тестов и проверки совместимости. Исторически каждое ядро публиковалось в отдельной Book C-x, а в 2022 году EMVCo выпустила *Contactless Kernel Specification* (Book C-8) — общее ядро для всех сетей, которое сосуществует с унаследованными ядрами и лицензируется на тех же безвозмездных условиях, что и контактная спецификация EMV [130]. Visa, Mastercard и Мир используют разные наборы бесконтактных правил для терминала, и детали сертификации разбираются в главах 14, 15 и 16.

PPSE возвращает в FCI список Directory Entry (тег 61); каждая запись содержит ADF Name (4F), Application Label (50) и Application Priority Indicator (87). Combination Selection сопоставляет список AID карты со списком AID терминала и выбирает запись с меньшим значением Priority. На карте Мир–Maestro, которую ВТБ эмитирует с 2019 года [131], терминал в России выбирает приложение Мир с Priority 01. Ядро определяется по RID — первым пяти байтам AID по ISO/IEC 7816-5 [132]; нумерация ядер закреплена в EMVCo Book C, где Kernel 3 — VCPS Visa, а Kernel 2 — M/Chip Mastercard. Сроки действия приложения (теги 5F24/5F25) проверяются позже, после SELECT AID и GPO, на этапе Processing Restrictions, и отражаются в байте 2 TVR (табл. 9).

Таблица 15 — Маршрутизация AID к бесконтактному ядру (Мир–Maestro)

AID (RID)	Priority (87)	Ядро
A0 00 00 06 58 МРА Мир	**01**	**Mir kernel** НСПК
A0 00 00 00 04 Maestro	**02**	**Kernel 2** M/Chip
A0 00 00 00 03 Visa	—	**Kernel 3** qVSDC

Зелёная строка — выбранное приложение с меньшим Priority; строка Visa без Priority приведена для сравнения.

qVSDC (Visa)

qVSDC (quick Visa Smart Debit/Credit) — бесконтактное ядро Visa. В контактном EMV аутентификация и формирование криптограммы разделены, а в qVSDC они сближены, чтобы карта успевала ответить, пока находится в поле [13].

qVSDC поддерживают и карта, и ридер: это контактная EMV-транзакция, сжатая до минимума команд [66], а Quick Contactless — отдельная конфигурация терминала. Для Quick Contactless Visa прямо требует только онлайн-одобрение, но для программы Visa Easy Payment Service (VEPS) публичное руководство допускает как онлайн-, так и офлайн-одобрение. Типовой исход qVSDC — короткая онлайн-проверка; ридер с офлайн-приёмом обязан поддерживать fDDA и может одобрить операцию без обращения к эмитенту [66], а конкретный исход зависит от параметров терминала и правил рынка [55, 120].

M/Chip Contactless (Mastercard)

Бесконтактное ядро Mastercard поддерживает динамическую аутентификацию и офлайн-одобрение при подходящих параметрах риска: если сумма ниже *floor limit* терминала, карта может вернуть TC, и операция одобряется локально, без немедленного обращения к хосту [108].

Офлайн-одобрение работает на транспорте, парковках и при малых покупках, где связь нестабильна или важна минимальная задержка. Выше пороговой суммы или при иных условиях риска терминал запрашивает онлайн-проверку.

Мир бесконтактный

Бесконтактный профиль Мира — EMV-апплет МРА на стороне карты (MIR Payment Application; об устройстве апплета и среды Java Card / GlobalPlatform — в разделе 7.2). МРА реализует стандартные EMV-механизмы — DDA/CDA, взаимную онлайн-аутентификацию с эмитентом, вывод сессионных ключей по EMV CSK [133]; в профиле EMV-сертификатов открытых ключей платёжных систем национальная криптография задана через ГОСТ Р 34.10-2012 [134]. Радиоинтерфейс тот же, что у Visa и Mastercard; различия — в криптографии и правилах сети. Детали МРА, маршрутизации и кобейджа разобраны в гл. 16.

В таблице 16 используются аббревиатуры из гл. 7: fDDA (fast Dynamic Data Authentication, ускоренная динамическая аутентификация, см. раздел 7.4), CVC3

Таблица 16 — Сравнение основных бесконтактных ядер.

Параметр	qVSDC (Visa)	M/Chip Contactless (MC)	Мир бесконтактный
Аутентификация данных	fDDA	CVC3 или ARQC	ГОСТ 34.10
Тип криптограммы	ARQC	CVC3 или ARQC	ARQC (ГОСТ)
Офлайн-одобрение	нет (предпочтительно; офлайн возможен при fDDA)	да (ограниченно)	да
CVM limit	задаётся сетью по рынку	задаётся сетью по рынку	по правилам НСПК
Криптография	RSA + 3DES (AES)	RSA + 3DES (AES)	криптография ГОСТ в сочетании с AES

(Card Verification Code 3, динамический код бесконтактного апплета Mastercard), ARQC (Authorization Request Cryptogram, криптограмма авторизационного запроса, см. раздел 7.8); ГОСТ 34.10 — российский стандарт ЭЦП на эллиптических кривых; 3DES и AES — симметричные шифры (см. гл. 10).

ВАЖНО

CVC3 и ARQC в таблице разделены по способу бесконтактного приёма, а не по исходу «онлайн или офлайн», вопреки расхожим мнениям. В *mag-stripe mode*, где ядро эмулирует магнитную полосу для устаревших терминалов, ридер запрашивает у карты динамический CVC3 командой Compute Cryptographic Checksum; в *EMV mode* команда Generate AC возвращает ARQC, TC или AAC. CVC3 и ARQC эмитент проверяет онлайн. Выбор между онлайн и офлайн происходит внутри *EMV mode*: карта возвращает ARQC, TC или AAC (см. раздел 7.8), а CVC3 в этом выборе не участвует.

Порог CVM limit задаётся сетью и регулятором по каждому рынку отдельно. Во Франции и Германии он равен 50 EUR, в Австралии — от 100 до 200 AUD в зависимости от эмитента [135, 136], в Канаде — 250 CAD. В Великобритании с марта 2026 года FCA отменил фиксированный потолок 100 GBP, и порог теперь устанавливают сами банки по собственным моделям риска [13, 15, 137]. У продавца с высоким средним чеком (ювелирные товары, электроника) покупка чаще превышает порог и требует PIN; в общепите и на транспорте чек чаще укладывается в лимит.

В марте 2022 года Visa и Mastercard приостановили работу в России: карты российских банков этих сетей работают внутри страны до истечения срока действия, операции по ним обрабатывает НСПК [138]. Бесконтактные пороги по картам «Мир» устанавливает ПС Мир [75]. Числовые значения порогов приводятся в Стандартах Системы, вне публичной части Правил. Модель Offline Операции в ПС Мир опциональна: Правила допускают её только для карт с микропроцессором, для которых эмитент установил Offline-лимит [75]. Без такого лимита бесконтактная операция по умолчанию уходит на авторизацию эмитенту в реальном времени.

Динамические лимиты ридера (DRL)

Спецификации AmEx, а до августа 2025 года и Visa, позволяют ридеру хранить на один AID несколько наборов бесконтактных лимитов — по разным регионам эмиссии или иным признакам карты. Механизм называется Dynamic Reader Limit (DRL). У Visa профиль лимитов выбирался по APID (Application Program Identifier, идентификатор прикладной программы, тег `0x9F5A`), который карта отдаёт в ответе на SELECT: байты APID кодируют регион программы и код страны/валюты. У AmEx

для этого служит тег `0x9F70` с предзаписанными на карте наборами DRL. DRL включают там, где доли локальных и международных карт резко различаются: в банкоматах, магазинах в аэропортах и гостиницах. В TADG 3.3 (август 2025) Visa исключила DRL из требований к терминалам [55].

8.3 Мобильные платежи: SE, HCE и выпуск DPAN

В карте и кольце ключи хранятся внутри защищённого чипа и не покидают его. Телефон — устройство общего назначения, и мобильный платёж выстраивают на нескольких архитектурах доверия. В классическом кошельке используются защищённый элемент (Secure Element, SE) и эмуляция карты на стороне хоста (Host Card Emulation, HCE). Отдельный сценарий строится вокруг банковского приложения, которое само участвует в ближнем взаимодействии с терминалом через Bluetooth Low Energy, BLE [139, 140]. Эти сценарии различаются местом хранения ключевого материала и способом получения права действовать от имени карты.

Кошельки на SE и HCE строятся вокруг токена. Чтобы добавить карту в кошелёк, держатель вводит её данные в приложении, кошелёк передаёт их в токен-сервис карточной сети (TSP, Token Service Provider; подробнее — раздел 9.5), который обращается к эмитенту за подтверждением личности держателя, а эмитент при необходимости добавляет собственный шаг проверки — одноразовый код, push-подтверждение или иной механизм.

После одобрения TSP выпускает DPAN (Device PAN), привязанный к устройству и домену использования, и загружает его вместе с ключевым материалом в SE либо в профиль HCE. С этого момента телефон предъявляет себя терминалу как самостоятельный платёжный инструмент.

Secure Element (SE)

Apple Pay использует SE как отдельный защищённый чип внутри телефона или часов. Он физически изолирован от основного процессора и операционной системы, хранит ключи и выполняет криптографию так, чтобы ключевой материал не покидал SE. Скомпрометированная основная ОС не открывает доступ к SE [141].

Запрос терминала поступает от контроллера NFC к SE по выделенному пути, а ответ возвращается тем же маршрутом. Операционная система не видит ни содержимое ключей, ни сам криптографический обмен.

HCE (Host Card Emulation)

HCE (Host Card Emulation) — программная эмуляция карты: часть платёжной логики исполняется в операционной системе телефона, а не в отдельном чипе. Кошелёк опирается на сервис в ОС и связанный с ним защищённый раздел; его ключи ограничены по сроку или числу использований, поэтому кошелёк сильнее зависит от своевременного обновления через сетевые сервисы [142, 143].

Ключевой материал на устройстве состоит из пула LUK (Limited Use Keys, ограниченно используемые ключи), выпускаемых TSP и доставляемых кошельку при онлайн-связи. Каждый LUK ограничен порогами, которые задаёт эмитент через сетевой TSP: время жизни (TTL), количество транзакций и суммарный объём. При срабатывании любого порога ключ становится недействительным, при исчерпании пула кошелёк запрашивает пополнение у TSP-сервера [143]. Поэтому

HCE-кошелёк проводит без сети ровно столько операций, сколько у него осталось неиспользованных LUK; SE этим не ограничен — криптограмма формируется чипом из постоянного мастер-ключа и локального счётчика ATC, и для следующей операции сеть не нужна. *Floor limit* на стороне терминала и эмитента действует на оба класса одинаково.

Две модели сосуществуют из-за разного контроля над аппаратной платформой. Apple владеет и чипом SE, и контроллером NFC, и правилами доступа к ним. Исторически ни один сторонний кошелёк не получал прямого доступа к SE на iPhone. С августа 2024 года Apple открыла *in-app* NFC через SE для сторонних разработчиков в США, Великобритании, Канаде, Австралии, Новой Зеландии, Японии и Бразилии. В ЕС европейским разработчикам кошельков Apple открыла доступ раньше, по антимонопольным обязательствам перед Еврокомиссией от июля 2024 года — бесплатно и через HCE [144]. Apple Pay сохраняет аппаратную изоляцию SE; за пределами этих рынков доступ для остальных по-прежнему закрыт [141, 145]. В Android с его сотнями производителей SE есть только на части устройств, и доступ к нему контролирует OEM (Original Equipment Manufacturer, производитель устройства). HCE как программная эмуляция работает на любом устройстве с NFC за счёт более слабой модели доверия: ключи хранятся в ОС вместо отдельного чипа [142]. Для платёжной системы, которая не может требовать SE от каждого производителя, HCE остаётся единственным вариантом для массового выпуска.

Кошельки по архитектуре доверия

Кошельки ниже перечислены по убыванию аппаратной изоляции ключевого материала: от выделенного чипа SE через TEE к чисто программному HCE. Apple Pay работает по SE-модели: eSE на iPhone и Apple Watch с апплетом Apple Pay и собственной изолированной операционной системой; ATC и криптограмма — внутри чипа [141]. Fitbit Pay — SE на уровне носимого устройства; для него Google открыл Device Tokenization для SE-кошельков на носимых устройствах, чтобы переиспользовать инфраструктуру выпуска DPAN с отдельным TRID [146].

Samsung Pay — гибрид, ближе к TEE (Trusted Execution Environment), чем к отдельному eSE. TEE — изолированная среда исполнения внутри основного процессора: параллельно основной ОС работает доверенная, со своей памятью, недоступной основной системе; в смартфонах эту изоляцию обеспечивает ARM TrustZone. Ключи Samsung Pay хранятся в TrustZone Knox, а не в независимом сертифицированном чипе; криптограмма формируется внутри Secure World, ОС в Normal World ключей не видит, но физического разделения кремния, как у Apple, нет [147]. Схема Google Wallet зависит от устройства: на большинстве Android-устройств — HCE с обновлением пула LUK через TSP; на Pixel с Titan M через StrongBox API Google Pay может использовать аппаратное хранилище для ключевого материала, приближаясь к SE-модели [148]. Mir Pay — HCE через Mir HCE SDK поверх TSP НСПК; SE-варианта у Mir Pay нет, и архитектурно он сопоставим с Google Wallet на Android-устройстве без Titan M [37]. Garmin Pay на часах — SE: встроенный защищённый элемент NXP PN80T, токен выпускается через VTS и MDES у банков-партнёров [149].

С 10 марта 2022 года Apple Pay и Google Wallet не выпускают DPAN на карты Visa и Mastercard российского выпуска; существующие токены отключались поэтапно (гл. 9). В России кошельком с активным TSP остаётся Mir Pay (HCE); Apple Watch, Garmin и Fitbit карты «Мир» не поддерживают: Apple Watch потеряли их вместе с Apple Pay в марте 2022 года, Garmin Pay с ПС Мир не работает [150].

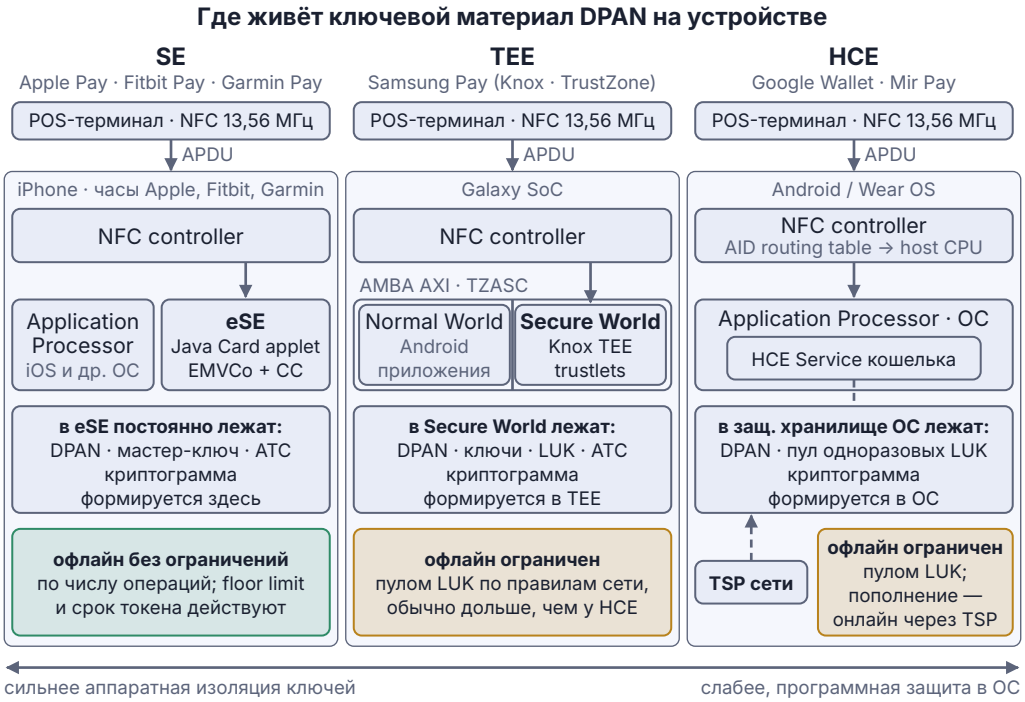


Рис. 22 — Где хранится ключевой материал DPAN: SE, TEE, HCE.

Таблица 17 — Архитектура доверия мобильных кошельков.

Свойство	SE (Apple Pay, Fitbit Pay, Garmin Pay)	TEE (Samsung Pay)	HCE (Google Wallet, Mir Pay)
Хранение ключей	отдельный сертифицированный чип eSE	TrustZone Secure World основного CPU	защищённое хранилище ОС, ключи в RAM при оплате
Криптограмма	генерирует SE из мастер-ключа и ATC	генерирует Secure World из LUK или мастер-ключа	генерирует приложение ОС из LUK
Обновление пула ключей	не требуется до истечения токена	по правилам сети, чаще, чем у SE	регулярное, при онлайн-связи с TSP
Офлайн	ограничен только сроком токена и *floor limit* сети	ограничен пулом LUK и *floor limit*	ограничен пулом LUK и *floor limit*
Зависимость от OEM	требует чипа SE на устройстве	требует TrustZone Knox	работает на любом Android с NFC

Карта секретов: что компрометируется и как далеко

Исторически модель угроз была нацелена на кремний карты; к 2026 году в чипе карты по-прежнему хранится её UDK, но остальной ключевой материал распределён по узлам инфраструктуры, и оценка риска начинается с защиты секрета и радиуса поражения при его компрометации — от одного устройства до всего портфеля эмитента.

Таблица 18 — Где хранятся секреты платёжной системы и радиус компрометации каждого.

Узел	Секрет	Защита	Радиус компрометации
HSM эмитента и эквайера	мастер-ключи IMK, LMK, ZMK	FIPS 140-3, PCI PTS HSM, dual control и split knowledge (раздел 10.3)	вся иерархия производных ключей и карт эмитента
Бюро персонализации	транспортный ключ (ТК)	dual control и split knowledge (раздел 7.11)	ключи всей выпущенной партии
eSE телефона или часов	ключи токена в чипе	аппаратная изоляция, Common Criteria	одно устройство; нужна физическая атака на чип
TEE (Knox)	ключи в Secure World	TrustZone, но общий кремний с CPU	устройство; шире eSE — физического разделения нет
HCE-пул LUK	ограниченные ключи LUK в хранилище ОС	TTL, лимиты числа и суммы, обновление от TSP	узкий: лишь неизрасходованные LUK до истечения
TSP	соответствие токена и PAN, генерация LUK	серверный периметр сети или НСПК	широкий: токены всех устройств TSP

Смещение секрета из карты в HSM, бюро и телефон перераспределило риск: самые широкие радиусы — у мастер-ключа HSM и транспортного ключа бюро, поэтому для них нужна церемония ключа с dual control и split knowledge (раздел 10.8). На устройстве радиус меньше: eSE ограничивает его физикой, HCE — сроком и числом LUK.

Банковские приложения Pay: BLE, СБП и зачем при Mir Pay

Mir Pay обслуживает один сегмент: Android, NFC, карта «Мир». SberPay, T-Pay, AlfaPay, VTBPay нужны для других сценариев — iPhone, расчёта через СБП и банковского бренда.

iPhone. Apple не открыла России доступ к NFC-API ни по модели EC, ни по отдельному соглашению, и Mir Pay на iOS не работает. С июля 2021 по март 2022 года карта «Мир» добавлялась в Apple Pay; 24 марта 2022 года Apple прекратила добавление карт Мир, а затем отключила уже добавленные [151]. Для iPhone российские решения используют BLE: в технологии НСПК «Волна» терминал обменивается данными со смартфоном по BLE, приложение подтверждает операцию, расчёт проходит через СБП [140, 152]. Сбер запустил на технологии «Волна» сервис «Вжух», работающий с 25 августа 2025 года на своих терминалах [153, 154]; Т-Банк включил BLE-оплату в T-Pay для iPhone с 15 сентября 2025 года, сначала на терминалах Сбера с «Вжухом», позднее — на терминалах T-Bank и Альфа-Банка [155].

Расчёт через СБП. Mir Pay использует карточную авторизацию и экономику ПС Мир с interchange; «Волна» в приложениях банков оформляет операцию как платёж по СБП (см. гл. 19), где тариф фиксированный и не привязан к карте. Для эмитента это смена канала: вместо карточной авторизации — кредитный перевод со счёта плательщика на счёт ТСП через ОПКЦ НСПК.

Бренд банка. В Mir Pay банк представлен через единый интерфейс НСПК: кнопка «платить» одна, кэшбэк эмитента показывается отдельно. SberPay, T-Pay, AlfaPay расширяют банковское приложение продуктовой логикой банка: лимитами, биометрией, лояльностью, программой рассрочки. Собственный Pay удерживает клиента

в приложении банка: помимо переводов и проверки баланса клиент из него же и платит.

Онлайн-кнопка и приложения партнёров. SberPay, T-Pay, AlfaPay встроены в формы оплаты на сайтах партнёров и в приложения ТСП как отдельный способ оплаты — помимо карты «Мир» и QR-СБП (см. раздел 22.3). Mir Pay этот сценарий не обслуживает — он NFC-кошелёк, не интернет-эквайер. Кнопка SberPay или AlfaPay позволяет ТСП принимать оплату от клиентов банка без отдельной карты на стороне покупателя. На странице оплаты (*checkout*) ТСП вызывает платёжный шлюз банка по REST (у Альфа-Банка — `payment.alfabank.ru/alfapay/payment.do`), шлюз отдаёт ссылку, по которой ОС открывает приложение банка через глубокую ссылку (*deep link*); клиент подтверждает операцию в привычном ему интерфейсе, ТСП получает результат вебхуком (*webhook*). Привязка кошелька клиента (`bindingId` в терминологии Альфы) переиспользуется для последующих списаний CIT и MIT (Customer- и Merchant-Initiated Transaction, см. раздел 30.2), и кнопка Pay работает для банка как эквайринговый способ оплаты поверх обычной привязки карты (*card-on-file*) [156].

BLE-сценарий требует привязки устройства, подлинности экземпляра приложения, риск-правил и совместимости с терминальным парком: ключевой материал DPAN тут не участвует, операцию подтверждает само банковское приложение через связь с серверной частью банка [157]. Доработанные терминалы под «Волну» и «Вжух» принимают одним жестом и платежи по СБП, и операции по картам «Мир» [140].

Выпуск DPAN: как телефон становится картой

Процедура привязки, описанная в начале раздела, одинакова для обеих архитектур; различается ключевой материал. В SE-сценарии на устройство загружается постоянный мастер-ключ и хранится в аппаратном чипе; в HCE-сценарии вместо него кошелёк получает от токен-сервиса ограниченный набор ключей LUK с пределами по сроку, числу и сумме операций; токен-сервис периодически их перевыпускает, а само платёжное приложение исполняется в среде ОС и использует программные средства защиты. Шаг ID&V (Identification & Verification, проверка личности держателя при выпуске DPAN) может завершиться по-разному: при достаточных данных эмитент выдаёт бесшовное (*frictionless*) одобрение, при недостатке — запрашивает повышенную проверку (*step-up*: одноразовый код или push-подтверждение), а при подозрениях — отказывает в привязке.

Процедура одинакова для Apple Pay, Google Pay и российских кошельков поверх TSP НСПК [158, 159]. Различия между VTS, MDES и TSP НСПК, а также их ограничения разобраны в разделе 9.5 и в главах 14, 15 и 16.

CDCVM: биометрия вместо PIN

При оплате телефоном верификация держателя происходит на самом устройстве через Face ID, Touch ID, отпечаток пальца или код разблокировки. Метод называется CDCVM (Consumer Device CVM) и сообщает эмитенту только одно — локальная проверка на устройстве прошла успешно [128]. Такой отметки достаточно, чтобы в мобильном платеже не запрашивать PIN на терминале и учитывать результат при оценке риска [55, 143].

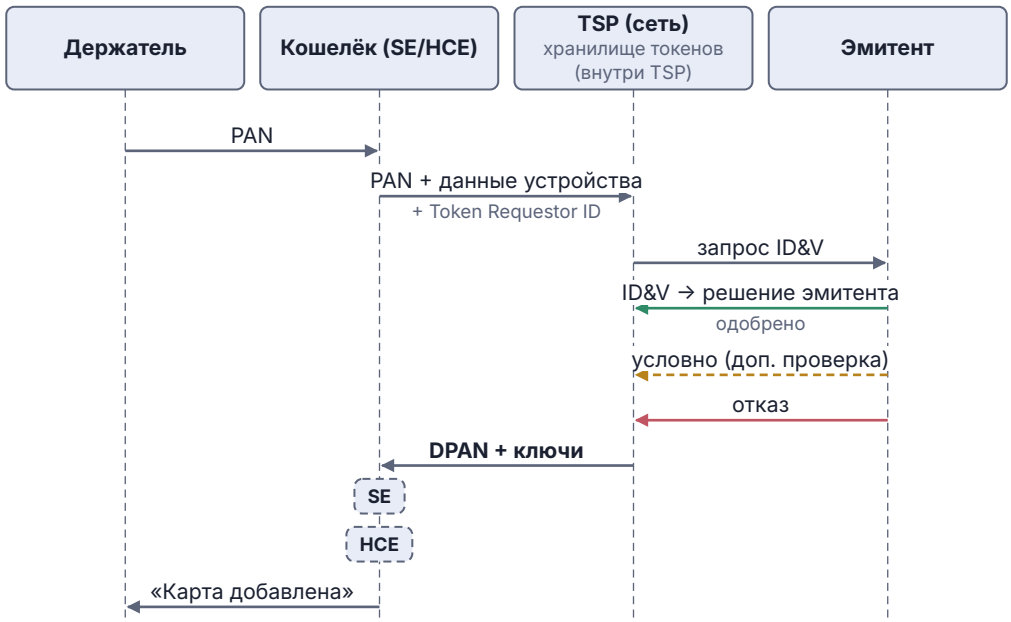


Рис. 23 — Выпуск и привязка токена при подключении мобильного платежа.

Содержимое авторизационного сообщения мобильного платежа

Авторизационное сообщение мобильного платежа несёт элементы, по которым эмитент отличает кошелёк от карты, определяет устройство и оценивает риск [35, 55].

Первый признак — DE 2, в котором передаётся DPAN, токен вместо настоящего PAN, выданный TSP при выпуске DPAN. DPAN выглядит как PAN, но относится к отдельному диапазону и представляет конкретное устройство или домен использования. DPAN приходит от терминала в DE 2, и сеть детокенизирует его до передачи запроса эмитенту [35].

Второй признак — DE 22, который сообщает, что операция выполнена бесконтактно; его значение то же, что у бесконтактной карты, и кошелёк выдают дополнительные поля EMV. Они несут криптограмму, счётчики и признаки, связанные с устройством и проверкой держателя, и по ним эмитент отличает обычную бесконтактную карту от мобильного кошелька и использует эти данные в модели выявления фрода [46, 55].

Третий признак — Token Requestor ID (TRID, идентификатор сервиса, запросившего выпуск DPAN). Он связывает токен с кошельком или сервисом и указывает сервис выпуска токена [35].

На пути к эмитенту карточная сеть детокенизирует запрос, заменяя DPAN на FPAN (Funding PAN, исходный номер карты, к которой привязан токен), и передаёт вместе с ним признаки токена. Настоящий PAN появляется только там, где нужен для авторизационного решения [35].

8.4 Носимые устройства: кольцо, часы, браслет

В кольце, часах и браслете работает тот же базовый принцип, что и в телефоне: антенна NFC, платёжное приложение и ядро бесконтактного обмена. По источнику питания носимые устройства делятся на два класса. Активные устройства (умные часы) имеют аккумулятор и могут нести собственный защищённый чип. Пассивные устройства (платёжные кольца и стикеры) получают питание только от поля терминала [128, 160]. Это разделение определяет, есть ли у устройства собственный CVM и какие сценарии для него доступны.

Носимые устройства проходят одобрение Level 1 по общему процессу EMVCo для мобильных устройств (*mobile*) плюс набор требований к антенне и устойчивости связи, специфичных для носимых устройств [139, 161]. Для пассивных колец требования особенно жёсткие: маленькая антенна и питание только от поля терминала оставляют узкий запас по энергии и стабильности обмена.

Умные часы с собственной ОС получают токен так же, как телефон, через кошелёк, интеграцию с TSP и выпуск DPAN. Пассивные кольца и стикеры проходят персонализацию при производстве, когда платёжное приложение и ключи прошиваются в чип на фабрике, а держатель привязывает кольцо к карте через сервис эмитента или процедуру поставщика устройства [139].

Верификация держателя на носимых устройствах ограничена устройством ввода. Клавиатуры нет, и часы используют контроль ношения на запястье (*on-wrist detection*): если часы сняли и надели заново, кошелёк требует повторной проверки. Это слабее биометрии: датчик ношения не различает, кому принадлежит запястье. Пассивные кольца и стикеры отдельного метода верификации не дают вовсе, и их сценарии ограничены суммами ниже бесконтактного порога.

Без CVM пассивные устройства целиком зависят от порога. Когда порог повышается, как во многих странах после 2020 года, без проверки проходит больше бесконтактных платежей, и риск при утере кольца растёт вместе с лимитом. Эмитент компенсирует это собственными порогами и лимитами по частоте (*velocity*) на стороне авторизации.

8.5 Relay attack и пределы защиты

Бесконтактный интерфейс упрощает атаку, которую для контактного Chip & PIN показали ещё в 2007 году [162], — *relay attack*: злоумышленник ставит одно устройство рядом с картой жертвы, второе — рядом с терминалом, и в реальном времени ретранслирует между ними протокольный диалог через Bluetooth, Wi-Fi или интернет. Терминал видит настоящую карту, карта видит настоящий терминал, а физическое расстояние между ними ограничено лишь задержкой ретрансляционного канала и Frame Waiting Time по ISO 14443-4: десятки метров через Bluetooth, произвольное расстояние через IP [129, 163].

Криптограмма при этом остаётся корректной, ведь её вычисляет настоящий чип на основании настоящих данных транзакции, и простая привязка к сумме или времени в этом сценарии бесполезна. Атакующий переносит протокол на расстояние, не ломая его [129].

Криптографический ответ на *relay attack* — *distance bounding* (привязка по расстоянию), отсечка ответов с подозрительно длинной задержкой, выявляющая удалённое устройство по времени отклика. В массовых терминалах общего назначения *distance bounding* почти не встречается. Mastercard с 2016 года включает в бесконтактную

спецификацию собственный вариант — Relay-Resistant Protocol (RRP), где ридер измеряет *round-trip time* отдельных обменов с картой; к 2020 году в эксплуатации он не встречался. Реализация остаётся дорогой, и для большинства сетей оборудование с такой точностью не оправдано текущим уровнем потерь [164, 165].

Вместо *distance bounding* платёжные системы опираются на независимые проверки. Бесконтактный порог отсекает крупные суммы без верификации; эмитент дополнительно ограничивает количество и сумму последовательных операций без PIN. Контроль частоты на стороне эмитента повышает риск-оценку для нескольких бесконтактных операций за короткий интервал или в нехарактерной для держателя географии. CDCVM в мобильных кошельках требует биометрию или код разблокировки перед каждой операцией, и *relay attack* одного диалога по NFC требует физического участия владельца устройства [55, 128].

У пассивных карт и колец CDCVM нет, и защита опирается только на порог и частотные лимиты. При высоком пороге и слабом контроле частоты *relay attack* остаётся практически осуществимой атакой. Для мобильных кошельков с CDCVM она технически возможна, но требует одновременного доступа к разблокированному устройству и к ретранслятору, и массовое применение исключено [129].

9 Токенизация PAN

Утечка базы сохранённых карт даёт злоумышленнику миллионы PAN. Украденный токен привязан к конкретному ТСП, устройству или каналу и за их пределами обычно бесполезен.

9.1 Назначение токенизации

PAN редко остаётся в одной системе. Продавец хранит его для оплаты, PSP (Payment Service Provider, платёжный провайдер) — для возвратов, подписочный сервис — для рекуррентных списаний. Каждая копия расширяет зону риска: компрометация одной из систем раскрывает PAN, прошедший через все остальные.

Heartland Payment Systems с конца 2007 по январь 2009 года потеряла порядка 130 миллионов PAN после того, как SQL-инъекция на корпоративном веб-сервере открыла атакующим доступ к процессинговой сети, где они установили вредоносное ПО для перехвата карточных данных [166]. Удар пришёлся на процессинговый узел, через который проходили карты множества эмитентов и клиентов. По данным 10-K Heartland за 2010 финансовый год (подан в SEC 10 марта 2011) совокупные расходы и урегулирования по инциденту с момента раскрытия в январе 2009 и до 31 декабря 2010 года составили $146,1 млн до страхового возмещения [167]. Каждый скомпрометированный PAN означал потенциальный перевыпуск с новым номером, новым пластиком и обновлением всех подписочных привязок у держателя карты. Эмитент платит за перевыпуск напрямую, держатель карты — прерванными подписками и ручным обновлением реквизитов.

Если вместо PAN по маршруту передаётся токен, утечка базы ТСП не раскрывает настоящий PAN. Украденный токен бесполезен вне своего домена: он привязан к конкретному ТСП, устройству или каналу и в чужом контексте не сработает [35].

Токенизация также сужает периметр PCI DSS (Payment Card Industry Data Security Standard, подробно — в гл. 12), но только при разделении доступа. От требований освобождены компоненты, которые работают исключительно с токенами и не имеют доступа к детокенизации. Хранилище токенов и любая система с доступом к PAN остаются в периметре. Подробнее о периметре CDE (Cardholder Data Environment, среда обработки карточных данных), сужении периметра, P2PE (Point-to-Point Encryption) и разновидностях токенизации (сетевая, токен PSP, vault и FPE, Format-Preserving Encryption) — в разделе 12.3.

Сетевая и локальная токенизация различаются охватом. Локальный токен действует внутри сервиса, который его выпустил и может детокенизировать. Сетевой токен выпускает и распознаёт сама карточная сеть, поэтому он проходит весь путь от ТСП до эмитента: компрометация любого узла маршрута раскрывает токен, а не PAN. Матрица в табл. 19 показывает узлы по периметру PCI: *в CDE* — полный набор требований PCI DSS, *расширенный CDE* — узел содержит vault детокенизации, *вне CDE* — узел видит только токен или DPAN. Vault в сетевой токенизации существует внутри одной карточной сети: VTS у Visa, MDES у Mastercard, TSP НСПК у ПС Мир. Единого хранилища на все сети нет: один и тот же PAN у разных сетей токенизируется независимо.

Таблица 19 — Узлы × сценарии токенизации; цвет ячейки — PCI-периметр узла

Узел	До токенизации	Локальная токенизация	Сетевая токенизация
ТСП A e-commerce	**PAN-копия** в CDE	**локальный токен** вне CDE	**DPAN** вне CDE
ТСП B другая площадка	**PAN-копия** в CDE	**локальный токен** отдельный от ТСП A	**DPAN** свой DPAN на каждый ТСП
PSP / шлюз провайдер платежей	**PAN-копия** в CDE	**PAN + токен (vault)** в CDE, расширенный периметр	**DPAN** вне CDE — детокенизация в сети
Подписка card-on-file / MIT	**PAN-копия** в CDE	**локальный токен** вне CDE	**DPAN + PAR** card-on-file без PAN

Заливка ячейки показывает периметр PCI DSS узла: красный — в CDE, жёлтый — расширенный периметр, зелёный — вне CDE.

9.2 Разночтения термина «токен»

Под словом «токен» разные источники понимают разные объекты, а семейство `*PAN` у EMVCo, PCI SSC, Visa, Mastercard и НСПК использует несовместимые определения. Поэтому словарь фиксируется до разбора архитектуры: иначе понятия придётся сверять на каждом шаге.

PCI SSC определяет токенизацию широко — это любой суррогат исходного PAN: vault, FPE, сетевой токен. EMVCo Payment Tokenisation Framework, напротив, описывает только сетевой токен с собственным BIN из выделенного сетью диапазона и детокенизацией через TSP; суррогаты из vault и FPE для EMVCo токенами не являются [35, 168]. Visa и Mastercard в публичных материалах используют свои бренды (Visa Token, MDES, MDES for Merchants, Visa Token Management Service) — они конкретизируют EMVCo, не расширяют его.

Правила ПС Мир называют токен «альтернативным номером Карты (Токеном)» [169]. Пары «Токен (DPAN)» и «номер карты (FPAN)» встречаются в условиях Mir Pay, которые публикуют банки-эмитенты [170]: «DPAN» там используется как второе имя «Токена», область действия устройства отдельно не выделена. У EMVCo `token` — родовой класс, который ограничивают устройством, ТСП или сценарием платежа [35]; DPAN и MPAN — отраслевые имена токенов с областью действия устройства или ТСП. `MPAN` в канонической документации НСПК как термин отсутствует, и функционального аналога нет: Mir Pay SDK app2app работает поверх DPAN (выпуск DPAN (*provisioning*) в Mir Pay из приложения банка плюс *In-Application e-commerce* — оплата из приложения ТСП), а токена с областью действия ТСП под именем `MPAN` в правилах ПС Мир не определено [37].

Терминология TSP воспроизводит ту же асимметрию: у Visa и Mastercard это VTS и MDES, формально TSP по EMV Payment Tokenisation Specification — Technical Framework. В документации НСПК слово «TSP» в этом смысле не применяется; банковские условия Mir Pay называют «Провайдером» поставщика приложения Mir Pay, АО НСПК.

Прочерк в колонке НСПК означает, что термина в канонической российской документации нет: «pseudo PAN» и «MPAN» встречаются только у PCI SSC и западных сетей. Инженеру, который ищет «MPAN у Mir Pay», в документации НСПК нужны имена «Mir Pay In-Application» и «app2app».

Таблица 20 — Семейство *PAN по источникам.

Термин	EMVCo	PCI SSC	Visa	Mastercard	Жаргон	НСПК
token	сетевой только	любой суррогат	Visa Token	MDES token	любой суррогат	«альтернативный номер Карты (Токен)»
DPAN	область действия устройства	—	Visa Token (device)	MDES (device)	= сетевой токен	синоним «Токена» в условиях Mir Pay банков
MPAN	область действия ТСП	—	VTS / TMS	MDES for Merchants (M4M)	путают с vault CoF	—
FPAN	исходный PAN	—	источник средств	исходная карта	реальный PAN	«номер карты (FPAN)» в условиях Mir Pay банков
pseudo PAN	—	— (канон — «surrogate value»)	—	—	нестрого = токен	—
surrogate	—	surrogate value (канон)	—	—	редко	—
TSP	Token Service Provider	—	VTS	MDES	любой токен-сервис	«Провайдер» Mir Pay

Канон книги дальше по тексту: *токен* — сетевой токен EMVCo, если не сказано иное; *токен в vault* и *FPE* упоминаются явно с уточнением «суррогат для хранения и аналитики, не для маршрутизации»; *TSP НСПК* обозначает функциональную роль «Провайдера» Mir Pay, а не официальный российский термин.

С 10 марта 2022 года Visa и Mastercard не обслуживают карты российских банков, а их TSP-сервисы (VTS, MDES, M4M, TMS) российскому эмитенту и эквайеру недоступны: новые DPAN и MPAN на Visa/Mastercard российского выпуска не генерируются, существующие DPAN в Apple Pay и Google Pay прекратили работу поэтапно: у карт пяти банков под санкциями — с 25 февраля 2022 года, у остальных карт Visa и Mastercard российского выпуска — с 10 марта [171—173]. В России с этого дня единственный действующий сетевой TSP — TSP НСПК для карт «Мир»: Mir Pay (DPAN, область действия устройства) и Mir Pay SDK app2app для *In-Application e-commerce*. Операции UnionPay в РФ обрабатывает НСПК, но токенизация UnionPay принадлежит UnionPay International и через TSP НСПК не проходит. Разбор VTS, MDES, M4M и TMS дальше служит справочным образцом модели EMVCo: российскому эмитенту он даёт терминологию для разговора с международными вендорами, но не доступ к этим инструментам.

9.3 Структура сетевого токена

Сетевой токен несёт больше данных, чем обычный PAN: к номеру прикреплены метаданные о запросчике, проверке держателя карты и разрешённом домене [174].

Первый атрибут — **Token Requestor**, участник, запросивший токен: кошелёк, ТСП, PSP или подключённое устройство. В модели EMVCo TRID (Token Requestor ID) назначает Token Service Provider при регистрации запросчика. Первые три цифры идентификатора — TSP Code, который выдаёт сама EMVCo, оставшиеся — порядковый номер запросчика у конкретного TSP. По TRID и сеть, и эмитент определяют, через какой канал выпущен токен. Одна карта может породить несколько токенов с разными сценариями и жизненными циклами: отдельно для телефона, для браузера, для подписки [174].

Второй набор метаданных связывает токен с качеством проверки держателя карты. В терминологии EMVCo это **Token Assurance Method** — характеристика того, как программа токенизации оценила проверку держателя карты при выпуске. Отдельные сети затем отображают эту характеристику в свои уровни и коды. Чем строже проверка при выпуске, тем выше доверие к токену в дальнейших операциях [174].

Token Domain Restriction Controls задают контекст, в котором токен разрешено использовать: NFC, интернет-покупки у конкретного ТСП или рекуррентные списания у определённого получателя. Попытку вывести токен за пределы домена сеть отклоняет до этапа авторизации [35, 174].

TSP проверяет домен до детокенизации: сервер сопоставляет канал запроса (contactless, CNP — Card-Not-Present, операции без физического предъявления карты, см. гл. 11; recurring — рекуррентное списание), TRID инициатора и MID (Merchant ID, идентификатор ТСП в эквайринге) с атрибутами ограничения, записанными при выпуске токена. При несовпадении TSP возвращает отказ на шаге маршрутизации, до того как запрос дойдёт до эмитента.

Компонент TSP, выполняющий это сравнение, дальше назван *matcher*'ом. У токена — набор атрибутов (разрешённые каналы, TRID, опциональный список MID), у запроса — фактические значения; matcher сверяет их поэтапно, и при любом несовпадении возвращает отказ с причиной, не отправляя авторизационный запрос эмитенту. На листинге ниже — его учебная реализация с атрибутами: канал, TRID и опциональный список MID. Промышленный TSP той же поэтапной проверкой разбирает также статус токена, криптограмму (TAVV — Token Authentication Verification Value, криптограмма сетевого токена для e-commerce, разобрана в разделе 9.9), срок действия и уровень доверия к токену.

```
from dataclasses import dataclass
from enum import Enum


class Channel(Enum):
  CONTACTLESS = "contactless"
  CNP = "cnp"  # card-not-present, e-commerce
  RECURRING = "recurring"


@dataclass(frozen=True)
class TokenRestrictions:
  allowed_channels: frozenset[Channel]
  token_requestor_id: str
  # None -- ограничение по MID не задано (типично для NFC-токена устройства).
  allowed_merchants: frozenset[str] | None = None


@dataclass(frozen=True)
class Request:
  channel: Channel
  token_requestor_id: str
  merchant_id: str


def check_domain(token: TokenRestrictions, request: Request) -> str | None:
  if request.channel not in token.allowed_channels:
```

(продолжение)

```
    return f"канал {request.channel.value} не входит в разрешённые"
  if request.token_requestor_id ≠ token.token_requestor_id:
    return "TRID запроса не совпадает с TRID токена"
  if (
    token.allowed_merchants is not None
    and request.merchant_id not in token.allowed_merchants
  ):
    return f"MID {request.merchant_id} не входит в разрешённые"
  return None
```

У токена есть собственные операции жизненного цикла: публичные материалы Visa перечисляют activate, resume, suspend и delete [36], а НСПК в описании Mir HCE (Host Card Emulation, см. гл. 8) SDK отдельно описывает управление жизненным циклом токена [37]. Скомпрометированный токен останавливают отдельно, оставляя саму карту действующей [35].

9.4 Семейство токенов по области действия

Сетевые токены различаются по области разрешённого использования: устройство или ТСП. Один FPAN (см. раздел 4.1) порождает столько токенов, сколько у держателя карты точек оплаты, и компрометация одного из них не затрагивает остальные.

DPAN действует в пределах одного устройства: у каждого устройства держателя карты — iPhone, Apple Watch, Pixel, Galaxy Wearable — свой DPAN. Скомпрометированный DPAN отзывается отдельно; FPAN и остальные DPAN продолжают работать [35, 36]. Физическое место хранения DPAN на устройстве (SE, TEE, HCE) и различия между Apple Pay, Samsung Pay, Google Wallet, Mir Pay, Garmin / Fitbit Pay разобраны в разделе 8.3.

MPAN действует в пределах одного ТСП: ТСП получает токен при первой авторизации и использует дальше для *card-on-file*. У Mastercard этот класс реализован как MDES for Merchants (M4M); у Visa аналогичная функциональность доступна через VTS и Token Management Service (Visa Acceptance Solutions). MPAN нельзя путать с токеном в vault у PSP: такой токен действует внутри хранилища провайдера и не передаётся в сеть, MPAN — полноценный сетевой объект с собственным TRID и Token Domain Restriction Controls. У НСПК аналога нет: Mir Pay SDK app2app реализует привязку к устройству поверх DPAN (выпуск DPAN и *In-Application e-commerce*), а токен с областью действия ТСП под именем MPAN в правилах ПС Мир не определён [37].

Токен в vault на стороне PSP относится к отдельному семейству суррогатов вне модели EMVCo. Шлюз хранит PAN в собственном защищённом хранилище и возвращает ТСП непрозрачную ссылку. Эта ссылка не маршрутизируется в сети, не требует TSP-детокенизации и не несёт сетевого контекста (*assurance*, *domain restriction*). Архитектурное различие с сетевыми токенами разобрано в разделе 9.6.

Pseudo PAN стоит особняком: синтаксически валиден как PAN (длина и алгоритм Луна совпадают), но маршрутизируется не в сеть, а в vault или ключевую инфраструктуру. Платёжным объектом он не является, к авторизации непригоден и служит для сужения CDE [168, 175].

Таблица 21 — Семейство *PAN по области действия и маршрутизации.

Параметр	FPAN	DPAN	MPAN	Vault PSP	Pseudo PAN
Эмитент токена	банк-эмитент	TSP сети	TSP сети	PSP	организация
Область действия	глобальная	одно устройство	один ТСП	один vault	один vault/ключ
Маршрутизация	в сети	в сети	в сети	не в сети	не в сети
Детокенизация	—	TSP перед эмитентом	TSP перед эмитентом	PSP перед сетью	vault/FPE-ключ
Хранение	эмитент, vault сети	TEE/SE устройства, vault сети	vault сети, у ТСП	vault PSP	vault или ключи
Отзыв	перевыпуск карты	отдельно по DPAN	отдельно по MPAN	отдельно по записи	ротация ключей
Где встречается	везде	Apple/Google/ Mir Pay	крупные *card-on-file*-ТСП	PSP-интеграции	сужение CDE

9.5 VTS, MDES, TSP НСПК

У каждой крупной карточной сети свой токен-сервис, и архитектура у всех почти одинакова: TSP работает с Token Requestors, при необходимости запрашивает подтверждение эмитента на выпуск токена и встраивает этот токен в платёжный поток вплоть до авторизации. Различия касаются правил управления, жизненного цикла и интеграционной политики [35, 174].

VTS (Visa Token Service)

Token Requestor (например, мобильный кошелёк) подаёт запрос на выпуск токена. Провайдер обращается к эмитенту, чтобы подтвердить личность держателя карты, и при необходимости запрашивает дополнительную проверку. После одобрения Visa заменяет PAN сетевым токеном и передаёт его цифровому платёжному сервису для использования онлайн и через NFC. По документации Visa такой токен ограничивают конкретным устройством, интернет-продавцом или числом покупок до истечения [36].

API эмитента в VTS Visa делит на выпуск (Provisioning), управление учётными данными (Credential Management) и уведомления (Notifications). ID&V (Identification & Verification, проверка личности держателя карты при выпуске токена) и дополнительная проверка относятся к выпуску. В управление учётными данными входят Token Inquiry, который отдаёт данные об устройстве и риске, и Token Lifecycle с операциями activate, resume, suspend и delete [36].

MDES (Mastercard Digital Enablement Service)

Mastercard описывает MDES как единую платформу для эмитентов, поставщиков кошельков, ТСП и других участников, запрашивающих токены. В документации MDES Token Connect среди открытых token requestors перечислены кошельки на мобильных и встраиваемых устройствах, торговые платформы и ТСП [176, 177].

Token Connect (*push-provisioning*) позволяет эмитенту инициировать выпуск токена в сторонний кошелёк или к ТСП без отдельной интеграции с каждым из них [177].

Таблица 22 — Архитектурные компоненты TSP карточной сети.

Компонент TSP	Назначение
Token Requestor Interface	Связь с ТСП, кошельком или провайдером
Token Vault	Хранит соответствие токена и PAN
Issuer Interface	Взаимодействие с эмитентом при выпуске токена

У Visa ту же задачу решает Visa Card Enrollment Hub: одна интеграция даёт *push-provisioning* во все подключённые кошельки и ТСП [178].

TSP НСПК

Публичные материалы НСПК раскрывают модель токенизации ПС Мир скупее, чем Visa или Mastercard, но описывают сценарии, в которых Mir HCE SDK вызывает сервисы НСПК для токенизации карт «Мир». Держатель карты подаёт заявку на токенизацию, указывает метод ID&V, получает одноразовые ключи для транзакций и управляет жизненным циклом токена [37].

Национальный маршрут и приложение Мир разобраны в гл. 16.

9.6 Сетевой токен и токен PSP

Сетевой токен рассчитан на путь от точки продажи через эквайера и платёжную сеть до авторизации у эмитента; локальная токенизация на стороне PSP остаётся внутри более узкого периметра ТСП и его PSP [35].

Локальный токен PSP убирает PAN из базы ТСП и заменяет его непрозрачной ссылкой на хранилище провайдера, но сетевого токенового контекста не создаёт. EMVCo, напротив, описывает сетевой токен как идентификатор, который можно ограничить ТСП, устройством или платёжным сценарием [35, 174].

Эмитент получает с сетевым токеном дополнительный контекст: кто запросил токен, как была проверена личность держателя карты и в каком домене токен разрешено использовать. По EMVCo сетевыми токенами можно управлять и заменять их для ТСП, устройств или типов транзакций, часто без участия держателя карты [35].

Локальная токенизация проще в интеграции: весь обмен замкнут внутри PSP. Сетевая токенизация требует прямой работы с токен-сервисом сети или подключения провайдера, который скрывает эту интеграцию от ТСП.

Хранилищная (*vault*) токенизация и FPE для защиты хранимых данных решают другую задачу: заменяют PAN суррогатом в базах аналитики, CRM или биллинга, чтобы эти системы вышли из периметра CDE. Карточная сеть здесь не участвует, и такой суррогат непригоден для транзакции.

Табл. 23 сводит архитектурное различие к практическим последствиям для интегратора: переносимости токена, периметру PCI DSS у ТСП и PSP, жизненному циклу при перевыпуске карты и стоимости интеграции.

Таблица 23 — Сравнение сетевого токена и токена PSP.

Параметр	Сетевой токен (VTS / MDES / TSP НСПК)	Токен PSP
Переносимость	да	нет
Область PCI DSS ТСП	минимальная	сужена
Область PCI DSS PSP	сужена	полная
Доля одобрений	по маркетинговым материалам сетей — выше	без изменений
Жизненный цикл	автообновление	ручное + Account Updater
Стоимость интеграции	средняя	низкая

Более высокую долю одобрений по сетевому токену заявляют сами сети в маркетинговых материалах: публичного независимого подтверждения нет, а величина зависит от сегмента ТСП. Обновление реквизитов у токена PSP идёт вручную или через Account Updater — сервис сети, обновляющий PAN и срок действия карты у ТСП при перевыпуске.

9.7 Внутренняя токенизация банка

Внутренний vault нужен банку, когда PAN надо вынести из собственных нижестоящих (*downstream*) систем — CRM, аналитики, биллинга, антифрод-витрин, — но при этом сохранить обратную операцию для узкого круга авторизованных сервисов. Сетевой токен решает другую задачу — убирает PAN из авторизационного и клирингового потока до эмитента; внешний vault PSP переносит хранение PAN за периметр организации. Три механизма не взаимозаменяемы: банк, который пытается сократить периметр PCI DSS одним из них, не получит ожидаемого результата. Различия сведены в табл. 24.

Таблица 24 — Внутренний vault, сетевой токен и внешний PSP-vault: критерии выбора.

Критерий	Внутренний vault	Сетевой токен (DPAN, MPAN)	Внешний PSP-vault
Что уходит в авторизацию до эмитента	PAN: vault подставляет его перед отправкой	токен на всём маршруте	PAN: PSP подставляет его перед сетью
Где хранится PAN	внутри банка	в vault карточной сети	у PSP
Сокращает ли CDE нижестоящих систем (CRM, аналитика, биллинг)	да, основная задача	частично: если эти системы видят токен, а не PAN	да, если ТСП передаёт PAN только PSP
Кто контролирует ключи (851-П, ГОСТ Р 57580.1-2017)	банк	TSP карточной сети	PSP
Автообновление при перевыпуске карты	нет, нужен внешний Account Updater	да, через обновление жизненного цикла токена в TSP	зависит от PSP

Vault со справочной таблицей и FPE

Vault со справочной таблицей (*lookup*) генерирует случайный токен и хранит соответствие PAN ↔ токен в отдельном защищённом хранилище. Безопасность опирается на хранилище и разграничение доступа: знание токена без доступа к vault не даёт PAN. PCI SSC Tokenization Product Security Guidelines (2015) выделяет Card Data Vault в отдельный домен требований (Domain 3): обязательное шифрование PAN внутри хранилища и управление доступом; жизненный цикл ключей по ISO/IEC 11568-1 вынесен в Domain 4 (Cryptographic Key Management) [179].

Format-Preserving Encryption (FPE) по NIST SP 800-38G — другой класс: PAN шифруется в значение той же длины и алфавитного состава без отдельного хранилища соответствий, обратная операция — расшифровка тем же ключом. Действующая редакция SP 800-38G (2016) описывает режимы FF1 и FF3 [175]. Второй публичный черновик SP 800-38G Revision 1 (3 февраля 2025) оставил только FF1 и исключил FF3 после работы Beyne, показавшей уязвимость в схеме подмешивания настроечного параметра — твика (*tweak*) — в раунды шифра; уязвимость затрагивает FF3, но не FF1. Тот же черновик поднял минимальный размер домена со ста до миллиона возможных входов, запретил обратную функцию AES и арифметику с плавающей точкой (*floating-point*) в реализациях FF1 (последнее — из-за исторической ошибки Bouncy Castle, обнаруженной Bleichenbacher) [180].

Vault и FPE расходятся по модели компрометации. В vault компрометация хранилища или ключа шифрования раскрывает все хранящиеся PAN, но компрометация отдельной записи ограничивается этой записью. В FPE компрометация ключа — это компрометация всех когда-либо выданных токенов сразу: каждый из них криптографически выводится из PAN и общего ключа, один секрет связывает их все.

Архитектура vault внутри банка

Хранилище соответствий хранит пары PAN ↔ токен. PAN зашифрован: у западного банка — AES-256-GCM на ключах, управляемых KMS или HSM; у российской финорганизации в CDE по ГОСТ Р 57580.1-2017 — Кузнечик через сертифицированное СКЗИ [181]. PCI SSC требует, чтобы хранилище соответствий и настоящие PAN находились в PCI DSS-периметре, даже если все нижестоящие системы видят только токены [168].

HSM или KMS поверх HSM управляет ключами шифрования хранилища и ключами генерации токенов, если те используются. Для аппаратных продуктов токенизации PCI SSC рекомендует валидацию по FIPS 140-2 Level 3 и работу в FIPS-режиме либо HSM из перечня PCI [179]; для *cloud HSM-as-a-Service* действуют отдельные требования по изоляции между арендаторами и передаче ключей. У российской финорганизации HSM сертифицирован ФСБ как СКЗИ класса КС2 или КС3; ключи шифрования хранилища выводятся из ключевой иерархии, разобранной в гл. 10.

API `tokenize` и `detokenize` разделены по правам. Системы, записывающие данные, имеют только право `tokenize`: передают PAN, получают токен. Системы, выполняющие авторизацию или возврат, имеют право `detokenize`: передают токен, получают PAN. Большинство нижестоящих узлов не получают ни того, ни другого — они работают только с уже выданными токенами. Так CDE сужается до vault и узлов детокенизации; остальные системы выходят из периметра PCI DSS.

Аудит хранит каждый вызов `tokenize` и `detokenize`: кто инициировал, какой токен затронут, для `detokenize` — обязательная причина. По ГОСТ Р 57580.1-2017 (направление РЗИ раздел 8) финансовая организация ведёт учёт объектов и ресурсов доступа на всех уровнях информационной инфраструктуры и регистрирует действия

работников и клиентов с автоматизированными системами по детализированному составу полей (дата, время, идентификатор работника, код участка, результат) [181].

Облачный vault (AWS Payment Cryptography, Azure Confidential Computing, Google Cloud HSM) разворачивается за недели, но для российского банка, которому надо выполнять 851-П и ГОСТ Р 57580.1-2017, эта модель неприемлема: ключи и хранилище оказываются за пределами суверенного периметра. *On-premises* vault с собственным HSM — единственный рабочий вариант для российского банка; срок развёртывания на порядок больше, а сертификация ФСБ и приёмка — отдельный проект со своими сроками, бюджетом и командой, а не строка в плане внедрения vault.

Российская специфика: vault как единственный путь

В России FPE нет среди сертифицированных криптографических механизмов. ТК 26 (Технический комитет по стандартизации «Криптографическая защита информации» при Росстандарте) не стандартизировал ни один режим FPE — ни на Кузнечике (ГОСТ 34.12-2018), ни на AES. В опубликованных Рекомендациях по стандартизации (серия Р 1323565.1) и Методических рекомендациях ТК 26 на 2024–2026 годы FPE не упоминается; тематически ближайший документ — МР по режиму работы блочных шифров для защиты носителей информации с блочно-ориентированной структурой, который решает другую задачу (защита данных на диске, не FPE короткого поля) [182]. Сертификата ФСБ на FPE-конструкцию, построенную поверх Кузнечика или AES, нет ни у одного российского производителя.

Следствие для российского банка: внутренняя токенизация — это vault, а не FPE. Конструкция: хранилище соответствий с PAN, зашифрованным Кузнечиком через сертифицированное СКЗИ; ГОСТ TLS до vault при обращении по сети; HSM или СКЗИ в доверенном сегменте сети; меры по ГОСТ Р 57580.1-2017 в зависимости от уровня защиты, требуемого регулятором для конкретного банка — усиленный для системно значимых организаций и операторов услуг платёжной инфраструктуры значимых платёжных систем, стандартный для остальных [181].

Когда внутреннего vault достаточно, когда нет

Внутренний vault сокращает периметр нижестоящих систем; PAN остаётся в авторизационном и клиринговом потоке до эмитента, пока не используется сетевой токен, и остаётся внутри организации, пока хранение не вынесено во внешний PSP-vault.

Архитектура крупного российского банка использует все три механизма одновременно: внутренний vault для аналитики, CRM и биллинга; сетевые токены через TSP НСПК для карт «Мир» (другие сетевые токены российскому эмитенту с марта 2022 недоступны — VTS и MDES не обслуживают карты российских банков, а UnionPay токенизирует на стороне UnionPay International, не через НСПК); внешние PSP-vault для *e-commerce*-ТСП, где банк выступает эквайером. Эти механизмы не взаимозаменяемы: у каждого свой жизненный цикл, свой набор требований PCI DSS и своя точка ответственности при инциденте.

9.8 Антипаттерн: BIN и хвост вместо токена

Локальная схема, где токен строится из сохранённого BIN, случайных средних цифр и последних четырёх цифр исходного PAN, остаётся маской PAN: CDE у ТСП

не сокращается, а записи независимых утечек склеиваются в один профиль по совпадению маски — без PAN и без доступа к vault. Такую маску выдают за локальную токенизацию у небольших ТСП и молодых PSP, потому что она сохраняет привычное отображение на чеке и даёт маршрутизацию по карточной сети без обращения к vault.

Сколько PAN проходит проверку Луна под одной маской

При 16-значном PAN со стандартной маской «BIN 6 + хвост 4» средняя часть содержит 6 цифр. Сумма Луна по модулю 10 — линейное уравнение от цифр, удвоение в алгоритме Луна — биекция на $\{0,\dots,9\}$ (0→0, 1→2, 2→4, 3→6, 4→8, 5→1, 6→3, 7→5, 8→7, 9→9). Для любой комбинации d свободных цифр сумма пробегает все десять остатков равномерно; из 10^d комбинаций ровно 10^{d-1} проходят проверку Луна. Для маски 6+4 это $10^5 = 100\,000$ PAN на один публичный слепок (*fingerprint*). Полная длина PAN создаёт видимость пространства 10^{16}; маска оставляет пять десятичных порядков.

После ревизии ISO 7812 2017 года идентификатор эмитента занимает восемь цифр [54]; требование 3.4.1 PCI DSS ограничивает отображение PAN полным BIN и последними четырьмя цифрами [70], а FAQ 1492 разъясняет это правило для 8-значного BIN [73]. У стандартного 16-значного PAN свободная часть сжалась до четырёх цифр, и количество кандидатов на маску упало до $10^3 = 1\,000$. Расширение BIN увеличивает адресное пространство эмитентов и одновременно сужает множество кандидатов у маски, выданной за токен, в сто раз.

Для любой длины PAN ответ равен 10^{d-1}, где d — число свободных цифр в средней части (для шестизначного BIN и четырёхзначного хвоста: 13-значный устаревший PAN Visa — 10^2, 15-значный Amex — 10^4, 19-значный длинный PAN — 10^8). Формула проверяется прямым перебором: при учебной длине 8 цифр с маской 3+2 формула даёт 10^2, и перебор всех 10^3 комбинаций средней части даёт то же число.

Код ниже реализует этот антипаттерн: `tokenize_by_bin_tail` получает длину BIN и хвоста, генерирует свободные средние цифры и подбирает последнюю свободную цифру так, чтобы суррогат проходил проверку Луна. Vault намеренно не моделируется: даже если связь суррогат → FPAN хранится отдельно, публичное значение уже сохраняет слепок исходного PAN.

```
import secrets


def luhn_valid(pan: str) → bool:
  total = 0
  double = False
  for ch in reversed(pan):
    digit = int(ch)
    if double:
      digit *= 2
      if digit > 9:
        digit -= 9
    total += digit
    double = not double
  return total % 10 == 0


def tokenize_by_bin_tail(
  fpan: str,
  bin_length: int,
  tail_length: int,
) → str:
  if not fpan.isdecimal() or not luhn_valid(fpan):
    raise ValueError("FPAN должен быть PAN с корректной цифрой Луна")
```

(продолжение)

```
    free_digits = len(fpan) - bin_length - tail_length
    if free_digits <= 0:
      raise ValueError("маска не оставляет места для случайной части")

    head = fpan[:bin_length]
    tail = fpan[-tail_length:] if tail_length else ""
    middle_prefix = "".join(str(secrets.randbelow(10)) for _ in range(free_digits - 1))

    for last in range(10):
      candidate = head + middle_prefix + str(last) + tail
      if luhn_valid(candidate):
        return candidate
    raise AssertionError("ровно одна цифра из десяти проходит Луна")
```

Корреляция утечек без знания PAN

Маска `(BIN, last4)` — детерминированная функция PAN без ключа. Один и тот же PAN у двух разных ТСП даёт одинаковые BIN и хвост; две независимые утечки баз токенов склеиваются по равенству маски без знания исходного PAN, без доступа к vault и без криптоанализа. Несвязываемость (*unlinkability*), ради которой токенизация существует как механизм защиты PAN, у такой схемы отсутствует по определению [168]. Вероятность случайного совпадения BIN и хвоста у двух независимых PAN равна 10^{-10} в равномерной модели.[1] Для одной известной маски и корпуса из 10^7 карт ожидаемое число ложных совпадений равно 10^{-3}; массовую склейку утечек ограничивает распределение BIN, потому что секретности в схеме уже нет.

Метаданные транзакций сокращают поиск

Yves-Alexandre de Montjoye и соавторы показали на трёхмесячном корпусе из 1,1 миллиона держателей карт, что четыре пары *(дата, торговая точка)* однозначно идентифицируют 90 % участников [183]. В их корпусе нет ни PAN, ни BIN, ни хвоста. Когда утечка добавляет к метаданным слепок `(BIN, last4)`, атакующий начинает с малой группы кандидатов по самой маске; дата и торговая точка нужны уже для редких совпадений после первичного поиска.

Допустимая роль маски

Сохранённые BIN и хвост — это *маска для отображения* (чек, письмо, интерфейс, уведомление в приложении), разрешённая PCI DSS 4.0.1 при условии, что больше нигде вне CDE PAN не хранится [70, 73]. Как *суррогат для хранения* такая конструкция не работает: по PCI DSS Tokenization Guidelines суррогат выводит систему из CDE только если необратим без доступа к vault и если сам vault изолирован [168]; маска `(BIN, last4)` не удовлетворяет ни одному из двух условий.

BIN и хвост в суррогате нужны для маршрутизации по карточной сети и диапазону карточного продукта без обращения к vault. Эту задачу решает справочная таблица BIN рядом с непрозрачным токеном из vault; сам суррогат остаётся случайным. Выбор зависит от назначения:

[1] Равномерная модель трактует все шестнадцать цифр PAN как независимые равномерные на $\{0, \ldots, 9\}$. Контрольная цифра Луна определена остальными пятнадцатью, поэтому last4 содержит три независимые цифры, а не четыре; на оценку 10^{-10} это не влияет, так как контрольная сумма распределена равномерно по своим префиксам. Реальные BIN неравномерно распределены по 10^6 комбинациям — сконцентрированы на действующих эмитентах, — и фактическая вероятность совпадения BIN на несколько порядков выше: 10^{-10} — нижняя оценка.

- для отображения — та же маска BIN и хвост, но без хранения средней части (короткая строка «BIN, четыре звёздочки, last4», не суррогат);
- для внутреннего vault — случайный непрозрачный токен без привязки к цифрам PAN, либо FPE FF1 на криптографическом ключе [175];
- для авторизационного потока — сетевой токен (DPAN или MPAN) через TSP сети [35].

9.9 Детокенизация и доступ к PAN

Эмитенту нужен настоящий PAN для авторизации. В модели EMVCo сетевой токен проходит от точки продажи до эмитента через звенья [35]:

- **продавец** отправляет транзакцию с сетевым токеном и не обязан хранить PAN карты;
- **эквайер / PSP** передаёт запрос дальше как обычную платёжную операцию, но уже в токенизированном виде;
- **токен-сервис сети / TSP** распознаёт токен, применяет ограничения токена и готовит запрос на авторизацию по PAN;
- **эмитент** получает запрос на авторизацию по PAN вместе с контекстом токена и может учесть, через какой сервис прошёл выпуск и насколько надёжно была подтверждена личность держателя карты.

Продавец передаёт эквайеру токен (DPAN из кошелька, см. раздел 8.3, либо MPAN *card-on-file*, см. раздел 9.4), срок действия токена, криптограмму (TAVV, Token Authentication Verification Value, криптограмма сетевого токена для e-commerce; бесконтактную криптограмму для NFC-кошелька) и свой MID. Пластиковая карта в этом маршруте не участвует: терминал читает с чипа настоящий FPAN, и авторизация идёт мимо TSP без детокенизации. Эквайер формирует авторизационный запрос (MTI 0100) и направляет его в карточную сеть. Сеть распознаёт диапазон BIN (Bank Identification Number, банковский идентификационный диапазон PAN) как принадлежащий токенам и маршрутизирует запрос в TSP. TSP проверяет статус токена (active, не suspended и не deleted), ограничение домена (канал запроса совпадает с разрешённым доменом, TRID и MID соответствуют записи выпуска) и валидность криптограммы. При успехе TSP извлекает из vault исходный FPAN (Funding PAN, исходный PAN, к которому привязан токен) и expiry, присоединяет Token Assurance Method и направляет детокенизированный запрос эмитенту. Эмитент видит FPAN и дополнительный контекст: через какой Token Requestor пришла операция и с каким уровнем проверки личность держателя карты была подтверждена при выпуске токена. Ответ эмитента возвращается через TSP, который заменяет FPAN обратно на токен, прежде чем передать ответ эквайеру, так что продавец не видит настоящий PAN. Значения на рис. 24 учебные: реальные Token BIN range у VTS, MDES и TSP НСПК — закрытая часть документации.

PAN восстанавливается там, где он нужен для авторизационного решения. Если токен приостановлен, удалён или вышел из допустимого состояния, транзакция не доходит до авторизации: состояние токена определяет исход операции по карте [35, 36].

Публичные документы EMVCo стандартизуют общую модель авторизации; детали клиринга и представления данных о токене задают правила конкретной сети, и из схемы EMVCo они не выводятся.

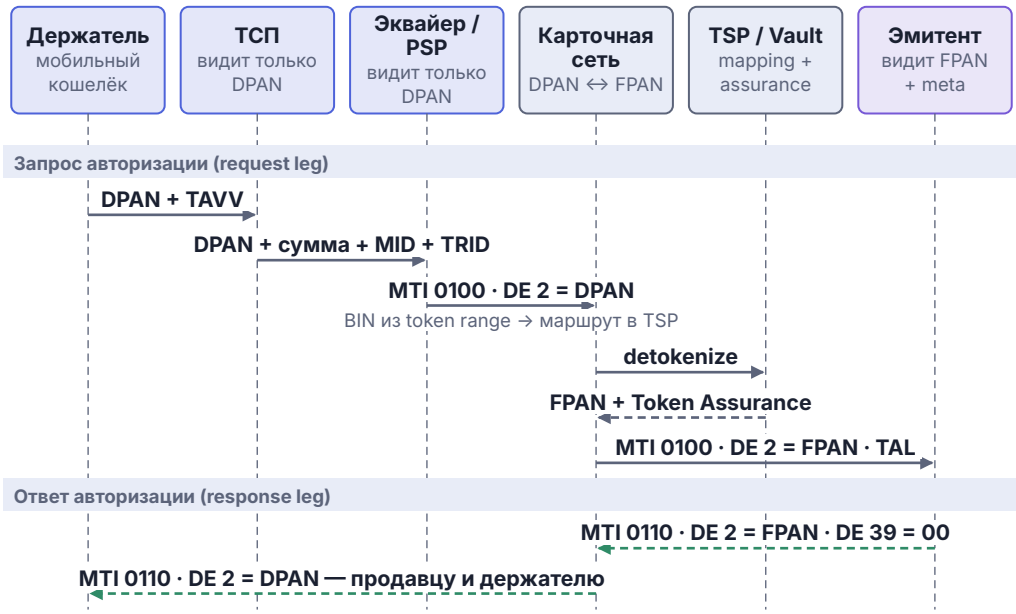


Рис. 24 — Токенизированная авторизация: подмена DPAN ↔ FPAN на стороне TSP.

Первый сценарий: TSP недоступен или отвечает с таймаутом. Карточная сеть не может детокенизировать запрос и возвращает эквайеру системный отказ. Отказывает общий TSP сети, поэтому смена эквайера не меняет результат: любой эквайер детокенизирует запрос через тот же TSP. ТСП может повторить запрос через короткий интервал или отправить транзакцию по FPAN, если тот доступен. Доступность FPAN — заранее принятое архитектурное решение: либо ТСП сам хранит FPAN и уже несёт полный периметр PCI DSS, либо FPAN хранит PSP, и тогда переход на FPAN выполняет PSP без последствий для периметра ТСП. ТСП, который видел только токен (кошелёк, iframe-интеграция PSP), перейти на FPAN не может.

Второй сценарий: токен приостановлен или удалён между моментом формирования запроса и его обработкой в TSP. Это возможно при блокировке карты, когда эмитент отправляет suspend, а транзакция в процессе обработки (*in-flight*) прошла через эквайера. TSP проверяет статус, видит suspended и отклоняет операцию: продавец получает отказ, хотя секундой ранее тот же токен работал.

Третий сценарий: подписочный MIT (*merchant-initiated transaction*, списание по инициативе ТСП). Карта перевыпущена, PAN изменился, и сетевой токен автоматически переключается на новый FPAN через обновление жизненного цикла. Если обновление ещё не завершилось к моменту очередного списания, TSP детокенизирует в старый FPAN, по которому эмитент уже выдаёт отказ из-за закрытой карты. После синхронизации проблема исчезает, но первое списание после перевыпуска может потребовать повтора через несколько часов.

Сквозная работа сетевого токена через нескольких эквайеров требует, чтобы все участники маршрута поддерживали поля токена и его ограничения по домену; иначе токен на одном из переходов преобразуется обратно в PAN или операция отклоняется.

В первых двух сценариях запрос с сетевым токеном останавливается на стороне TSP, в третьем отказ выдаёт эмитент; эквайер во всех трёх не получает PAN. Продавец после системного отказа TSP может повторить операцию по PAN, но рискует

двойным списанием после восстановления сервиса. В ISO 8583 идемпотентность повторов строится на комбинации RRN (DE 37) и STAN (DE 11) либо на Transaction Life Cycle Identifier из редакции 2003, а в PSP-API передаётся отдельный ключ идемпотентности (*idempotency key*), генерируемый клиентом.

Эквайер выделяет TSP-отказы (timeout, token suspended, domain mismatch) отдельной метрикой. Такие коды возвращаются в том же DE 39, что и отказы эмитента, но со специальными значениями (набор значений задаёт каждая сеть; плюс дополнительные поля сети, DE 44 и DE 62), поэтому от эмитентских их отличают по значению кода.

Эмитент сводит долю операций, не дошедших до авторизации из-за состояния токена, в ту же витрину, что и отказы по стоп-листу: для держателя карты результат один — карта числится рабочей, операция не прошла, — а корневая причина различна. Повторы после отказа разобраны в разделе 33.3.

Связь токенизации и 3-D Secure разобрана в разделе 11.8, влияние токенизации на периметр PCI DSS — в разделе 12.3, на антифрод — в гл. 29.

10 Криптография в платежах

Платёжная криптография отвечает на инженерные вопросы: что произойдёт, если из терминала утечёт ключ; почему нельзя хранить PIN в базе и сверять его программно; как карта и эмитент доверяют друг другу, если секреты нельзя раздать всем участникам расчёта.

10.1 Симметричная криптография: 3DES и AES

В симметричной криптографии один и тот же ключ используется для шифрования и расшифрования, поэтому отправитель и получатель заранее договариваются о секрете и хранят его в тайне. Платёжная индустрия исторически строилась на симметричных алгоритмах: они быстрые, компактные и хорошо подходят к задачам, где обе стороны находятся внутри одной доверенной инфраструктуры.

3DES

3DES, он же Triple DES или TDEA (Triple Data Encryption Algorithm), — тройное применение DES, разработанного в 1970-х годах. Одиночный DES с 56-битным ключом давно непригоден для практической защиты; тройное применение с двумя или тремя ключами повышает стойкость и сохраняет совместимость с парком устройств, рассчитанных на DES.

В платёжной инфраструктуре 3DES закрепился на многих критических участках. С его помощью рассчитывают CVV магнитной полосы (раздел 4.3), генерируют криптограмму ARQC (Authorization Request Cryptogram, см. раздел 7.8) на чипе, шифруют PIN-блок при онлайн-авторизации, вычисляют MAC (Message Authentication Code, имитовставка в отечественной терминологии) для защиты целостности ISO 8583-сообщений в канале между эквайером и сетью. За десятилетия он стал частью терминалов, HSM (Hardware Security Module, аппаратный модуль безопасности; подробно в разделе 10.3) и процессинговых систем. Его замена стала долгой и дорогой миграцией.

NIST с 1 января 2024 года отозвал SP 800–67 Rev. 2; после этого NIST не считает 3DES утверждённым блочным шифром, и он сохраняется лишь в ограниченных унаследованных сценариях: расшифрование, распаковка ключей и проверка MAC ранее защищённых данных [184, 185].

AES

AES (Advanced Encryption Standard) — блочный шифр, принятый NIST в 2001 году на замену DES [186]. Он работает с 128-битными блоками и поддерживает длину ключа 128, 192 или 256 бит. AES быстрее 3DES, требует меньше вычислительных ресурсов и даёт значительно больший запас стойкости для новых систем.

AES постепенно вытесняет 3DES в платёжной инфраструктуре. Новые терминалы и модули HSM поддерживают AES напрямую, но миграцию сдерживает обратная совместимость с унаследованным парком устройств.

MAC

MAC (Message Authentication Code) — значение, вычисляемое по содержимому сообщения на разделяемом секретном ключе. Получатель по нему проверяет, что сообщение не изменилось в пути и пришло от стороны, владеющей ключом. В ISO 8583 MAC размещают в DE 64 или DE 128 и используют для защиты авторизационного сообщения на участке между терминалом, эквайером и сетью.

В платёжной практике применяются CBC-MAC поверх 3DES или AES в режиме CBC (Cipher Block Chaining, сцепление блоков шифротекста) и более современный CMAC (Cipher-based MAC, NIST SP 800-38B) на AES. Выбор определяется поддержкой терминального парка и стороны эмитента.

10.2 Асимметричная криптография: RSA и ECC

Симметричная схема использует один общий ключ; асимметричная — пару: открытый ключ распространяется свободно, закрытый хранится в тайне. Данные, зашифрованные открытым ключом, расшифровываются только закрытым; подпись, созданная закрытым, проверяется открытым. Асимметрия устанавливает доверие между сторонами, которые заранее не обменивались секретами [30].

RSA в EMV

RSA остаётся базовым асимметричным алгоритмом в платёжной индустрии. В разделе 7.4 показано применение RSA для аутентификации данных на чипе. Карточная сеть выпускает сертификаты ключей, эмитент подписывает сертификат карты, терминал проверяет цепочку доверия по заранее загруженному открытому ключу корневого центра.

С момента появления EMV контактный чип опирался на RSA, а длины ключей EMVCo пересматривает ежегодными бюллетенями «RSA Key Lengths Assessment»: требования зависят от роли ключа, версии спецификации и текущего миграционного периода [187, 188]. Универсальная рекомендация «RSA-NNNN бит» быстро устаревает.

ECC

ECC (Elliptic Curve Cryptography) — семейство алгоритмов на эллиптических кривых. Основное преимущество перед RSA — сопоставимая стойкость при существенно меньшем размере ключа: открытый ключ P-256 в сжатой форме занимает 33 байта против 256 байт у RSA-2048 [189], сертификатная цепочка короче. На стороне карты выигрыш заметнее: подпись на чипе быстрее на порядок, а ключевой материал занимает меньше EEPROM. На стороне терминала ECC не выигрывает в скорости проверки: проверка подписи RSA с малой открытой экспонентой $e = 65\,537$ обходится примерно 17 модульными умножениями и работает в разы быстрее проверки ECDSA P-256. Узкое место EMV-транзакции — подпись внутри карты за короткое бесконтактное касание, и переход на ECC ускоряет именно её [187].

EMVCo официально добавил поддержку ECC в спецификации контактного чипа [187]. В ПС Мир подпись на эллиптических кривых по ГОСТ 34.10–2018 применяется к клиринговым файлам (раздел 10.3) [190]. Переход с RSA идёт постепенно: терминалы, карты и сертификационные цепочки должны одновременно поддерживать старый и новый набор алгоритмов.

Постквантовая криптография

В августе 2024 года NIST выпустил первые стандарты постквантовой криптографии: FIPS 203 (ML-KEM, инкапсуляция ключа на основе Kyber), FIPS 204 (ML-DSA, подпись на основе Dilithium) и FIPS 205 (SLH-DSA, подпись на хеш-функциях) [191—193]. Квантовый компьютер угрожает платёжной криптографии неравномерно. Алгоритм Шора ломает асимметрику — RSA и ECC; алгоритм Гровера лишь квадратично ослабляет симметрику, и удвоения длины ключа достаточно, чтобы криптограмма и MAC устояли. Поэтому онлайн-авторизация EMV, где карта и эмитент доверяют друг другу через симметричную криптограмму, по существу квантово-устойчива. Под угрозой офлайн-аутентификация данных карты (SDA, DDA, CDA) и сертификатные цепочки на RSA и ECC — тот самый участок, где переход от RSA к ECC ещё не завершён, а NIST уже стандартизовал следующую замену.

Атака «собрать сейчас, расшифровать потом» (*harvest now, decrypt later*) для чиповой транзакции малосущественна: динамическая криптограмма одноразова, а симметричные ключи карты не переносятся под RSA, поэтому из перехвата нечего извлечь задним числом [194]. EMVCo в заявлении о своей позиции оценивает практический горизонт угрозы консервативно — не ранее 2040 года [194, 195]; Mastercard в докладе 2025 года выделяет криптографическую гибкость (смену алгоритма без переписывания систем) [196] и с 2022 года одобряет для эмитентов квантово-устойчивые бесконтактные карты по спецификации Enhanced Contactless [197]. PCI DSS 4.0 уже требует инвентаризации используемых шифронаборов и протоколов и их пересмотра; это готовит ту же гибкость, но постквантовых требований не вводит. Первые платёжные HSM с ML-KEM и ML-DSA и валидацией PCI HSM Futurex объявила в июне 2025 года [198]. Двойной стек ГОСТ (раздел 10.9) уже показывает, как инфраструктура поддерживает два набора алгоритмов одновременно; постквантовый переход потребует того же приёма для RSA и ECC. Конкретные даты, как и с Format 4 (раздел 10.7), в код закладывать не стоит.

10.3 HSM

Любой криптографический алгоритм стоек ровно настолько, насколько защищён его ключ. Если ключ хранится файлом на сервере, его можно извлечь вместе с дампом памяти или резервной копией. HSM — физически защищённое устройство, в котором ключевой материал остаётся внутри корпуса, а наружу передаётся только результат операции.

Программная реализация теряет ключ из оперативной памяти через дамп процесса, через *cold-boot*-атаку (извлечение ключей из ОЗУ после быстрого охлаждения модулей и аварийной перезагрузки) или через доступ DMA с вредоносного PCIe-устройства. Каждый путь обходит алгоритм: хватает физического или привилегированного доступа к машине.

HSM проектируют так, чтобы он противостоял физическим атакам: корпус обнаруживает вскрытие, внутренние цепи защищают ключи от считывания, побочные каналы минимизированы. Физическую прочность удостоверяет формальная сертификация. FIPS 140–3 (серия стандартов NIST для криптографических модулей) описывает четыре уровня безопасности. Поверх FIPS Совет PCI SSC ведёт PCI PTS HSM — требования к модулям, обрабатывающим PIN. Сам платёжный HSM сертифицируют по FIPS 140–3 и PCI PTS HSM, а PCI PIN оценивает среду организации, в которой модуль работает [199—201].

Верификация криптограммы ARQC при онлайн-авторизации целиком проходит внутри HSM: эмитент или его процессор передаёт данные транзакции в модуль, а HSM деривирует сессионный ключ из мастер-ключа эмитента, вычисляет ожидаемую криптограмму и сравнивает с полученной. Тот же модуль генерирует ARPC (Authorization Response Cryptogram, ответная криптограмма эмитента), проверяет PIN, расшифровывая PIN-блок и сверяя его с эталоном без выпуска PIN наружу, перешифровывает PIN-блок между зонами безопасности, генерирует и проверяет CVV/CVV2, готовит ключи при персонализации карт и вычисляет MAC для защиты ISO 8583-сообщений.

Маршрут ARQC от терминала до хоста эмитента показан на рис. 25. HSM эквайера хранит TPK/ZPK под LMK и перешифровывает PIN-блок из TPK под ZPK (команда Thales payShield `CA`, ответ `CB`); зональный HSM перешифровывает PIN-блок при смене ZPK (`CC`/`CD`). HSM эмитента проверяет CVV (`CY`/`CZ`; `CW`/`CX` генерирует CVV при выпуске), деривирует MK_AC из IMK-AC по PAN+PSN, затем сессионный SK_AC по ATC, верифицирует ARQC и генерирует ARPC методом 1: ARPC = 3DES(SK_AC, ARQC XOR ARC) (команда `KQ`, ответ `KR`). Деривация сессионного ключа — из Common Session Key Derivation, Annex A1.3 EMV Book 2 [30]; команды — из Thales payShield Host Programmer's Manual [202] (это отдельный документ от «Legacy Host Commands» с другим набором команд: AA, AE, CI, JS); публичная сводка соответствий — у EFTlab [203].

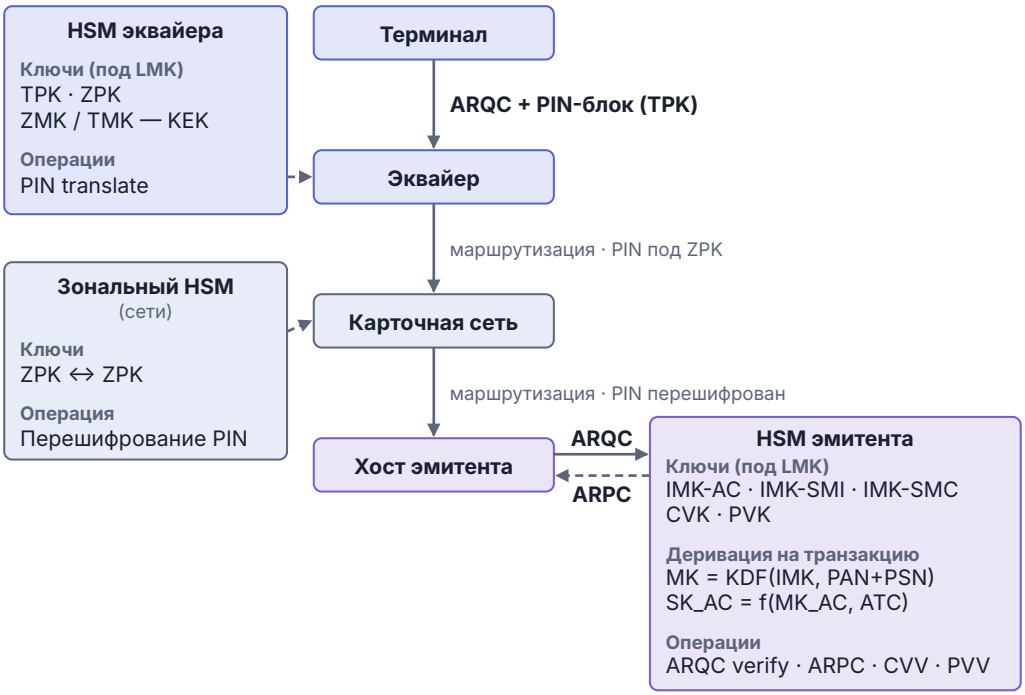


Рис. 25 — HSM в авторизационном потоке ARQC/ARPC: эквайер, зональный узел, эмитент.

В промышленной инфраструктуре HSM включают в отказоустойчивый пул, обслуживающий авторизацию, персонализацию и процессинг PIN. Пул требует собственного планирования ёмкости и церемонии ключа, но узким местом задержки не становится: обращение к HSM занимает единицы миллисекунд (см. раздел 37.2).

ПРАКТИКА

При отказе HSM авторизация останавливается. Без доступа к мастер-ключу нельзя ни деривировать сессионный ключ, ни верифицировать ARQC. Типовая схема — кластер *active-active* из двух HSM с синхронизированными ключами и регулярной проверкой того, что оба устройства дают одинаковый результат на контрольной операции.

HSM эмитента карт «Мир»

Российский эмитент карт «Мир» работает по той же модели HSM, но в другой нормативной среде и с гибридной криптографией. Требования к функциям модуля закреплены в Функционально-технических требованиях Банка России от 28.02.2020 № ФТ-56-3/35 «Аппаратный модуль безопасности (HSM)» [204]: поддержка ARQC/ARPC по EMV CSK, MAC по ГОСТ 34.12/34.13, форматы PIN-блока ISO 9564 0, 1, 3 и 4. Положения 821-П [205] и 851-П [206] требуют применять СКЗИ, сертифицированные ФСБ. Например, ViPNet HSM сертифицирован как СКЗИ класса КВ и средство ЭП класса КВ2 по Приказу ФСБ России от 27.12.2011 № 796 «Требования к средствам ЭП и УЦ» [207]; приказ действует до 01.01.2027 [208].

В открытых источниках для российских эмитентов указаны сертифицированные модели: КриптоПро HSM 2.0 R3 с Платёжным модулем [209], ViPNet HSM PS [210] и SPB HSM PS [211]. Все три поддерживают одновременно и ГОСТ 34.10/34.11/34.12/34.13, и 3DES/AES/RSA, потому что карта «Мир» использует гибридную схему: онлайн-криптограммы ARQC рассчитываются по 3DES CSK, а ГОСТ применяется для MAC канала с НСПК (на ZAK) и для подписи клиринговых файлов с УЦ ПС Мир. Хост-API у всех трёх вендоров эмулирует формат Thales payShield для совместимости с устоявшимся процессинговым ПО — SmartVista, TranzWare, Way4.

Российская схема отличается от международной сертификацией (ФСБ вместо FIPS 140–3), MAC канала (ГОСТ 34.13 вместо ISO 9797-1 alg. 3) и подписью клиринговых файлов (ГОСТ 34.10–2018 + Стрибог). Публичная часть Программы безопасности ПС Мир [49] конкретный список рекомендованных моделей HSM не раскрывает.

Таблица 25 — HSM эмитента карт «Мир» и международная схема: сертификация, ключи, MAC, подпись клиринговых файлов

Операция	Международная сеть (Visa, Mastercard, Amex)	ПС Мир (НСПК, банки-эмитенты)
Норматив	PCI SSC, scheme rules	ЦБ 821-П, 851-П, ФСБ № 796
Сертификация HSM	FIPS 140-3 L3–L4, PCI PTS HSM	ФСБ: СКЗИ КВ, ЭП КВ2 + реестр Минпромторга
LMK (корневой)	AES / 3DES	AES / 3DES, опц. Кузнечик
Зональный ключ к ПС	ZMK Visa/MC (3DES / AES)	ZAK НСПК (ГОСТ 34.12/34.13)
PIN-блок (ZPK)	ISO 9564 F0, 3DES / AES	F0 (3DES), F4 опц., Кузнечик опц.
Online ARQC / ARPC	EMV CSK на 3DES / AES	EMV CSK на 3DES (ГОСТ не активирован)
MAC канала с ПС	3DES-MAC, ISO 9797-1 alg. 3	ГОСТ-MAC по ГОСТ 34.13
ЭП клир. файлов и хеш	RSA / ECDSA + SHA-2	ГОСТ 34.10-2018 + Стрибог
Хост-API HSM	Thales A0 / JA / KQ …	Thales-эмуляция + PKCS#11 GOST
Offline auth (SDA/DDA/CDA)	RSA, сертификат CA сети	RSA, сертификат CA НСПК

Российские платёжные HSM, три вендора в эмиссионной инфраструктуре Мир: КриптоПро HSM 2.0 R3, ViPNet HSM PS, SPB HSM PS.

10.4 Иерархия ключей

Если бы эмитент использовал один и тот же секрет для всех карт и всех транзакций, компрометация одного узла обернулась бы системной аварией. Поэтому ключи в платёжной криптографии организуют в иерархию — дерево, где каждый уровень порождает ключи следующего через деривацию. Компрометация ключа нижнего уровня не должна нарушать работу всей системы [212].

Без деривации эмитент хранил бы N независимых случайных ключей, по одному на каждую карту. При ста миллионах карт это сто миллионов записей в HSM; при смене оборудования или восстановлении из резервной копии пришлось бы переносить все записи. Деривация устраняет обе проблемы. Один IMK детерминированно воспроизводит ключ любой карты, без дополнительного хранения и без передачи ключей между системами.

Иерархия ключей эмитента в EMV:

- **мастер-ключ (Issuer Master Key, IMK)** — секретный ключ эмитента, хранящийся исключительно в HSM. Для каждого типа операции может существовать отдельный мастер-ключ. IMK-AC отвечает за криптограммы, IMK-SMI — за Secure Messaging Integrity (целостность команд эмитента к чипу, *issuer scripts*), IMK-SMC — за Secure Messaging Confidentiality (конфиденциальность тех же команд, например при удалённой смене PIN).
- **ключ карты (*UDK, Unique Derivation Key*)** — выводится из мастер-ключа по PAN и порядковому номеру карты (PAN Sequence Number, PSN); в терминологии EMV Book 2 и Mastercard тот же ключ называется ICC Master Key (MK_AC). Ключ карты записывается в чип при персонализации.
- **сессионный ключ (Session Key)** — производный от ключа карты через ATC (Application Transaction Counter) как диверсификатор. Сессионный ключ уникален для каждой транзакции и используется для вычисления криптограммы.

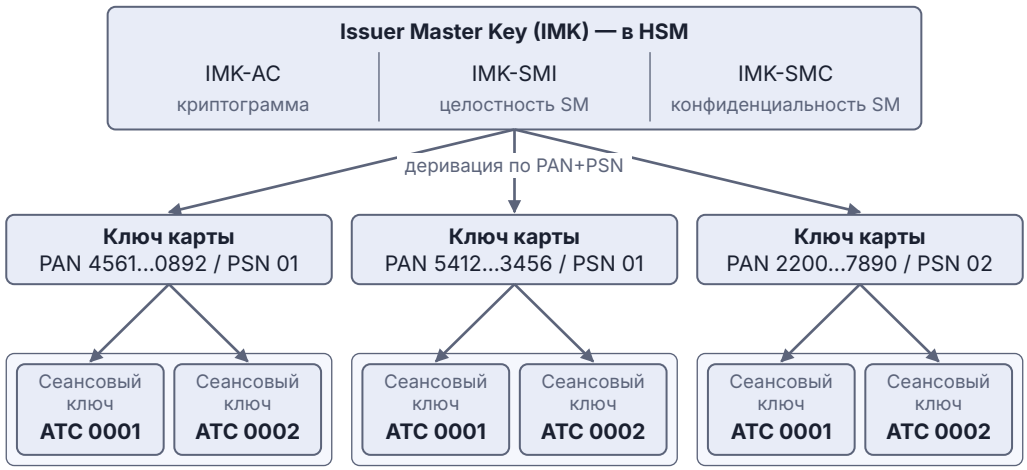


Рис. 26 — Дерево деривации EMV: IMK, ключ карты, сессионный ключ.

Деривация работает как односторонняя функция: зная мастер-ключ, вычисляют ключ любой карты; зная ключ карты, вычисляют сессионный ключ для любого ATC. Обратная операция невозможна, поэтому компрометация сессионного ключа одной транзакции не восстанавливает ни ключ карты, ни мастер-ключ. Компрометация ключа одной карты не раскрывает ключи других, поскольку деривация по PAN даёт разные результаты для разных номеров [30].

Компрометация мастер-ключа разрушает иерархию: все карты эмитента оказываются скомпрометированы разом. Мастер-ключ никогда не покидает HSM в открытом виде и загружается при начальной настройке через формальную процедуру Key Ceremony (раздел 10.8).

Деривация на практике: UDK и сессионный ключ

EMV задаёт иерархию ключей точными формулами. Ключ карты UDK (Unique Derivation Key) эмитент выводит из мастер-ключа IMK по PAN и порядковому номеру карты PSN (EMV Book 2, Annex A1.4, Option A для PAN до 16 цифр) [30]. Пусть Y — 16 младших цифр конкатенации PAN и PSN, упакованные в 8 байт; тогда

$$\mathrm{UDK}_L = \mathrm{3DES}_{\mathrm{IMK}}(Y), \qquad \mathrm{UDK}_R = \mathrm{3DES}_{\mathrm{IMK}}(\overline{Y}),$$

где $\overline{Y}$ — побитовое дополнение Y (XOR с $\mathtt{FF}\ldots\mathtt{FF}$), а $\mathrm{UDK} = \mathrm{UDK}_L \,\|\, \mathrm{UDK}_R$ после коррекции на нечётную чётность DES. Дополнение делает половины ключа различными: при одинаковом входе они иначе совпали бы. Для PAN длиннее 16 цифр (Option B) Y получают децимализацией SHA-1 от PAN и PSN; остальная формула не меняется.

Сессионный ключ выводится из UDK по счётчику ATC (EMV Common Session Key, Annex A1.3) [30]. Левая и правая половины различаются служебным байтом `F0` и `0F`:

$$\mathrm{SK}_L = \mathrm{3DES}_{\mathrm{UDK}}(\mathrm{ATC} \,\|\, \mathtt{F0} \,\|\, 00\,00\,00\,00\,00), \quad \mathrm{SK}_R = \mathrm{3DES}_{\mathrm{UDK}}(\mathrm{ATC} \,\|\, \mathtt{0F} \,\|\, 00\,00\,00\,00\,00),$$

$\mathrm{SK} = \mathrm{SK}_L \,\|\, \mathrm{SK}_R$, снова с коррекцией чётности. Уникальный ATC в каждой операции даёт уникальный сессионный ключ; им же карта считает MAC криптограммы ARQC.

Версия криптограммы определяет, нужен ли этот второй шаг: CVN 10 берёт UDK сессионным ключом напрямую, CVN 18 — выводит SK по ATC формулой выше.

Единственный примитив обеих дериваций — блок 3DES в ECB (плюс коррекция на нечётную чётность DES):

```
from cryptography.hazmat.decrepit.ciphers.algorithms import TripleDES
from cryptography.hazmat.primitives.ciphers import Cipher, modes

_COMPLEMENT = b"\xff" * 8  # маска XOR для правой половины UDK (Option A)


def des3_ecb_block(key: bytes, block: bytes) → bytes:
  """Один блок 3DES (TDEA) в ECB -- единственный примитив деривации EMV.
  Ключ 16 байт (double-length), блок 8 байт."""
  assert len(key) == 16 and len(block) == 8
  enc = Cipher(TripleDES(key), modes.ECB()).encryptor()
  return enc.update(block) + enc.finalize()


def adjust_parity(key: bytes) → bytes:
  """Нечётная чётность DES: младший бит каждого байта -- бит чётности."""
  out = bytearray(key)
  for i, b in enumerate(out):
    if bin(b).count("1") % 2 == 0:
      out[i] = b ^ 1
  return bytes(out)
```

Из него по два вызова 3DES складываются ключ карты и сессионный ключ, без хранения состояния между транзакциями:

```
def derive_udk(imk: bytes, pan: str, psn: str = "00") → bytes:
  """IMK + PAN + PAN Sequence Number → ключ карты UDK.
  EMV Book 2, Annex A1.4, Option A (PAN до 16 цифр). Для длинных PAN --
  Option B: Y получается децимализацией SHA-1 от PAN||PSN, далее без изменений."""
  digits = (pan + psn)[-16:].rjust(16, "0")  # 16 младших цифр, дополнение слева
  y = bytes.fromhex(digits)  # 8 байт BCD
  left = des3_ecb_block(imk, y)
  right = des3_ecb_block(imk, bytes(a ^ b for a, b in zip(y, _COMPLEMENT,
     strict=True)))
  return adjust_parity(left + right)


def derive_session_key(udk: bytes, atc: bytes) → bytes:
  """UDK + ATC → сессионный ключ SK (EMV Common Session Key, Book 2, A1.3).
  Левая половина ветвится байтом 'F0', правая -- '0F'; остальные байты нулевые."""
  assert len(atc) == 2
  left = des3_ecb_block(udk, atc + b"\xf0" + b"\x00" * 5)
  right = des3_ecb_block(udk, atc + b"\x0f" + b"\x00" * 5)
  return adjust_parity(left + right)
```

На сессионном ключе считается сама криптограмма: `arqc()` — это Retail MAC (ISO 9797-1, алгоритм 3, метод дополнения 2) поверх данных транзакции (EMV Book 2, Annex A1.2):

```
def _des_ecb_block(key: bytes, block: bytes) → bytes:
  """Один блок одинарного DES в ECB (ключ 8 байт)."""
  assert len(key) == 8 and len(block) == 8
  enc = Cipher(TripleDES(key), modes.ECB()).encryptor()
  return enc.update(block) + enc.finalize()


def _pad_method2(data: bytes) → bytes:
  """ISO/IEC 9797-1 padding method 2: добавить 0x80, затем 0x00 до кратности 8."""
  data += b"\x80"
  while len(data) % 8:
    data += b"\x00"
  return data


def _xor8(a: bytes, b: bytes) → bytes:
```

(продолжение)

```
    return bytes(x ^ y for x, y in zip(a, b, strict=True))

def arqc(session_key: bytes, data: bytes) → bytes:
    """Криптограмма EMV (ARQC/TC/AAC): Retail MAC по ISO/IEC 9797-1 алгоритм 3
    поверх данных транзакции на сессионном ключе (EMV Book 2, Annex A1.2).
    CBC одинарным DES на левой половине ключа, финальный блок -- 2-key 3DES."""
    assert len(session_key) == 16
    kl, kr = session_key[:8], session_key[8:]
    blocks = _pad_method2(data)
    h = bytes(8)
    for i in range(0, len(blocks) - 8, 8):
        h = _des_ecb_block(kl, _xor8(blocks[i : i + 8], h))
    return des3_ecb_block(kl + kr, _xor8(blocks[-8:], h))
```

На эталонном векторе цепочка сходится целиком: мастер-ключ IMK `9E15...AD29` даёт UDK `4519...62FD`, из него по ATC `007C` — сессионный ключ, а Retail MAC над данными транзакции — ARQC `43 C1 14 60 F9 14 64 00`. Это та же криптограмма, что в поле `9F26` разобранного DE 55 (гл. 7, раздел 7.8); `test_de55.py` проводит всю цепочку от IMK до этой криптограммы и сверяет результат байт в байт.

Односторонность та же, что у DUKPT ниже: зная IMK, эмитент в HSM повторяет UDK и сессионный ключ любой карты, а вычислить IMK по производным ключам мешает стойкость 3DES.

10.5 Secure Messaging: защита сценариев эмитента

Сценарии эмитента (*issuer scripts*) меняют состояние уже выпущенной карты: сбрасывают счётчик попыток PIN, блокируют приложение, изменяют параметры. Карта принимает такую команду только после доказательства, что её написал именно эмитент. Это доказательство даёт Secure Messaging (EMV Book 2, §9) [30].

Каждая команда сценария передаётся в теге `0x86` с MAC в конце. MAC считается на сессионном ключе SK_SMI — производном от IMK-SMI той же деривацией, что и ключ криптограммы, — поверх заголовка APDU и данных команды. Карта выводит SK_SMI из своего ключа, пересчитывает MAC и сверяет; при несовпадении отвергает команду. IMK-SMI держит только эмитент, поэтому подделать принимаемый картой сценарий нельзя, а привязка к ATC не позволяет повторить старую команду в новой сессии.

Когда команда несёт секрет — например, новый PIN в `PIN CHANGE`, — её данные дополнительно шифруются на SK_SMC (от IMK-SMC). Гарантии разведены по ключам: SK_SMI отвечает за «команду не подменили», SK_SMC — за «содержимое не прочитали». По младшему ниблу класса CLA (C или 4) карта различает форматы защищённой команды: Format 1 несёт данные как BER-TLV, Format 2 — без TLV-обёртки; набор полей под MAC у них отличается.

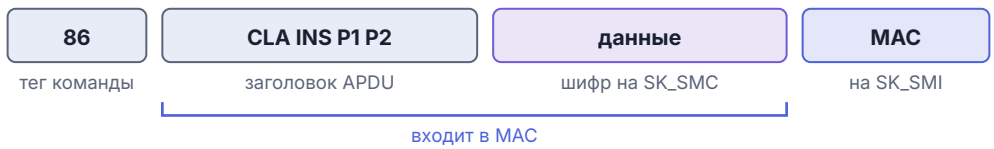


Рис. 27 — Защищённая команда эмитента: MAC на SK_SMI, шифр данных на SK_SMC.

10.6 DUKPT

Иерархия ключей EMV (мастер-ключ → ключ карты → сессионный ключ) хорошо работает для чиповых карт, где ключевой материал защищён внутри чипа. POS-терминал, в отличие от чипа, размещён в торговой точке: его можно украсть, разобрать и попытаться извлечь ключ из памяти. Если терминал хранит мастер-ключ и деривирует из него сессионные ключи по счётчику, кража одного терминала раскрывает всю иерархию.

DUKPT (Derived Unique Key Per Transaction) — схема управления ключами, разработанная для этой задачи. В актуальной редакции ANSI X9.24–3 она описана как AES DUKPT, в которой Base Derivation Key (BDK) порождает уникальные начальные ключи устройств, а из них по номеру транзакции выводятся рабочие ключи отдельных операций [213]. Ключевое свойство схемы: одноразовость транзакционных ключей. Компрометация текущего ключа не даёт вычислить ключи прошлых операций.

Без DUKPT терминал запрашивал бы свежий ключ с сервера на каждую транзакцию. Для POS в торговой точке это неприемлемо: терминал должен работать при нестабильном или временно отсутствующем соединении. Терминал с DUKPT деривирует ключ автономно из локального счётчика, без обращения к серверу в момент транзакции:

- центральная система хранит BDK (Base Derivation Key) — корневой ключ, из которого деривируются ключи для всех терминалов;
- при инициализации терминала из BDK выводится уникальный начальный ключ конкретного устройства;
- из этого начального ключа по номеру транзакции терминал выводит рабочий ключ отдельной операции;
- после использования транзакционный ключ стирается и больше не применяется.

AES DUKPT строится в два шага деривации. Эквайер хранит в HSM 128-битный BDK. При инициализации терминала с идентификатором Initial Key ID (IKI, 8 байт) HSM вычисляет начальный ключ устройства Initial Key (IK) одним блоком AES в режиме ECB:

$$\mathrm{IK} = \mathrm{AES\text{-}ECB}_{\mathrm{BDK}}(\mathrm{DD}_{\mathrm{init}}),$$

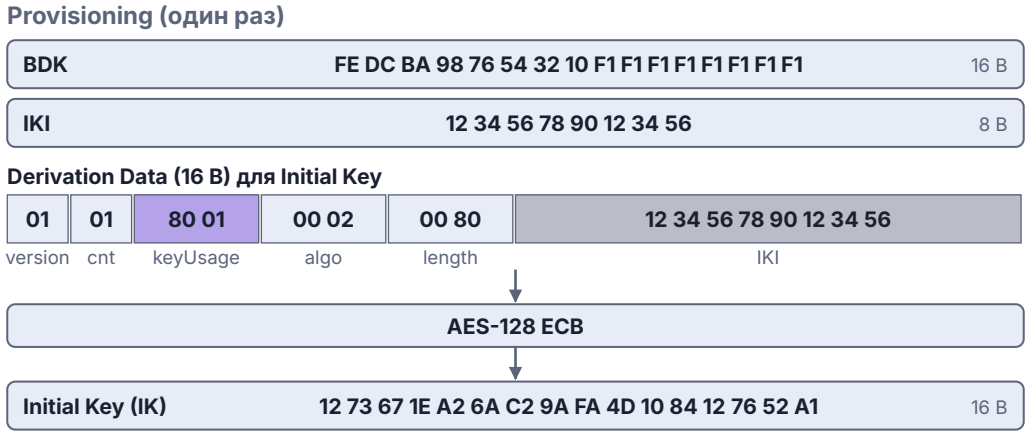


Рис. 28 — AES DUKPT по ANSI X9.24–3–2017, provisioning: деривация Initial Key из BDK.

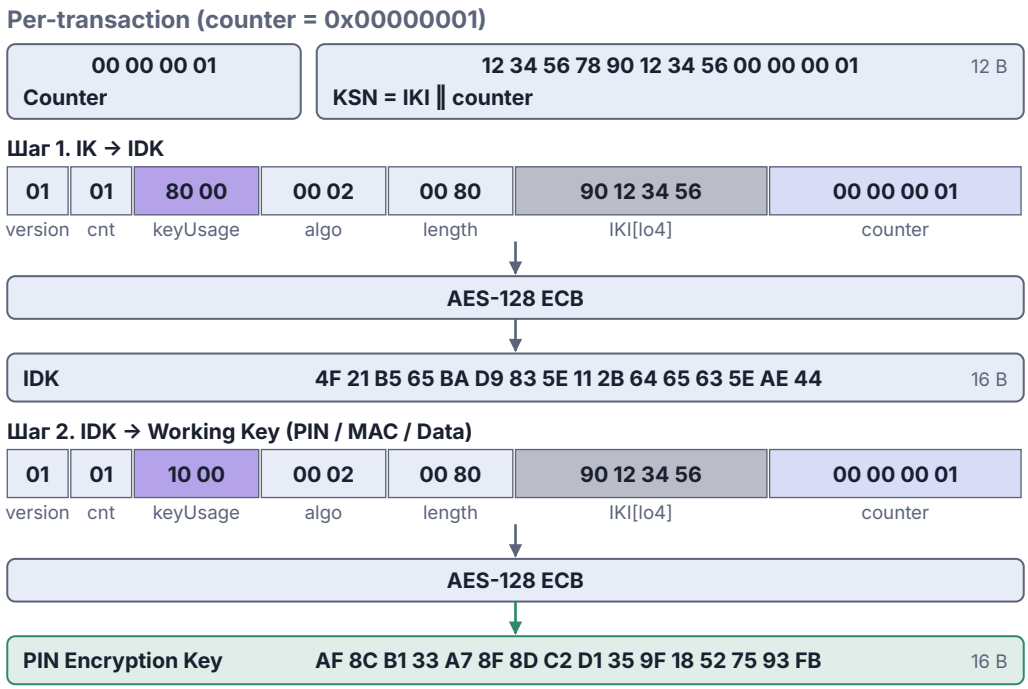


Рис. 29 — AES DUKPT по ANSI X9.24–3–2017, per-transaction: деривация IDK из IK и Working Key из IDK.

где $\mathrm{DD}_{\mathrm{init}}$ — 16-байтовая структура *derivation data* со служебными полями (*version*, *key usage* = `0x8001` для Initial Key, *algorithm* = AES-128, *length* = 128) и младшими 8 байтами, равными IKI [213]. Терминал получает только IK; BDK в терминал не попадает и существует только в HSM.

Затем используется 32-битный счётчик транзакций (*transaction counter*). Терминал держит 32 регистра промежуточных ключей Intermediate Derivation Key (IDK) — по одному на каждую позицию бита счётчика. Рабочий ключ конкретной операции выводится из соответствующего IDK ещё одним шагом AES-ECB с другими данными деривации:

$$\text{Working Key} = \text{AES-ECB}_{\mathrm{IDK}}(\mathrm{DD}_{\mathrm{wk}}),$$

где *key usage* в $\mathrm{DD}_{\mathrm{wk}}$ равно `0x1000` для ключа шифрования PIN, `0x2000` — для MAC, `0x3000` — для шифрования данных [213]. После транзакции счётчик инкрементируется, набор IDK перестраивается под новые установленные биты, а использованный рабочий ключ стирается. Серверная сторона (хост эквайера или платёжная сеть), зная BDK и полученный с транзакцией Key Serial Number $\mathrm{KSN} = \mathrm{IKI} \,\|\, \mathrm{counter}$ (12 байт), повторяет ту же цепочку деривации и получает тот же рабочий ключ, не храня промежуточного состояния.

Компрометация рабочего ключа транзакции N не раскрывает прошлые операции. AES-ECB необратима без ключа, а IDK прошлых позиций счётчика стираются при инкременте и больше не хранятся на устройстве. Атакующий с украденным терминалом получает текущие IDK, из которых выводятся только будущие рабочие ключи; прошлые ключи невосстановимы. Значения счётчика, в которых установлено больше 16 бит, пропускаются, поэтому ресурс устройства — порядка $2{,}4 \cdot 10^9$

транзакций; после его исчерпания терминал требует повторной инициализации с новым IK [213].

В примере все три шага деривации реализованы в одном файле; функция `make_derivation_data` строит 16-байтовый блок по разметке из рис. 28 и 29, а `aes_ecb_block` — единственный криптографический примитив:

```
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes

# keyUsage codes из X9.24-3 sec.6.3.3
KU_INITIAL_KEY = 0x8001
KU_DERIVATION_KEY = 0x8000  # Intermediate Derivation Key (IDK)
KU_PIN_ENCRYPTION = 0x1000
KU_MAC_GENERATION = 0x2000
KU_DATA_ENCRYPTION = 0x3000

_ALG_AES128 = 0x0002
_KEY_LENGTH_AES128 = 0x0080  # 128 бит
_VERSION = 0x01
_BLOCK_COUNTER = 0x01


def make_derivation_data(key_usage: int, payload: bytes) → bytes:
  """Собрать 16-байтовый блок derivation data по X9.24-3 sec.6.3.
  Поле payload -- либо InitialKeyID целиком (для Initial Key),
  либо последние 4 байта IKI плюс 4 байта transaction counter
  (для IDK и working keys).
  """
  assert len(payload) == 8
  return (
    bytes([_VERSION, _BLOCK_COUNTER])
    + key_usage.to_bytes(2, "big")
    + _ALG_AES128.to_bytes(2, "big")
    + _KEY_LENGTH_AES128.to_bytes(2, "big")
    + payload
  )


def aes_ecb_block(key: bytes, block: bytes) → bytes:
  """Один блок AES-128 ECB -- единственный примитив деривации в AES DUKPT."""
  assert len(key) == 16 and len(block) == 16
  enc = Cipher(algorithms.AES(key), modes.ECB()).encryptor()
  return enc.update(block) + enc.finalize()


def derive_initial_key(bdk: bytes, iki: bytes) → bytes:
  """BDK + InitialKeyID → Initial Key. Однократно при настройке терминала."""
  assert len(iki) == 8
  return aes_ecb_block(bdk, make_derivation_data(KU_INITIAL_KEY, iki))


def derive_idk(initial_key: bytes, iki: bytes, counter: int) → bytes:
  """Initial Key + counter → Intermediate Derivation Key для данной
     counter-позиции."""
  payload = iki[4:] + counter.to_bytes(4, "big")
  return aes_ecb_block(initial_key, make_derivation_data(KU_DERIVATION_KEY, payload))


def derive_working_key(idk: bytes, iki: bytes, counter: int, key_usage: int) → bytes:
  """IDK + назначение (PIN / MAC / Data) → одноразовый working key транзакции."""
  payload = iki[4:] + counter.to_bytes(4, "big")
  return aes_ecb_block(idk, make_derivation_data(key_usage, payload))
```

Получение рабочего ключа для конкретной транзакции — последовательность вызовов без хранения промежуточного состояния:

```
  ik = derive_initial_key(bdk, iki)
  idk = derive_idk(ik, iki, counter)
  pin_key = derive_working_key(idk, iki, counter, KU_PIN_ENCRYPTION)
```

На официальных векторах из Supplement to X9.24–3–2017 [214] эти три вызова возвращают значения, приведённые на рис. 28 и 29. Замена `KU_PIN_ENCRYPTION` на `KU_MAC_GENERATION` или `KU_DATA_ENCRYPTION` даёт независимый рабочий ключ того же IDK для других операций (*key separation*).

10.7 Онлайн PIN-блок: форматы ISO 0, 1, 3, 4

Когда держатель карты вводит PIN на клавиатуре терминала для онлайн-авторизации, его нужно передать так, чтобы ни терминал, ни промежуточные узлы не хранили PIN в открытом виде дольше необходимого. Для этого PIN упаковывают в PIN-блок: структурированное значение длиной 8 байт для унаследованных форматов или 16 байт для Format 4 на основе AES, готовое к передаче по сети без раскрытия PIN. Затем его шифруют ключом терминала или зональным ключом и отправляют в DE 52 авторизационного сообщения. Стандарт ISO 9564 определяет несколько форматов PIN-блока. В платёжной практике используются унаследованные форматы 0, 1, 3 и AES-формат 4 [215]. Все четыре относятся к онлайн-сценарию — передаче PIN-блока в авторизационном сообщении. Format 2 предназначен для офлайн-проверки EMV и здесь не рассматривается.

Format 0 (ISO 9564 Format 0)

Самый распространённый унаследованный формат. Он привязывает PIN к PAN: один и тот же PIN даёт разные блоки на разных картах, что усложняет словарный перебор по базе перехваченных шифротекстов.

Сборка показана на рис. 30 на примере PIN = 1234 и тестового PAN Stripe 4242424242424242 [216]: PIN и PAN упаковываются в два 8-байтовых поля (по 16 ниблов), которые XOR-ятся в итоговый блок. PIN-поле — формат-идентификатор `0`, длина PIN, цифры PIN, заполнитель `F`. PAN-поле — четыре нибла нуля, далее правые 12 цифр PAN без контрольной цифры (*check digit*). Результат XOR — 8-байтовый блок, готовый к шифрованию ключом PEK (PIN Encryption Key) [215].

Та же привязка снижает безопасность при утечке PAN. Если PAN есть в тех же логах, восстановить PIN из перехваченного PIN-блока проще. При смене PAN, например при перевыпуске карты, PIN-блок меняется, даже если сам PIN остался прежним.

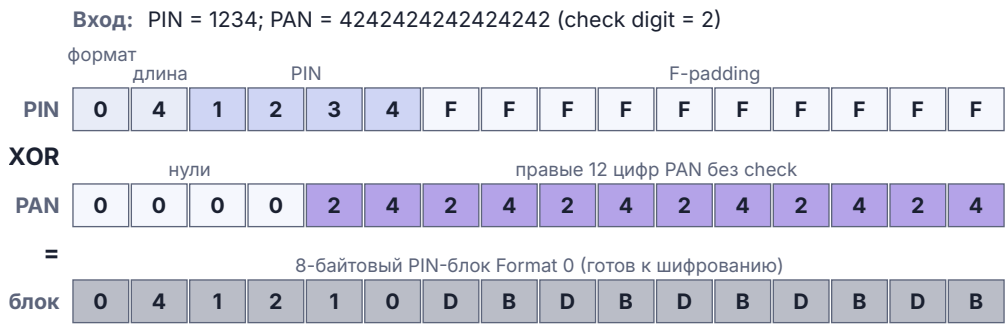


Рис. 30 — Сборка PIN-блока Format 0: PIN-поле, PAN-поле, XOR двух полей.

Format 1 и Format 3

Format 1 шифрует PIN без привязки к PAN и в карточных потоках встречается заметно реже, чем Format 0 и Format 3.

Format 3 остаётся унаследованным форматом, но снижает повторяемость блока: вместо постоянного заполнителя использует переменные значения, и одинаковые PIN и PAN дают разные выходы в разных транзакциях. Это ослабляет статистические атаки на перехваченные блоки [215].

Format 4 (AES)

Format 4 заменяет 3DES-логику PIN-блока на AES для новых систем [215].

ВАЖНО

Процессинг должен одновременно поддерживать AES и унаследованный 3DES; сроки PCI PIN Security пересматриваются [217, 218] — не закладывайте даты в код.

Перешифрование PIN-блока (PIN translation)

Когда PIN-блок передаётся между зонами безопасности (например, от эквайера к карточной сети и далее к эмитенту), каждый участник использует свой ключ шифрования. На каждом стыке зон HSM выполняет перешифрование PIN-блока: расшифровывает одним ключом и тут же зашифровывает другим, не выпуская PIN в память сервера. Операция атомарна и выполняется исключительно внутри HSM. Поэтому любой узел, обрабатывающий PIN, обязан иметь HSM.

10.8 Церемония ключа (Key Ceremony)

Мастер-ключ — корневой секрет платёжной инфраструктуры; его компрометация означает компрометацию всех производных ключей, всех карт, всех транзакций. Процедуру генерации, загрузки и хранения мастер-ключа называют Key Ceremony — церемония генерации, разбиения и загрузки ключа с двумя обязательными правилами. *Dual control* — любая операция с ключом требует одновременного участия двух операторов; *split knowledge* — ни один участник не владеет полным ключом [200].

Порядок церемонии:

- HSM генерирует ключ и делит его на компоненты, ни один из которых сам по себе не позволяет восстановить исходный секрет;
- компоненты записывают на отдельные носители и передают разным хранителям;
- хранители подтверждают получение и хранят свои части отдельно;
- для загрузки ключа компоненты собирают только внутри защищённого периметра HSM.

Нарушение dual control или split knowledge на любом из шагов — инцидент безопасности, требующий перегенерации ключа.

Для одного мастер-ключа с тремя компонентами и двумя HSM (основной плюс резервный) церемония занимает 4–8 часов: подготовка помещения, генерация и разбиение, раздельная передача компонентов хранителям, загрузка в резервный HSM и верификация, документирование и опечатывание сейфов.

Split knowledge защищает от инсайдера: даже если один из хранителей скомпрометирован или действует под принуждением, у него нет полного ключа. Dual control

добавляет второй барьер: ни одно действие с мастер-ключом не завершается без участия второго человека. Атака на мастер-ключ требует сговора нескольких людей.

Иерархия церемоний и доверия

Чем ближе ключ к корню доверия, тем строже процедура и тем дороже каждое обращение к нему; чем ниже — тем больше операций и тем выше степень автоматизации:

- **корневой уровень** — Local Master Key (LMK) внутри HSM эквайера или эмитента и корневой ключ PKI (Public Key Infrastructure, инфраструктура открытых ключей), которым подписываются сертификаты сервера RKI (Remote Key Injection, удалённая загрузка ключей), генерируются и загружаются очной церемонией с dual control и split knowledge. То же относится к корневому ключу CA (Certification Authority, удостоверяющий центр) эмитента, под которым выпускаются сертификаты карт EMV. Эти ключи используются годами, и их перевыпуск требует отдельного проекта.
- **межорганизационный уровень** — Zone Master Key (ZMK) или Key Encryption Key (KEK), которыми банк, процессор и карточная сеть обмениваются ключами между собой, передаются компонентами под подписанные акты — также в ходе формальной церемонии, хотя без присутствия на одной площадке (компоненты доставляются курьером в опечатанных конвертах).
- **производный уровень** — терминальные ключи (TPK, Terminal PIN Key, для шифрования PIN-блока; TMK, Terminal Master Key, как локальный ключ хранения), рабочие ключи DUKPT и ключи отдельных карт. HSM выпускает их автоматически из ключей верхнего уровня и рассылает участникам по защищённым каналам без отдельной церемонии на каждое устройство. Путь ключа карты UDK от мастер-ключа эмитента IMK до чипа под транспортным ключом (TK) разобран в разделе 7.11.

RKI смещает церемонию на один уровень выше: вместо ручной загрузки ключа в каждый терминал церемонией один раз обслуживается корневой ключ сервера RKI, а из него автоматически выводятся ключи отдельных терминалов.

Загрузка ключей в терминалы (key injection)

Ключи загружаются в POS-терминалы ручным или удалённым способом:

- **ручная загрузка (*manual key injection*)** — терминал привозят в защищённую зону, где оператор загружает начальный ключ через специальное устройство. Процедура трудоёмка и плохо масштабируется, но по-прежнему применяется для первоначальной инициализации.
- **удалённая загрузка (Remote Key Injection, RKI)** — ключ загружают по защищённому каналу через специальный сервер. Терминал проходит взаимную аутентификацию и принимает только тот ключ, который поступил по доверенному каналу. RKI упрощает логистику больших терминальных сетей. В терминологии PCI PIN это удалённое распределение и установление ключей с использованием асимметричных методов из Annex A — первичная загрузка ключей с корневым доверенным сертификатом PKI [200].

Таблица 26 — Криптография ГОСТ и международные алгоритмы по ролям

Роль	ГОСТ	Международный
Подпись	ГОСТ 34.10	ECDSA / ECC
Шифрование	ГОСТ 34.12: Кузнечик, Магма	блочные шифры: AES, 3DES
Режимы	ГОСТ 34.13	NIST SP 800-38: GCM / CBC / CTR
Хеш	ГОСТ 34.11: Стрибог	SHA-256

10.9 ГОСТ в платёжном приложении Мир

Процессингу карт «Мир» мало RSA, 3DES и AES: российская платёжная криптография строится вокруг алгоритмов ГОСТ; регуляторные требования разобраны в разделе 25.2 [205, 206]. Базовый набор криптографических ГОСТ для ПС Мир:

- **ГОСТ 34.10–2018** — алгоритм электронной подписи на эллиптических кривых; российский функциональный аналог ECDSA [190].
- **ГОСТ 34.11–2018**, он же Стрибог, — функция хеширования, используемая при построении подписи и в ряде криптографических протоколов [219].
- **ГОСТ 34.12–2018** — блочные шифры Кузнечик и Магма, применяемые для шифрования данных и вычисления имитовставки (имитовставка — эквивалент MAC в отечественной терминологии) [220]. В российской криптографии Магма остаётся унаследованным (*legacy*) шифром (наследник ГОСТ 28147–89), а Кузнечик применяется в новых протоколах; пара соответствует международному разделению «3DES legacy / AES current».
- **ГОСТ 34.13–2018** — режимы работы блочных шифров (простая замена, гаммирование, гаммирование с обратной связью, выработка имитовставки), на которых строятся протоколы шифрования и имитозащиты [221].

Исторически основным симметричным шифром был ГОСТ 28147–89; в ГОСТ 34.12–2018 этот алгоритм включён под названием «Магма», а ссылки на 28147–89 встречаются в унаследованных конфигурациях и в ряде межведомственных документов как опорный алгоритм [222]. Для процессинга ГОСТ означает двойной стек (*dual-stack*) — HSM одновременно поддерживает ГОСТ и международные алгоритмы. ARQC карты «Мир» рассчитывается по 3DES CSK, а ГОСТ защищает MAC канала с НСПК и подпись клиринговых файлов (раздел 10.3). Процессинг эмитента должен обрабатывать оба семейства алгоритмов, HSM — хранить и использовать оба набора ключей [190, 220].

Внедрение поддержки ГОСТ начинается с HSM: ряд западных моделей получает алгоритмы ГОСТ только с дополнительным модулем или прошивкой. После обновления HSM нужна отдельная церемония ключа для набора ГОСТ, загрузка ключей ГОСТ для MAC канала с НСПК и подписи клиринговых файлов. Тестовая среда тоже держит оба набора, иначе сценарии кобейджа не воспроизвести.

Устройство ПС Мир, внутренняя маршрутизация и сценарии кобейджа разобраны в гл. 16.

11 3-D Secure

В операциях без физического предъявления карты (*card-not-present*, CNP) продавец оценивает риск до авторизации, но не может затягивать оформление заказа: каждая лишняя проверка отсекает часть покупателей. 3-D Secure разрешает это противоречие: эмитент проверяет держателя карты, а правила сети определяют, как при этом перераспределяется ответственность за фрод.

11.1 Происхождение 3DS: фрод по CNP

В базовой модели CNP продавец располагает лишь карточными реквизитами: номером карты, сроком действия, CVV2 и, возможно, адресом или почтовым индексом. Этих данных достаточно, чтобы сформировать авторизационный запрос, но недостаточно, чтобы доказать, что покупку инициирует именно законный держатель карты. Реквизиты можно выманить фишингом или получить из утечки, и после этого злоумышленник инициирует CNP-платежи от имени законного держателя.

Чип EMV сделал клонирование физической карты менее выгодным, и атаки сместились в дистанционный канал. Миграция на чип в точке продажи заняла больше десяти лет, и всё это время канал CNP оставался без сопоставимой защиты.

На европейском рынке это подтверждают данные ЕЦБ. В отчёте по SEPA фрод по CNP составил около 84 % стоимости карточного фрода и в 2020, и в 2021 году; этот сдвиг ЕЦБ объясняет ростом электронной коммерции и усилением защиты канала с физическим предъявлением карты [223]. Даже на фоне снижения абсолютной стоимости фрода по CNP в 2021 году этот канал оставался основным источником карточных потерь у европейских эмитентов.

Для транзакций CNP карточным сетям был нужен механизм, который решал бы ту же задачу, что чип решает в терминале: давал независимое подтверждение того, что транзакцию инициировал законный держатель карты. Им стал 3-D Secure. Сначала рынок знал этот протокол по брендам «Verified by Visa» и «Mastercard SecureCode», а затем по единой спецификации EMVCo [224].

Распространённость 3DS по рынкам остаётся неоднородной. В Европе обязательность усиленной аутентификации плательщика (Strong Customer Authentication, SCA) по второй европейской директиве о платёжных услугах (Payment Services Directive 2, PSD2 [225]; см. раздел 21.1) привела к массовому внедрению 3DS 2; в США обязательного требования нет, и продавцы ищут баланс между конверсией и защитой. В России 3DS используется повсеместно по инициативе эмитентов и по правилам системы Мир.

Magecart — общее имя семейства группировок (Group 1–12+), занимающихся JavaScript-скимммингом с 2015 года [226]: вредоносный код внедряется в CMS магазина или приходит через сторонние теги (аналитика, чаты, A/B-тестирование) и встраивается в поля ввода на странице оплаты. AVS (Address Verification Service) сверяет номер дома и ZIP; поддерживать его обязаны эмитенты США, Канады и Великобритании, в Европе — только по картам Visa, в других регионах поддержка не гарантирована [227]; там аутентификацию держателя карты выполняет 3DS. 3DS снижает риск фишинга и захвата учётной записи (*account takeover*, ATO), частично помогает против Magecart и перебора краденых карт (*card testing*), но не помогает против *fullz*/AVS. После первой авторизации PAN на стороне PSP заменяется сетевым

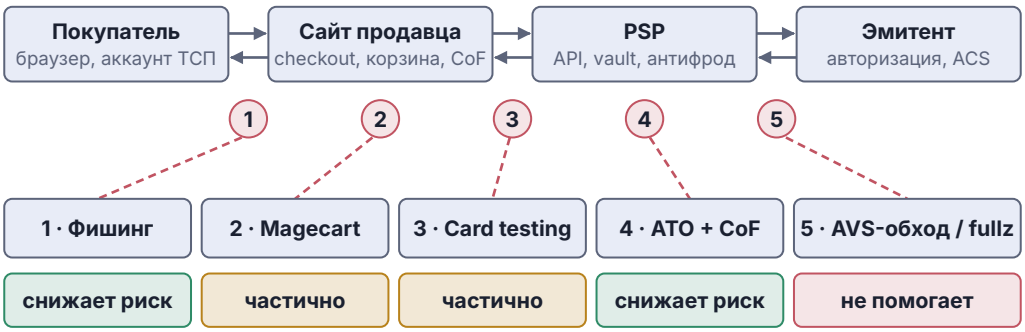


Рис. 31 — Векторы компрометации CNP и зона эффективности 3DS.

токеном (гл. 9), и уже токен, а не открытый PAN, хранится в *card-on-file* (CoF — сохранённые продавцом реквизиты карты для последующих списаний) и используется в последующих операциях.

11.2 Три домена 3DS

Название протокола, 3-D Secure, означает «безопасность в трёх доменах». В спецификации EMVCo они называются *Issuer Domain*, *Acquirer Domain* и *Interoperability Domain*; далее используются краткие имена — домен эмитента, домен эквайера и домен интеграции соответственно. В домене эмитента находится ACS (Access Control Server) — сервер эмитента или его процессора, который принимает решение об аутентификации держателя карты. В домене эквайера со стороны продавца различают *3DS Requestor* — роль инициатора аутентификации (продавец или его PSP — Payment Service Provider, платёжный провайдер) и *3DS Server* — технический компонент, который от имени Requestor формирует Authentication Request (AReq) и обменивается сообщениями с Directory Server. Если у продавца нет собственной 3DS-инфраструктуры, роль Requestor выполняет PSP: он предоставляет 3DS Server и встраивает его в инфраструктуру продавца. Между доменами эмитента и эквайера расположен домен интеграции с Directory Server карточной сети.

Распределение ролей жёсткое: 3DS Server передаёт контекст, DS маршрутизирует, ACS принимает решение. Продавец клиента не подтверждает; сеть в решение эмитента не вмешивается. От v1 к v2 менялись интерфейсы, объём передаваемых данных и способы подтверждения, но это разделение оставалось прежним.

Домен интеграции нужен, потому что эквайер и эмитент не связаны напрямую. Эквайер не может по одному PAN найти нужный ACS: у сотен эмитентов разные реализации, разные эндпоинты и разные версии протокола. Directory Server маршрутизирует запрос: по BIN карты (Bank Identification Number, банковский идентификационный диапазон) определяет нужный ACS и доставляет ему сообщение. Без этого промежуточного звена каждый эквайер был бы вынужден хранить адресную книгу всех эмитентов и обновлять её при каждом изменении адресов ACS.

11.3 3DS v1: редирект и его проблемы

Первая версия протокола работала через браузерный редирект. При оплате на сайте продавца браузер перенаправлялся на страницу ACS эмитента, где держатель

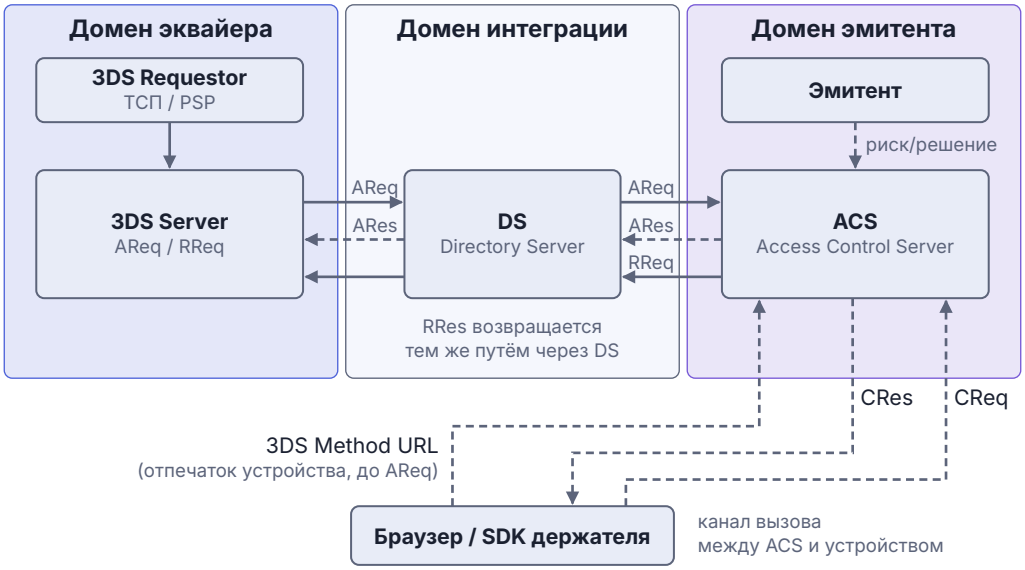


Рис. 32 — Архитектура трёх доменов 3-D Secure.

карты вводил пароль, связанный с программой «Verified by Visa», «SecureCode» или её локальным аналогом. На стороне продавца за обмен с Directory Server отвечал MPI (Merchant Plug-In) — встроенный компонент 3DS v1, формировавший пару VEReq/VERes (Verify Enrollment Request/Response) для проверки участия карты в программе и пару PAReq/PARes (Payer Authentication Request/Response) для собственно аутентификации.

Опыт держателя карты зависел от статического пароля, который требовался раз в несколько месяцев. Его путали с PIN и с паролем от интернет-банка, вводили на странице с незнакомым доменом — и часть покупателей прерывала оформление. Переход на отдельный экран подтверждения показывал клиенту, что оплата происходит вне магазина, и доверие к покупке падало [228]. К концу жизненного цикла 3DS v1 многие эмитенты заменили статический пароль на одноразовый код по SMS, но сценарий полноэкранного редиректа на чужой домен и связанные с ним риски остались прежними.

Редирект на незнакомый домен упрощал фишинг: пользователь привыкал вводить пароль на странице, не похожей ни на магазин, ни на привычный интернет-банк, и атакующему оставалось воспроизвести похожий экран ACS на подконтрольном домене.

С переходом электронной коммерции на мобильные устройства проблема обострилась. 3DS v1 был спроектирован для десктопного браузера: редирект посреди оформления заказа ещё был приемлем на большом экране, но в мобильном вебе и тем более в нативных приложениях он прерывал сценарий покупки.

Логика принятия решения была грубой. ACS в 3DS v1 либо пропускал транзакцию без явной аутентификации, либо требовал статический пароль. У него не было ни достаточного контекста покупки, ни встроенного способа перенести подтверждение в мобильное приложение банка. Первая версия решала экономическую задачу переноса ответственности, а держателя карты аутентифицировала грубо и неудобно.

При всех недостатках эмитенты поддерживали 3DS v1, потому что протокол переносил ответственность (*liability shift*): если продавец использовал 3DS и аутентификация была одобрена, риск фрода смещался на эмитента, а продавец получал защиту от chargeback по причине фрода. Для продавцов это был компромисс: потеря конверсии в обмен на снижение доли chargeback [224]. Карточные сети прекратили поддержку 3DS v1 в октябре 2022 года: с этого момента аутентификация в электронной коммерции целиком перешла на EMV 3DS v2 [229].

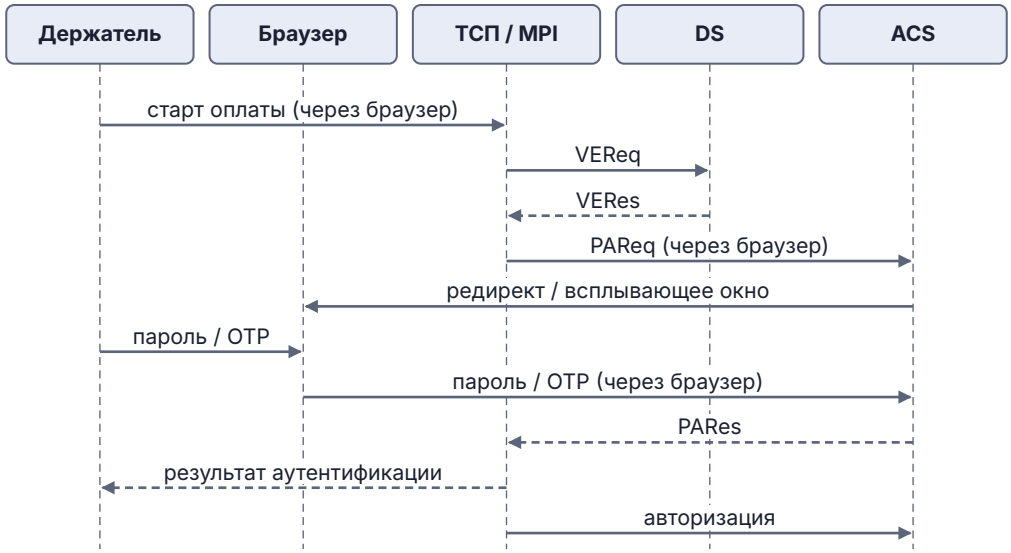


Рис. 33 — Поток 3DS v1: VEReq/VERes между MPI и DS, PAReq/PARes через браузер.

11.4 3DS v2: аутентификация на основе риска

Вторая версия 3DS сохранила дополнительную аутентификацию, но отказалась от обязательного редиректа и статического пароля. EMVCo развивает это семейство спецификаций как набор версий 2.x [224]. Главное нововведение — аутентификация на основе риска (Risk-Based Authentication, RBA). Вместо жёсткого выбора «пароль или ничего» ACS оценивает риск и выбирает подходящий сценарий.

Сценарий *frictionless*

Если ACS считает транзакцию низкорисковой, аутентификация происходит *незаметно* для держателя карты. 3DS Server отправляет контекст операции, ACS оценивает его, возвращает положительный результат, и транзакция передаётся на авторизацию без дополнительной паузы на экране оплаты. Этот сценарий сделал 3DS пригодным для массовой электронной коммерции — дополнительная проверка осталась в процессе, но перестала прерывать оформление заказа на каждом шаге.

Качество решения напрямую зависит от контекста, который передаёт 3DS Server. ACS получает сведения об устройстве, браузере или приложении, адресе доставки, истории покупок у конкретного продавца, характере самой операции и поведенческих признаках. По этому набору он решает, похожа ли текущая покупка на привычное действие держателя карты или требует дополнительного подтверждения. Чем

полнее и точнее эти данные, тем чаще эмитент пропускает операцию по сценарию *frictionless*, и тем больше выручки сохраняет продавец.

Цикл сообщений EMV 3DS начинается до AReq: браузер держателя карты может незаметно обратиться к *3DS Method URL* ACS — служебному адресу, который загружается в скрытом iframe; по нему ACS собирает сигнатуру устройства (*device fingerprinting*; механика и сигналы — в разделе 29.3) и привязывает её к идентификатору будущей транзакции. Затем 3DS Server отправляет в Directory Server Authentication Request (AReq), DS маршрутизирует его в нужный ACS и возвращает Authentication Response (ARes). В сценарии *frictionless* на ARes цикл и заканчивается. Если ACS запрашивает подтверждение, используется пара Challenge Request / Challenge Response (CReq/CRes) между ACS и браузером или 3DS SDK (клиентская библиотека для нативного мобильного приложения, заменяющая браузер в потоке аутентификации), а по её завершении ACS отправляет в DS итог в Results Request (RReq); DS ретранслирует его 3DS Server, который отвечает Results Response (RRes). Итоговый статус аутентификации доставляет в 3DS Server именно DS, а не ACS напрямую. Статус приходит в поле transStatus: `Y` — аутентификация пройдена, `N` — не пройдена, `A` — попытка аутентификации (*attempted authentication*; см. раздел 11.6).

Конкретный набор полей AReq определяет качество этих данных. Среди десятков полей спецификации EMVCo выделяются группы, которые напрямую влияют на долю *frictionless* [224]:

- **deviceChannel**, параметры браузера (`browserScreenHeight`, `browserLanguage` и др.) — сигнатура устройства, ACS сопоставляет текущую сессию с предыдущими;
- **threeDSRequestorAuthenticationInd** — тип операции (оплата, рекуррентное списание, добавление карты), задаёт порог риска;
- **acctInfo** — возраст учётной записи у продавца, дата последнего изменения адреса и количество покупок за 6 месяцев, то есть прямые индикаторы доверия;
- **merchantRiskIndicator** — сроки и способ доставки (в том числе цифровой товар), повторный заказ, предзаказ;
- **addrMatch** и адресные поля — расхождение адреса доставки с адресом биллинга, сигнал для запроса подтверждения;
- **threeDSRequestorPriorAuthenticationInfo** — ссылка на предыдущую успешную аутентификацию у того же продавца, снижающая порог для повторных покупок.

Точная доля *frictionless* и доля завершения (*completion rate*) для сценариев *challenge* зависят от сегмента ТСП, региона и качества данных по риску; публичные агрегированные цифры по ним редки, а маркетинговые материалы вендоров не дают общего правила, поэтому в книге они не приводятся.[1] Каждый дополнительный запрос подтверждения отсеивает часть покупателей, поэтому качество данных в 3DS-сообщении напрямую влияет на конверсию.

Сценарий *challenge*

Если ACS обнаруживает повышенный риск — например, новое устройство или нетипичную сумму, — он запускает *challenge*. В отличие от первой версии, протокол поддерживает несколько методов подтверждения в цифровом канале. Браузер (через iframe страницы оплаты) или 3DS SDK отправляет в ACS Challenge Request

[1] Внутренние A/B-измерения у крупных PSP стабильно показывают, что улучшение качества переданных в 3DS-сообщении полей даёт измеримый рост доли *frictionless* и совокупной конверсии страницы оплаты. Конкретные цифры у каждого продавца свои.

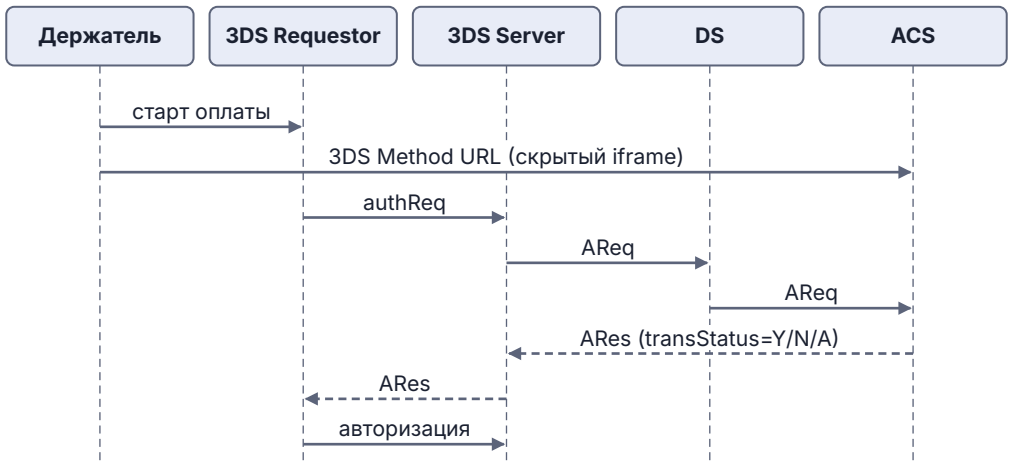


Рис. 34 — Поток 3DS v2, сценарий *frictionless*: AReq/ARes.

(CReq); ACS ведёт диалог с держателем карты и возвращает итог в Challenge Response (CRes) [224].

Метод подтверждения зависит от канала: одноразовый пароль по SMS или push-подтверждение с биометрией в мобильном банке. 3DS v2 использует интерфейсы, которыми держатель карты пользуется каждый день, и не зависит от редкого пароля [224].

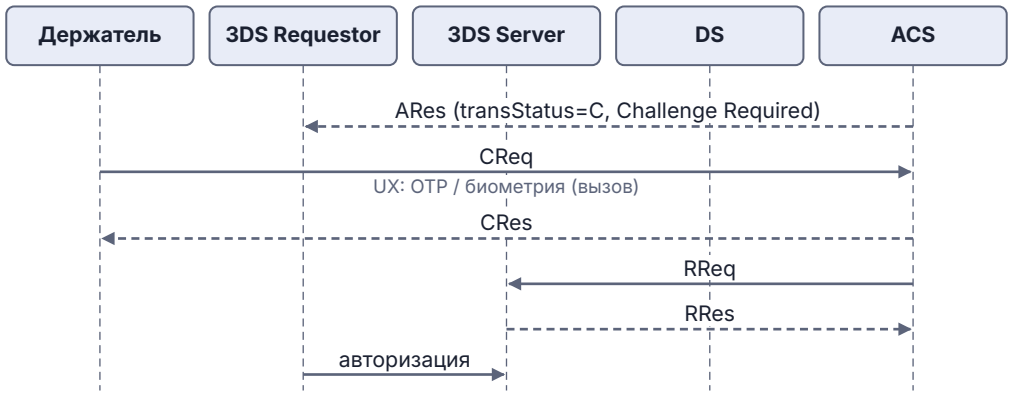


Рис. 35 — Поток 3DS v2, сценарий *challenge*: CReq/CRes, RReq/RRes.

11.5 Decoupled authentication

3DS v2 ввёл ещё один сценарий — *decoupled authentication*, то есть подтверждение, которое происходит *не в момент* покупки и *не в контексте* страницы оплаты. Обычный сценарий *challenge* предполагает, что держатель карты находится рядом с устройством и может немедленно ответить на запрос. Устройство интернета вещей без экрана — например, умная колонка или подключённый автомобиль — инициирует покупку без участия человека. В рекуррентном или ином 3RI-сценарии (3RI — 3DS Requestor Initiated, аутентификация, инициированная не держателем карты,

а продавцом или его 3DS Requestor) запрос тоже формируется без присутствия держателя карты. Для таких случаев предназначена *decoupled authentication* [230].

В отличие от обычного *challenge* ACS отмечает в сообщениях 3DS, что выбрана *decoupled authentication*, а итог позже передаёт в DS в Results Request (RReq), и DS ретранслирует его 3DS Server. Для продавца это промежуточный статус: заказ нельзя считать окончательно подтверждённым, пока не получен результат аутентификации [230].

После этого 3DS Server ждёт RReq, а продавец либо периодически запрашивает итоговый статус у 3DS Server, либо получает его по предусмотренному в интеграции асинхронному каналу. Параллельно эмитент связывается с держателем карты доступным способом: push-уведомлением или SMS [230].

Спецификация задаёт максимальное время ожидания (*decoupled max timeout*), после которого аутентификация считается неудавшейся. Если она не завершена вовремя, продавец либо отменяет заказ, либо отправляет транзакцию без результата аутентификации, принимая повышенный риск [230].

Сценарий *decoupled authentication* для держателя карты требует отдельного проектирования. Типичная формулировка — «Мы отправили вам уведомление в приложении: подтвердите, пожалуйста, покупку, и мы отгрузим заказ» — фиксирует заказ условно. Система управления заказами должна обработать промежуточный статус, таймаут и уведомление при подтверждении или отказе. Держателю карты нужно объяснить, что подтверждение завершается в банковском приложении [230].

11.6 Перенос ответственности

Перенос ответственности (*liability shift*) означает договорное перераспределение риска chargeback по причине фрода с продавца и эквайера на эмитента. Он остаётся ключевым экономическим стимулом для внедрения 3DS, но включается не автоматически: зависит от результата аутентификации, статуса операции, правил сети и, в Европе, от того, использовалось ли освобождение от SCA [13]. Исход зависит от сценария:

- **3DS выполнен, эмитент одобрил** — *frictionless* или пройденный *challenge*. При выполнении условий программы сети перенос ответственности действует, риск переходит к эмитенту. Продавец защищён от chargeback по коду причины, связанному с фродом.
- **получен результат попытки аутентификации** — случай, когда ACS эмитента не отвечает или эмитент не участвует в программе; результат фиксирует сервер сети в режиме *stand-in*, отвечающий от имени эмитента. Исторически некоторые программы давали продавцу защиту и в этом случае, но универсального правила в EMV 3DS нет: эффект зависит от конкретной сети и её текущей программы.
- **продавец не использует 3DS** — перенос ответственности не действует, продавец и эквайер несут ответственность за фрод.
- **продавец использует освобождение** — см. следующий раздел. По правилам Visa риск фрода несёт сторона, применившая освобождение: если его применил эквайер, перенос ответственности *не действует*, если эмитент — риск остаётся у эмитента [231].

Правила различаются по сетям и регионам: у Visa и Mastercard свои условия для попытки аутентификации, рекуррентных операций и отдельных категорий продавцов. Наиболее изменчивы правила попытки аутентификации.

Согласно Visa Secure Program Guide, эмитент-участник программы на EMV 3DS для держателя карты, не зарегистрированного в программе, возвращает «Not Authenticated»; ответ «Attempts» за неучаствующих эмитентов формирует Visa Attempts Server в режиме *stand-in* [232].

В России, где PSD2 не действует, перенос ответственности для внутрироссийских операций определяется правилами НСПК для карт Мир. До марта 2022 года аналогичные правила действовали для Visa и Mastercard; после приостановки операций этих сетей в России к внутрироссийским транзакциям они уже не применимы.

11.7 Освобождения PSD2 и специфика России

PSD2 и регуляторные технические стандарты (Regulatory Technical Standards, RTS) Европейской банковской службы (European Banking Authority, EBA) [233] требуют SCA для электронных платежей, кроме ряда освобождений: *low value* (операции на небольшие суммы), TRA (Transaction Risk Analysis — анализ риска транзакции эквайером или эмитентом), *trusted beneficiary* (доверенный получатель в белом списке держателя карты), *recurring* (рекуррентные списания с одинаковой суммой) и *secure corporate* (защищённые корпоративные платежи по выделенным протоколам). Общая модель и состав исключений разобраны в разделе 21.1.

Освобождение запрашивает продавец или эквайер, а решение принимает эмитент. Применение TRA или *low value* не отменяет его модели риска, и если транзакция выглядит подозрительно, эмитент вправе потребовать *challenge*. Использование освобождения может ослабить или полностью отменить перенос ответственности: убирая дополнительную проверку, продавец принимает риск фрода на себя [233]. 3DS v2 нужен и в этом случае как канал для индикаторов риска, запрошенных освобождений и итогового решения эмитента [233].

Специфика России

В российском законодательстве нет прямого аналога PSD2/RTS с тем же обязательным набором освобождений и их единым описанием. Необходимость аутентификации по 3DS для внутрироссийских транзакций определяют политика эмитента и правила карточной сети.

11.8 3DS и токенизация

Токенизация (гл. 9) и 3DS решают разные задачи. Токен отвечает на вопрос, какие именно карточные реквизиты участвуют в операции; 3DS — действительно ли её инициирует законный держатель карты. Вместе они дают эмитенту более полную картину риска. В сценарии *card-on-file* в электронной коммерции с EMV 3DS продавец передаёт в 3DS Server сетевой токен и связанные с ним атрибуты; Directory Server запрашивает у TSP (Token Service Provider, поставщик услуг токенизации) детокенизацию с верификацией (*de-tokenisation with verification*) — проверкой криптограммы и доменных ограничений на стороне TSP — и передаёт нужные данные в ACS, а ACS использует их, чтобы решить, нужен ли *challenge* и можно ли сформировать значение аутентификации (*authentication value* — криптографическое доказательство успешной аутентификации: CAVV у Visa, AAV у Mastercard, передаваемое в авторизации) [174].

В EMV 3DS версии 2.2 и выше последующие аутентификации повторных списаний *recurring* или рассрочки *instalment* могут выполняться как 3RI-запросы. 3DS Requestor указывает 3RI Indicator и передаёт DS Transaction ID и/или ACS Transaction ID (уникальные идентификаторы шага DS и ACS, выработанные при исходной клиентской аутентификации), чтобы ACS мог соотнести новую операцию с исходной аутентификацией держателя карты [234]. В руководстве EMVCo по токенизации указано, что в сценариях MIT (Merchant-Initiated Transaction — операция, инициированная продавцом по ранее установленному мандату держателя карты) свойства токена, способ его проверки и доменные ограничения наследуют контекст исходной клиентской операции [174]. Подробно о влиянии токенизации и 3DS на антифрод — в гл. 29.

12 PCI DSS

Архитектурный смысл PCI DSS сводится к вопросу: где именно в системе появляются данные карты и сколько компонентов должны их видеть. Ответ определяет, останется ли объём комплаенса в отдельном сегменте или распространится на всю инфраструктуру.

12.1 Двенадцать требований

PCI DSS (Payment Card Industry Data Security Standard) определяет требования к защите данных платёжных карт для любой организации, которая хранит, обрабатывает или передаёт данные держателя карты (cardholder data, CHD). Стандарт разрабатывает и поддерживает PCI SSC (Payment Card Industry Security Standards Council), созданный глобальными карточными сетями [70].

До появления PCI DSS у карточных сетей действовали собственные программы защиты данных. FAQ PCI SSC указывает, что общий стандарт возник из согласования программ Visa AIS/CISP (Account Information Security / Cardholder Information Security Program) и Mastercard SDP (Site Data Protection) [235]. Для ТСП, принимающего карты нескольких брендов, это заменило набор частично несовпадающих программ общей базовой планкой безопасности.

PCI SSC был создан в 2006 году American Express, Discover, JCB, Mastercard и Visa; разработанная учредителями версия 1.1 вступила в силу вместе с запуском совета [235, 236]. Утечки TJX и Heartland показали промышленный масштаб угрозы: компрометация затрагивает и отдельные магазины, и крупные процессинговые компании [166, 237].

Карточные сети передавали требования Visa CISP и Mastercard SDP через эквайеров, а не напрямую ТСП. Требования разных сетей расходились, поэтому у одного ТСП возникали несогласованные аудиты от нескольких эквайеров. Прямого финансового стимула инвестировать в безопасность у ТСП также не было: убытки от компрометации распределялись через chargeback между эквайером и эмитентом, а штрафы сетей выставлялись эквайеру. Единый стандарт изменил структуру стимулов: несоблюдение PCI DSS грозит ТСП штрафами и повышенными ставками, которые сеть взыскивает с эквайера, а эквайер взыскивает с ТСП по контракту.

Двенадцать требований PCI DSS группируются по областям защиты. Требования 1–2 задают сетевую защиту: межсетевые экраны, сегментацию и безопасные конфигурации без заводских паролей и лишних сервисов. Требования 3–4 относятся к карточным данным: требование 3 описывает защиту хранимого PAN и запрет хранения Sensitive Authentication Data (SAD), а требование 4 предписывает шифровать передачу CHD по открытым сетям.

Требования 5–6 охватывают защиту систем от вредоносного ПО, контроль уязвимостей, разработку, патчи и веб-приложения. Требования 7–9 сужают круг людей и систем, которые могут получить доступ к карточным данным, и требуют физической и логической дисциплины вокруг CDE (Cardholder Data Environment, среда обработки карточных данных — см. раздел 12.2).

Требования 10–11 требуют журналирования, мониторинга и регулярного тестирования безопасности среды, а требование 12 закрепляет эти меры в политике информационной безопасности.

Если токенизация, P2PE или полностью вынесенная платёжная страница удерживают данные карты вне среды ТСП, большая часть требований к этой среде не применяется.

12.2 CDE и периметр

Определение периметра CDE — центральная задача в работе по PCI DSS. Ошибка в определении периметра оценки означает либо недозащищённость, когда данные карты оказываются вне CDE без должной защиты, либо избыточность, когда организация тратит ресурсы на системы, которые карточных данных никогда не видят.

Scoping Information Supplement различает типы систем в периметре оценки [238]. Во-первых, это системы CDE, которые хранят, обрабатывают или передают CHD/SAD: серверы авторизации, базы данных с PAN, терминалы. PCI DSS прямо запрещает хранить SAD (CVV2, полные данные дорожки магнитной полосы, PIN/PIN block) после авторизации даже в зашифрованном виде; определение периметра не меняет это правило. Во-вторых, это непосредственно связанные системы (*connected-to systems*): они могут не видеть карточные данные, но соединены с CDE и способны повлиять на него; типичный пример — DNS-сервер или иной общий инфраструктурный узел в соседнем сегменте. Узел в том же сегменте, что и системы с CHD/SAD, сам относится к CDE. В-третьих, в периметр попадают системы, влияющие на безопасность (*security-impacting systems*): серверы аутентификации, системы мониторинга, антивирусные средства, серверы NTP и прочие компоненты, от которых зависит безопасность самого CDE. Обе категории — *connected-to* и *security-impacting* — относятся к области оценки, но не составляют сам CDE; Scoping Information Supplement отдельно оговаривает, что строгого разделения между ними нет: одна и та же система может относиться к обеим категориям.

Сетевая сегментация — главный способ удержать CDE компактным. Если карточные данные находятся в изолированном сегменте, отделённом от остальной инфраструктуры межсетевым экраном с политикой запрета по умолчанию, в периметр попадают этот сегмент и его ближайшие зависимости. Без такой изоляции CDE распространяется почти на всю сеть организации, и «точечный комплаенс» теряет практический смысл.

Критерий сегментации задают правила межсетевого экрана: система, которая не может инициировать соединение с CDE и в которую CDE не может инициировать соединение, остаётся вне периметра, даже если физически размещена в той же стойке. Такая система не получает сетевого пути к карточным данным, даже если полностью скомпрометирована.

ПРАКТИКА

ТСП выбрало SAQ A (Self-Assessment Questionnaire A, см. раздел 12.4), но разработчик добавил собственный скрипт на платёжную страницу. Сценарий перестаёт соответствовать SAQ A и переходит в SAQ A-EP (Partially Outsourced E-Commerce Merchants Using a Third-Party Website for Payment Processing) или SAQ D, потому что скрипт ТСП участвует в обработке данных карты. QSA (Qualified Security Assessor, аккредитованный аудитор PCI) фиксирует это на аудите; после этого следуют штрафы и срочная переработка интеграции. Изменение кода платёжной страницы меняет периметр PCI.

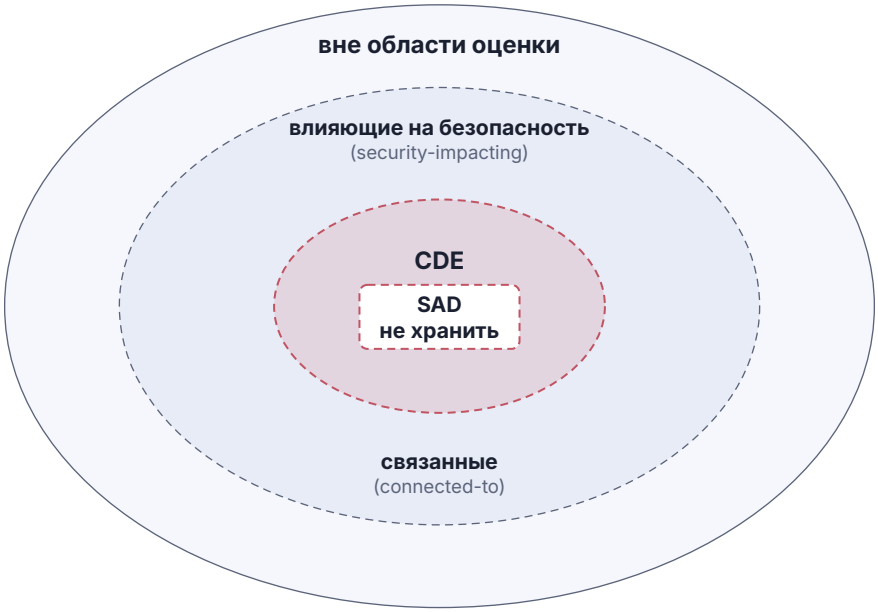


Рис. 36 — Периметр CDE и смежные системы.

12.3 Сужение периметра: токенизация, P2PE и вынесенные формы

Периметр оценки сужается только там, где архитектура сокращает число систем, способных увидеть PAN или повлиять на среды, в которых PAN существует.

Токенизация

В PCI токенизация встречается в трёх вариантах, которые нельзя смешивать; терминологическая матрица «термин × источник» и семейство токенов по области действия разобраны в разделах 9.2 и 9.4 гл. 9. Первый вариант — сетевые токены, описанные в разделе 9.3; они включают DPAN и MPAN, которые выпускает карточная сеть. Сетевые токены снижают ценность утечки и позволяют перестроить архитектуру так, чтобы настоящий PAN не проходил через системы ТСП. Подмена PAN токеном не выводит систему из периметра PCI сама по себе. Решающие вопросы: может ли среда увидеть PAN, использовать токен как полноценный платёжный идентификатор или повлиять на безопасность систем, где PAN существует [70].

Второй вариант — токенизация на стороне PSP (Payment Service Provider, платёжный провайдер). ТСП один раз передаёт PAN в платёжный шлюз, шлюз хранит его в собственном хранилище токенов (*vault*) и возвращает суррогатное значение (*payment token*). После этого ТСП работает только с этим суррогатом. Хранилище переносит основной объём требований на PSP, но у ТСП остаётся периметр вокруг точки первичного ввода PAN и интеграции со шлюзом. Шлюз, владеющий vault, остаётся полноценным субъектом PCI DSS, а точка первичного ввода PAN требует отдельной защиты [70].

Третий вариант — vault или FPE на стороне самой организации, без участия PSP или карточной сети. Vault при первом приёме PAN генерирует случайный суррогат

(в терминах PCI SSC — «surrogate value», в отраслевой терминологии — «pseudo PAN»). Синтаксически он валиден как PAN, но не маршрутизируется в сети и к авторизации непригоден [168]. Соответствие хранится в защищённом хранилище. Нижестоящие (*downstream*) системы — аналитика, биллинг, CRM — работают только с суррогатом и не видят PAN. В FPE (Format-Preserving Encryption, алгоритм FF1 по NIST SP 800-38G)[1] PAN шифруется в значение той же длины и символьного состава без отдельного хранилища соответствий; детокенизация требует ключа. В обоих случаях CDE сужается до vault или инфраструктуры ключей и точки первичного попадания PAN в систему. Прочие системы выходят из периметра. Ни карточная сеть, ни НСПК, ни внешний API здесь не задействованы [70, 168, 175].

Для российских кредитных организаций, работающих по 851-П и ГОСТ Р 57580.1-2017 (национальному стандарту по защите информации финансовых организаций) [181, 206], vault и FPE неравноценны. Аналога FPE по ГОСТ не существует — ТК 26 (Технический комитет по стандартизации «Криптографическая защита информации» при Росстандарте) не стандартизировал ни один режим FPE [182, 221], ни один российский производитель не имеет сертификата ФСБ (Федеральной службы безопасности) на конструкцию FPE — ни на базе Кузнечика, ни на базе AES. В vault сам токен не несёт криптографического содержания и не подпадает под требования к СКЗИ (средствам криптографической защиты информации в терминологии ФСБ). Требования к сертифицированной криптографии применяются к хранилищу соответствий (шифрование хранимых PAN — Кузнечик через сертифицированное СКЗИ) и к транспорту (ГОСТ TLS при обращении к vault по сети) [206].

P2PE (Point-to-Point Encryption)

P2PE — стандарт PCI, при котором данные карты шифруются непосредственно в терминале в момент считывания и расшифровываются только в HSM на стороне эквайера или процессора. Центральный элемент решения — модуль SRED (Secure Reading and Exchange of Data) внутри терминала. Это аппаратно защищённый компонент, который перехватывает считанные данные до их попадания в общую память терминала и шифрует их на ключе, введённом во время процедуры загрузки ключей (*key injection*). В результате через инфраструктуру ТСП проходит только зашифрованный блок данных, а не открытый PAN [239].

Модель P2PE разделяет ответственность между P2PE Component Provider, то есть поставщиком отдельных компонентов (терминала, HSM, системы управления ключами), и P2PE Solution Provider, то есть поставщиком сертифицированного конечного решения. ТСП с готовым решением P2PE выполняет меньше требований и может проходить валидацию по более короткому сценарию, если это допускают условия его платёжной программы и требования бренда карты. Среда расшифровки в HSM процессора остаётся в полном периметре PCI DSS, и процессор отвечает за защиту ключей [239].

Вынесенные поля оплаты и iframe

В электронной коммерции ТСП может не собирать данные карты на собственной странице. Вместо этого он встраивает iframe или вынесенные поля оплаты (*hosted*

[1] Для FF1 NIST рекомендует ограничивать применение доменами, в которых число возможных входов ($\mathrm{radix}^{\mathrm{minlen}}$) не меньше 10^6, поэтому на одиночные короткие поля он не применяется. Соседний алгоритм FF3 после атаки Durak–Vaudenay 2017 года был заменён на FF3-1 в черновике SP 800-38G Revision 1, а во второй редакции черновика (2025) предложен к полному исключению [180].

fields), которые предоставляет PSP. Ответственность здесь распределяется по принадлежности элемента DOM. Поле ввода размещено в домене PSP, нажатия клавиш отправляются прямо туда, и ни PAN, ни CVV не попадают ни в код JavaScript ТСП, ни на его серверы. От PSP ТСП получает платёжный токен и работает только с ним [70].

Если *все* элементы платёжной страницы поставляются только провайдером, соответствующим требованиям PCI DSS, ТСП может документировать соответствие через SAQ A. Если хотя бы часть элементов формируется на стороне ТСП, применяется SAQ A-EP. SAQ A v4.0.1 (r1), опубликованный в январе 2025 года, требует для сценария со встроенной платёжной формой (iframe или скрипт PSP) подтвердить, что весь сайт ТСП защищён от атак через скрипты, способных скомпрометировать ввод данных карты. Для чистого перенаправления и полностью вынесенной оплаты PCI SSC в FAQ 1588 это условие не распространяет [240—243].

Полное перенаправление на страницу PSP

Полное перенаправление (*redirect*) остаётся наиболее жёстким архитектурным способом вывести среду ТСП из CDE. Во время оплаты держатель карты полностью покидает сайт ТСП. Браузер перенаправляется на страницу платёжного шлюза, карточные данные вводятся и обрабатываются *целиком на стороне PSP*. После завершения держатель возвращается с уведомлением об успехе или отказе. PAN, CVV и срок действия карты в среде ТСП не появляются, и при выполнении условий вопросника этот путь ведёт к SAQ A [244].

Покупатель при этом замечает смену домена в адресной строке, и часть таких сессий заканчивается брошенной корзиной. PSP смягчают эффект стилизованными страницами оплаты, визуально близкими к сайту ТСП. Для малого бизнеса и для случаев, где упрощение комплаенса важнее непрерывности интерфейса, *redirect* остаётся предпочтительным вариантом [244].

Токенизация (как сетевая, так и vault/FPE на стороне ТСП или PSP) остаётся самостоятельным путём сужения периметра, независимым от выбора канала ввода: даже при сохранённой собственной форме оплаты вынос PAN из нижестоящих систем в vault или замена PAN на DPAN сокращает число систем, остающихся в CDE. При сужении периметра ответственность за CHD переносится на PSP или валидированное P2PE-решение; процесс всё равно остаётся подконтрольным PCI DSS.

12.4 SAQ A, SAQ A-EP и SAQ D

SAQ (Self-Assessment Questionnaire) — публикуемый PCI SSC шаблон самооценки; ТСП заполняет его и передаёт эквайеру по программе соответствия карточной сети без полного аудиторского цикла с участием QSA. Тип SAQ определяется конкретным способом взаимодействия с карточными данными — тем, как карта попадает в платёжный процесс и соприкасается ли ТСП с CHD [244].

Интернет-магазин, который при оплате полностью перенаправляет покупателя на страницу PSP по сценарию *redirect*, использует **SAQ A** — наиболее узкий вопросник для типичного ТСП в электронной коммерции с вынесенной страницей оплаты. Но SAQ A не означает нулевой периметр. PCI SSC отдельно уточняет, что веб-сервер ТСП, на котором расположен механизм *redirect*, остаётся в периметре, чтобы аудитор мог проверить конфигурацию и сам механизм перенаправления [245].

Со встроенным iframe критерий строже: если все элементы платёжной страницы, которые получает браузер, поступают только напрямую от поставщика услуг,

соответствующего требованиям PCI DSS, реализация может оставаться в SAQ A. Если же хотя бы часть элементов страницы формируется сайтом ТСП, применяется **SAQ A-EP**. Так PCI SSC различает *Direct Post* и iframe/URL *redirect*: в *Direct Post* сайт ТСП сам участвует в приёме карточных данных, тогда как в iframe и *redirect* страницу для ввода реквизитов формирует процессор [242, 243]. Для встроенной формы в SAQ A r1 добавлено условие — ТСП должно подтвердить, что его страница не подвержена атакам через скрипты; для чистого *redirect* и полностью вынесенной оплаты это условие не применяется [240, 241].

Для сценариев с физическими терминалами действуют отдельные типы вопросников. **SAQ B-IP** применяется к торговым точкам с терминалами, сертифицированными по PTS (PIN Transaction Security — программа PCI SSC по сертификации устройств приёма карт), подключёнными к платёжному процессору по IP. PCI SSC отдельно уточнил, что этот тип рассчитан на автономные устройства point-of-interaction (POI), одобренные PCI SSC и не смешанные с другими типами устройств в той же сетевой зоне [246].

SAQ C-VT рассчитан на колл-центр или бэк-офис, где сотрудник вручную вводит карточные данные через виртуальный терминал PSP, то есть через веб-интерфейс, который сам не хранит CHD. FAQ PCI SSC уточняет: это изолированный компьютер с браузером, через который вводится по одной транзакции [247].

Отдельные типы: **SAQ B** для торговых точек с импринтерами или автономными терминалами с коммутируемым (*dial-out*) соединением, без хранения CHD в электронном виде; **SAQ P2PE** — наиболее узкий вопросник для ТСП, использующих валидированное PCI P2PE-решение без доступа к открытым карточным данным.

Если архитектуру нельзя свести ни к одному из упрощённых сценариев, остаётся **SAQ D**. Он применяется ко всем ТСП, которые сами хранят, обрабатывают или передают CHD на собственных серверах и выходят за пределы специальных типов; для поставщиков услуг, которым сеть разрешает самооценку, SAQ D — единственный вопросник. SAQ D соответствует полному объёму требований PCI DSS. Разница между SAQ A и SAQ D — в трудоёмкости: больше тестов, больше документации, ежеквартальные внутренние сканы уязвимостей, ежегодный pentest (penetration test, тест на проникновение). Переход с SAQ D на SAQ A сокращает этот объём работ [244].

Крупные ТСП (Level 1 — уровень, который Visa и Mastercard назначают ТСП с годовым объёмом свыше 6 млн транзакций по своему бренду; Mastercard также может отнести к Level 1 ТСП после подтверждённой компрометации данных [47, 248]) и крупные поставщики услуг (service providers — организации, обрабатывающие, хранящие или передающие CHD от имени других) вместо SAQ проходят полный аудит QSA с выпуском ROC (Report on Compliance, отчёт о соответствии PCI). Конкретная стоимость соответствия зависит от размера CDE, сложности инфраструктуры, региональных тарифов QSA и состава внешних сервисов; усреднённых тарифов PCI SSC не публикует [70].

12.5 PCI DSS 4.0.1

Версия 4.0.1 ужесточила контроль платёжной страницы, инвентаризации скриптов и доказуемости внутренних процедур. Ключевые требования направлены против атак семейства Magecart, при которых злоумышленник внедряет вредоносный JavaScript на платёжную страницу для перехвата карточных данных [70].

Таблица 27 — Типы SAQ и условия их применимости

SAQ	Канал приёма	Условие применимости
A	e-commerce, redirect или iframe PSP	все элементы платёжной страницы поступают от PSP
A-EP	e-commerce, Direct Post или скрипт ТСП	часть элементов платёжной страницы формируется сайтом ТСП
B	физ. терминал, dial-out	импринтер или автономный POS, без электронного хранения CHD
B-IP	физ. терминал по IP	PTS-сертифицированный POI, автономный, по IP
C	торговая точка, POS-приложение	платёжное приложение на стороне ТСП, подключённое к интернету
C-VT	virtual terminal	колл-центр или бэк-офис; CHD вводят вручную через веб-интерфейс PSP
P2PE	валидированное PCI P2PE	сертифицированное end-to-end шифрование от POI до расшифровщика
SPoC	смартфон или планшет со считывателем PCI	валидированное решение SPoC (Software-based PIN entry on COTS), без доступа к открытым карточным данным
D	всё остальное	ТСП сам хранит, обрабатывает или передаёт CHD; полный объём PCI DSS

Заливка типа SAQ показывает объём требований: зелёный — сокращённый, жёлтый — промежуточный, красный — полный объём PCI DSS.

Требование 6.4.3 обязывает инвентаризировать, обосновывать и авторизовывать каждый JavaScript, загружаемый на странице ввода карточных данных. Для интернет-торговли это увеличивает объём работ: типичная платёжная страница подгружает десятки скриптов — аналитика, A/B-тесты, менеджеры тегов, виджеты чата — и каждый требует документирования и контроля целостности (CSP — Content Security Policy; Subresource Integrity, SRI — механизмы W3C для контроля загружаемых браузером скриптов).

Требование 11.6.1 обязывает обнаруживать несанкционированные изменения HTTP-заголовков и содержимого платёжной страницы: контроль целостности, клиентский мониторинг и процедуры, рассчитанные на электронный скимминг.

Многофакторная аутентификация (MFA, Multi-Factor Authentication) стала обязательной для всего неконсольного доступа к CDE, а не только для административного и удалённого, как в 3.2.1. Внутренние сканы уязвимостей должны выполняться с аутентификацией, чтобы выявлять конфигурационные и локальные проблемы, которые не видны снаружи. Для защиты PAN при передаче стандарт строже фиксирует работу с доверенными ключами и сертификатами: их нужно инвентаризировать, принимать только доверенные экземпляры и контролировать валидность. Целевой анализ риска (*Targeted Risk Analysis*, TRA) требует документировать периодичность контрольных мер, если стандарт допускает гибкость.

Большинство новых требований версии 4.0 до 31 марта 2025 года действовали как рекомендации и стали обязательными после завершения этого переходного периода [70].

12.6 Customized Approach

PCI DSS 4.0 ввёл альтернативный путь выполнения требований — Customized Approach (индивидуальный путь с собственными контрольными мерами и доказательством их эффективности; противопоставляется Defined Approach — стандартному выполнению требований по перечню обязательных контрольных мер). Организация вправе достичь той же цели безопасности альтернативной контрольной мерой при условии, что докажет эквивалентность на проверке [70].

Customized Approach строится на TRA. Анализ начинается с Customized Approach Objective — цели безопасности, которую стандарт связывает с конкретным требованием. Затем описываются текущее окружение, угрозы и уязвимости, относящиеся к этой цели, и документируется реализованная контрольная мера: какие выявленные угрозы она нейтрализует и почему достигает заявленной цели. Остаточный риск фиксируется в документации, свидетельства готовятся для QSA. Документация должна быть достаточной для независимой валидации: устная аргументация записи не заменяет [70].

Например, организация строит микросервисную архитектуру с сегментацией *zero-trust* (модель, при которой ни одна сеть или узел не считается доверенным по умолчанию, а доступ выдаётся по идентичности и контексту) вместо классических межсетевых экранов. Требование 1 (Install and Maintain Network Security Controls) в Defined Approach предполагает традиционные правила межсетевого экрана. В Customized Approach организация обосновывает, что mTLS (mutual TLS — взаимная аутентификация сторон по X.509-сертификатам) между сервисами, прокси с учётом идентичности (*identity-aware proxy*) и непрерывный мониторинг сетевого трафика достигают той же цели изоляции CDE. QSA должен независимо оценить эффективность этих мер.

TRA требует зрелой программы ИБ с формализованным управлением рисками, описанными контрольными мерами и регулярным пересмотром. QSA тратит больше времени на валидацию нестандартных контрольных мер, чем на проверку по списку Defined Approach. Для организации это означает и более высокие консалтинговые расходы, и более длительный аудит.

Для типовой архитектуры Defined Approach проще и дешевле. Customized Approach оправдан только там, где архитектура не укладывается в стандартный шаблон, но безопасность можно убедительно доказать.

12.7 PCI DSS и российские требования: 821-П, 851-П

Организация, работающая с карточными платежами в России, выполняет PCI DSS вместе с положениями Банка России 821-П и 851-П [205, 206] (см. раздел 25.2); конкретный состав мер положения задают через нормативную отсылку к ГОСТ Р 57580.1-2017, а оценку соответствия — по ГОСТ Р 57580.2-2018[181, 249] (разбор стандарта в разделе 25.2).

И PCI DSS, и российские положения требуют криптографической защиты данных, разграничения доступа, идентификации пользователей, MFA, журналирования, мониторинга, реагирования на инциденты и управления уязвимостями. Разница в том, что российские требования дополнительно опираются на сертифицированные СКЗИ и алгоритмы ГОСТ там, где это предписано регулятором (раздел 10.9), тогда как PCI DSS не навязывает конкретный алгоритм.

Обязательность алгоритмов ГОСТ опирается на сертификацию ФСБ — криптографический продукт должен пройти российскую процедуру оценки. PCI DSS допускает

AES, RSA и иную «strong cryptography» (в терминологии PCI — признанные отраслью алгоритмы с эффективной стойкостью ключа не менее 112 бит), но иностранные средства шифрования на AES-256 и RSA сертификатов ФСБ как СКЗИ не имеют. Поэтому в сценариях, где 821-П и 851-П требуют российские криптографические механизмы и сертифицированные средства защиты, они неприменимы [205, 206].

PCI DSS предполагает ROC, AOC (Attestation of Compliance, аттестат соответствия) или SAQ перед карточной сетью или эквайером, а российские требования добавляют собственную оценку соответствия, регуляторную отчётность и надзор Банка России. 851-П требует для категорий прикладного ПО, перечисленных в положении, либо сертификации, либо оценки соответствия не ниже ОУД4 (оценочный уровень доверия 4 по ГОСТ Р ИСО/МЭК 15408); для части иного прикладного ПО необходимость такой оценки банк определяет сам [206].

Прямого аналога этому в PCI DSS нет. Требование 6 PCI DSS описывает внутренние процессы безопасной разработки, управление уязвимостями и жизненный цикл изменений, но не вводит сопоставимой внешней процедуры сертификации или формальной оценки соответствия для прикладного банковского ПО. Для классов банковских приложений, попадающих в область применения 851-П, набор требований шире PCI DSS [206].

Практичный подход к параллельному комплаенсу — общая матрица контрольных мер, в которой каждому требованию PCI DSS сопоставлены пункты 821-П и 851-П. Матрица делится на блоки:

- **пересечения** — меры, удовлетворяющие оба свода одновременно: контроль доступа, журналирование, сетевая сегментация, управление инцидентами; большая часть требований;
- **технические расхождения** — криптооперации внутри периметра реализуются на алгоритмах ГОСТ с сертифицированными СКЗИ, тогда как тот же трафик дополнительно защищается TLS для требования 4;
- **непересечения** — сертификация или оценка соответствия прикладного ПО (только 851-П), регуляторная отчётность и контроль Банка России (только 821-П/851-П), SAQ/ROC перед карточной сетью (только PCI DSS).

Объединённая программа с общей доказательной базой и QSA, знающим российское регулирование, сокращает дублирующий сбор свидетельств по двум сводам и уменьшает общую трудоёмкость аудита.

PCI DSS и 57580 не заменяют друг друга: для российской финансовой организации в карточном периметре обязательны оба свода одновременно. Своды различаются объектом защиты. PCI DSS обращён к данным платёжных карт (CHD/SAD) у любого участника карточной сети; 57580 обращён к информации финансовой организации в целом, и карточный периметр в нём — лишь одна из зон применения.

Там, где обе области пересекаются — эквайринг, эмиссия, процессинг внутри лицензированного периметра — организация одновременно проходит оценку соответствия по 57580.2 (через проверяющую организацию с лицензией ФСТЭК и надзор Банка России) и аттестацию по PCI DSS (через QSA и отчёт перед карточной сетью).

Две оценки проходят разными циклами с разной длительностью и разной точкой отсчёта. PCI DSS требует ежегодного подтверждения соответствия: SAQ вместе с AOC или ROC вместе с AOC завершаются раз в год, и 12-месячный цикл отсчитывается от даты завершения предыдущей оценки (дата отчёта, *Date of Report*, для ROC; дата завершения самооценки, *Self-Assessment completion date*, для SAQ). Эквайеру и карточной сети передаётся AOC; ROC остаётся у QSA и оцениваемой стороны и предоставляется только по запросу [244]. Оценка соответствия по 57580.2 проводится не реже одного раза в два года: периодичность задаёт 851-П (п. 13.4) [206], а саму

методику — ГОСТ Р 57580.2-2018 [249]. Период отсчитывается от даты завершения предыдущей внешней оценки, отчёт хранится не менее пяти лет (851-П, п. 13.2; см. раздел 25.2). Внеплановые контрольные мероприятия Банка России возможны вне этого расписания на основании ст. 73 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации» [2].

QSA и проверяющая организация ФСТЭК работают независимо и не обмениваются свидетельствами; общая часть доказательной базы — конфигурации, журналы, политики, результаты сканов — собирается организацией один раз, но интерпретируется применительно к каждому своду отдельно. Если контрольная мера реализована альтернативным способом и закрывает требование PCI DSS через Customized Approach, российский регулятор всё равно требует обоснования по 57580. ГОСТ Р 57580.1-2017 предусматривает «иные (компенсирующие) меры» (п. 6.4): при невозможности технической реализации выбранной меры финансовая организация разрабатывает компенсирующую меру, направленную на нейтрализацию тех же угроз из модели угроз [181]. Это — аналог Compensating Controls в Defined Approach, а не Customized Approach: симметрии с Targeted Risk Analysis и отдельным Customized Approach Objective в 57580 нет.

13 Один tap

Между касанием карты и звуком терминала проходит немногим больше одной секунды. За это время одиннадцать участников по очереди читают и переписывают одно платёжное сообщение; каждый следует правилам, описанным в разных главах книги.

Предыдущие главы разбирали EMV, бесконтактный протокол, ISO 8583, криптографию, ОПКЦ и эквайера по отдельности. Эти разборы останавливались там, где начинается соседняя тема: гл. 7 не доходит до ОПКЦ, гл. 16 не разбирает GPO. Эта глава соединяет их: показывает, как одна APDU превращается в ISO 8583 и как ответ возвращается в карту; за деталями каждой фазы — ссылки на исходные главы.

13.1 Условия примера

Разбираемая транзакция: бесконтактная карта «Мир Дебетовая», эмитент — АО «Т-Банк», эквайер — ПАО Сбербанк, терминал — бесконтактный ридер на кассе федеральной розничной сети, сумма 1 420,50 руб. Карта приложена в 11:43:07 по московскому времени, чек распечатан в 11:43:09. В этот интервал укладываются одиннадцать фаз. Типовой бюджет — около 1200 мс: половина приходится на обмен данными карты с терминалом, вторая половина — на ОПКЦ и эмитента.

Транзакция онлайновая: сумма ниже бесконтактного лимита CVM (3000 руб. у ПС Мир [250]), PIN не запрашивается, но офлайн-лимит терминала (*floor limit*) ниже суммы, и терминал запрашивает авторизацию эмитента. Поэтому ARQC передаётся эмитенту, а сигнал звучит только после ответа. Низкие суммы с офлайн-подтверждением (*tap-and-go*) проходят иначе: решение принимается в поле, без ожидания сети; этот путь разобран в разделе 8.2.

С 1 апреля 2015 года весь внутрироссийский карточный трафик идёт через ОПКЦ НСПК [17], в 2016 году — до 20 млн операций в сутки [251]. 23 февраля 2024 года OFAC внёс НСПК в список SDN [252], дополнительно ограничив зарубежный приём карт российских эмитентов независимо от бренда. В 2026 году типовая платёжная транзакция в России — это карта «Мир», российские эквайер и эмитент, маршрут целиком внутри страны.

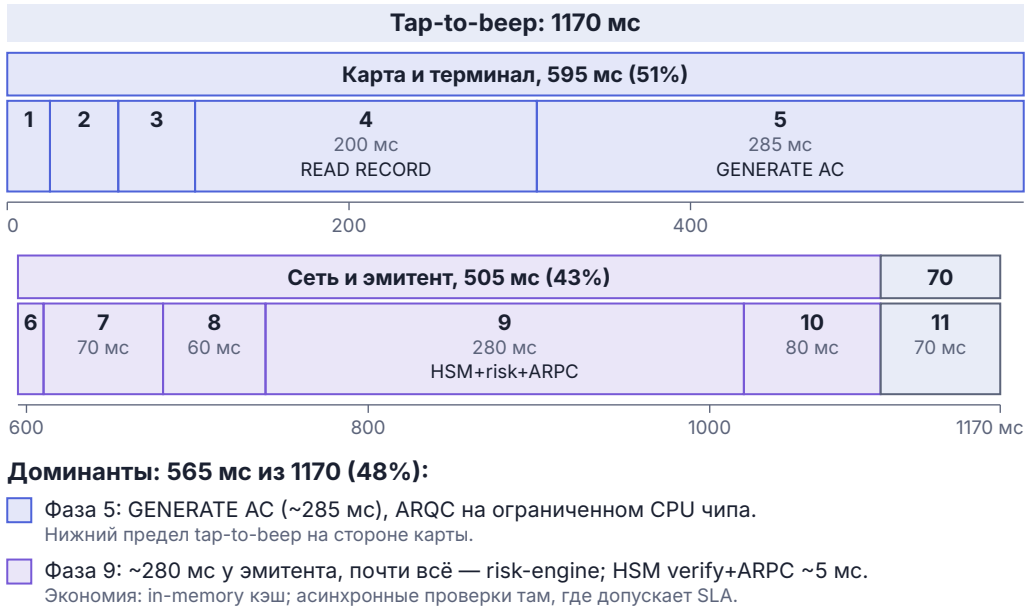


Рис. 37 — Расходование бюджета tap-to-beep: 1170 мс.

13.2 Карта в поле: фазы 1–5

Первые пять фаз — обмен между бесконтактной картой и терминалом. Карта попадает в рабочую зону антенны, получает питание от поля, ведёт EMV-диалог и отдаёт ARQC. Терминал в это время инициализирует радиоинтерфейс, выбирает приложение, читает запись карты и получает криптограмму. Независимый замер бесконтактного EMV на NFC-ридере Android-смартфона даёт 445–544 мс на сессию с пластиковой картой; у карты Mastercard 284 мс из 544 занимает одна GENERATE AC [253].

Фаза 1. RF-активация, антиколлизия, установление T=CL (0–25 мс)

Терминал излучает поле на 13,56 МГц. Антенна карты принимает его, выпрямительный диод заряжает накопительный конденсатор, чип запускается за единицы миллисекунд. Затем выполняется ISO 14443: WUPA (Wake-Up Type A) от терминала, ATQA (Answer To Request, Type A) от карты, антиколлизия по UID, SAK (Select Acknowledge), RATS (Request for Answer To Select), ATS (Answer To Select). К исходу этой фазы у карты и терминала есть согласованный транспортный канал T=CL по ISO 14443-4 [126, 127], с максимальным временем ожидания ответа FWT, по умолчанию 4,8 мс при FWI=4 (Frame Waiting Integer) и до 4,9 с при FWI=14 [127].

ISO 14443 не зависит от карточной сети: одна и та же радиофизика используется для Мир, Visa и UnionPay. Подробно об этом — раздел 8.1.

Фаза 2. PPSE и выбор приложения (25–65 мс)

Поверх T=CL терминал отправляет APDU `SELECT 2PAY.SYS.DDF01` — запрос PPSE (Proximity Payment System Environment). Карта возвращает FCI, в теге `0xA5`

которого содержится список Application Templates (тег 0x61): для каждого приложения — ADF Name (0x4F), Application Label (0x50) и Application Priority Indicator (0x87) [254]. На карте «Мир» ADF Name начинается с RID НСПК 0xA0 00 00 06 58, зарегистрированного по ISO/IEC 7816-5 за НСПК как поставщика приложения (*application provider*) [132].

Combination Selection сопоставляет AID карты со списком ядер, которые поддерживает терминал. Правила ПС Мир требуют: если на карте одновременно есть AID Мир и AID другой системы (например, в кобейдже Мир–UnionPay), терминал в России выбирает только AID Мир и передаёт управление Mir Kernel [169, 255]. Mir Kernel — собственное бесконтактное ядро НСПК; его терминальный интерфейс описан в публикуемой НСПК спецификации «Mir Payment System Contactless Terminal Kernel Specification» [256], низкоуровневые детали криптограммных проверок остаются в закрытой части документации для участников.

Выбор приложения по приоритетам разобран в разделе 7.3; кобейдж Мир–UnionPay и его исходы — в разделе 16.2.

Фаза 3. GPO, AIP, AFL (65–110 мс)

Терминал отправляет GET PROCESSING OPTIONS с PDOL, в который запакованы сумма, валюта, страна терминала, возможности терминала (*capabilities*), TTQ и UN. Карта возвращает AIP (Application Interchange Profile — какие проверки приложение поддерживает) и AFL (Application File Locator — адреса записей, которые терминал должен прочитать). Структура AIP / AFL — общая EMV-семантика, одинаковая по Books EMVCo и по Mir Kernel.

PDOL, AIP и AFL разобраны в разделе 7.2.

Фаза 4. READ RECORD и аутентификация данных (110–310 мс)

По AFL терминал читает несколько SFI/Record-записей: PAN (тег 0x5A) из диапазона 2200-2204 по ISO/IEC 7812 [54], срок действия (0x5F24), CDOL1, сертификат эмитента (0x90), открытый ключ эмитента (0x92) и данные карты для аутентификации. На картах «Мир» с криптографией по ГОСТ (см. раздел 10.9) сертификатная иерархия и алгоритмы подписи строятся на ГОСТ 34.10–2018 и ГОСТ 34.11–2018; на картах «Мир» с международной EMV-криптографией — на RSA / SHA. Терминальное ядро проверяет цепочку сертификатов по корневым ключам CA, загруженным в терминал через TMS [256].

Иерархия CA / IPK / ICC и общая схема CDA / fDDA — разделы 7.4 и 10.4.

Фаза 5. GENERATE AC и ARQC (310–595 мс)

Терминал собирает CDOL1 и отправляет GENERATE AC с P1=0x80 — запрос ARQC (Authorisation Request Cryptogram). Чип карты выводит сессионный ключ SK_{AC} из UDK по схеме, согласованной с НСПК (для ГОСТ-карт ключ выводится через Кузнечик / Магма; для карт с международной криптографией — по стандартной EMV-схеме на 3DES), считает MAC поверх данных транзакции, ATC и криптограммных параметров и возвращает ARQC, ATC, IAD и CID. По измерениям бесконтактного EMV одна такая APDU занимает около 280 мс на пластиковой карте [253] — самая длинная фаза обмена карты с терминалом, и именно она задаёт нижний предел *tap-to-beep* даже при идеальной сети. ГОСТ-карта может отвечать медленнее, если

Кузнечик реализован программно на конкретном чипе, но для массовой эмиссии бюджет остаётся в пределах 300 мс.

К концу фазы 5 карта может покинуть поле: у терминала есть всё нужное для онлайн-авторизации, и дальнейший обмен идёт без карты. В описанном онлайн-сценарии бесконтактный Mir Kernel не использует второй `GENERATE AC`: к моменту ответа эмитента карта уже не в поле.

Внутреннее устройство ARQC, набор полей CDOL1, разница ARQC / TC / AAC и место CID в решении — раздел 7.8.

13.3 Сеть в воздухе: фазы 6–10

После получения ARQC начинается сетевой участок: терминал упаковывает данные в ISO 8583, передаёт эквайеру, эквайер маршрутизирует сообщение в ОПКЦ, ОПКЦ доставляет его эмитенту, эмитент верифицирует криптограмму, принимает решение, генерирует ARPC и отправляет ответ обратно. Весь путь остаётся внутри России и занимает около 505 мс типового бюджета.

Фаза 6. Упаковка в ISO 8583 0100 по профилю НСПК (595–610 мс)

Терминальное приложение собирает авторизационное сообщение в формате ISO 8583 [74]: MTI 0100 (Authorization Request) с bitmap, где отмечены поля DE 2 (PAN из диапазона `2200-2204`), DE 3 (Processing Code), DE 4 (Amount), DE 7, DE 11, DE 12, DE 14, DE 22 (POS Entry Mode — бесконтактный), DE 25 (POS Condition Code), DE 48 (Additional Data) и DE 55 (Integrated Circuit Card System Related Data). DE 55 — это BER-TLV-капсула с теми же EMV-тегами, которые терминал получил от карты: ARQC (9F26), ATC (9F36), IAD (9F10), AIP (82), AFL (94), CVR (Card Verification Results) внутри IAD и другие теги. Полный набор полей и их интерпретация определяются спецификацией НСПК и доступны только участникам ПС Мир [17]; DE 55 без потерь переносит к эмитенту криптограмму и контекст её формирования.

Сама упаковка занимает единицы миллисекунд: терминал собирает ISO 8583 локально и не ждёт сетевого обмена. Структура bitmap и ISO 8583 в целом — раздел 6.1; маршрут через ОПКЦ и правила НСПК — раздел 16.2.

Фаза 7. Терминал → FEP эквайера → шлюз к ОПКЦ (610–680 мс)

Терминал передаёт сообщение через настроенный канал: GPRS/4G через встроенный модем, проводной Ethernet через кассу, реже WiFi. У российских ТСП большинство стационарных терминалов подключены к выделенной сети эквайера через VPN поверх 4G или по MPLS-каналу ТСП. Транспорт — TLS с клиентским сертификатом, который TMS загружает в терминал при регистрации (раздел 3.2 разбирает TMS и жизненный цикл прошивок).

На входе у эквайера сообщение принимает Front-End Processor (FEP) — сетевой шлюз, который терминирует TLS, разбирает ISO 8583, проверяет MAC терминала (если используется сессионный ключ поверх T=CL и отдельный MAC хоста) и по BIN определяет дальнейший маршрут. Сбер, крупнейший эквайер российского рынка с долей более 60 % по количеству терминалов [257, 258], эксплуатирует FEP-инфраструктуру на собственных мощностях; небольшие процессоры могут арендовать FEP у интегратора. BIN-таблица обновляется у эквайера из централизованного

перечня НСПК. По BIN `220070` (один из диапазонов Т-Банка) FEP определяет: карта «Мир», маршрут — на шлюз эквайера к ОПКЦ.

Шлюз эквайера к ОПКЦ выполняет во внутрироссийской сети ту же функцию, что Mastercard Interface Processor (MIP) в международной: это терминирующая точка авторизационного протокола между процессором и национальным коммутатором. Технически это собственная разработка эквайера или решение от интегратора (например, «Инфосистемы Джет» работали с НСПК над клиринговой системой Мир [251]); единого стандарта реализации аналога MIP в НСПК нет.

Бюджет фазы — 50–80 мс по российской магистральной сети, до 150 мс в регионе со слабым каналом.

Фаза 8. Маршрутизация ОПКЦ → шлюз эмитента (680–740 мс)

ОПКЦ (операционный и платёжный клиринговый центр НСПК) — центральный коммутатор внутрироссийских карточных операций. В отличие от распределённой сети Mastercard с региональными Authorization Platform и глобальной маршрутизацией, ОПКЦ работает как единый логический узел внутри России. ОПКЦ идентифицирует эмитента по BIN из собственной таблицы маршрутизации, формирует адрес шлюза эмитента и направляет туда сообщение [17, 259].

В устойчивой сети этот переход занимает 30–50 мс: одна короткая магистраль без глобальной маршрутизации между континентами. Для сравнения: круговая задержка (*round trip*) от Москвы до Нью-Йорка — около 120 мс, до Сингапура — около 190 мс [260]. Внутрироссийский маршрут Мир остаётся в стране, но дальние регионы по задержке сопоставимы с межконтинентальным участком: Москва — Хабаровск около 100 мс (раздел 13.5).

В сценариях *stand-in* ОПКЦ принимает решение об авторизации вместо недоступного эмитента по параметрам, согласованным заранее. В Правилах ПС Мир этот механизм называется *Сервисом Резервной Авторизации* (раздел 13) [169]; международный аналог — Visa STIP или Mastercard stand-in.

Фаза 9. Auth host эмитента: HSM проверяет ARQC, риск-движок, ARPC (740–1020 мс)

В ЦОДе Т-Банка сообщение принимает Authorization Host — центральный процесс эмитента, обслуживающий онлайн-авторизацию (раздел 3.1). Он распаковывает ISO 8583, извлекает из DE 55 теги ARQC, ATC, IAD, AIP и отдаёт их HSM на проверку.

У российских эмитентов HSM — это либо сертифицированный Thales payShield с прошивкой ГОСТ-модуля, либо отечественный HSM с поддержкой ГОСТ-2018 (Кузнечик, Магма, Стрибог). Получив команду на верификацию ARQC, HSM последовательно восстанавливает UDK из IMK эмитента и PAN, выводит сессионный ключ SK_{AC} по схеме НСПК и снова считает MAC поверх предъявленных данных транзакции, сверяя результат с ARQC карты. Один вызов HSM — единицы миллисекунд при правильной конфигурации очередей.

Параллельно с криптопроверкой риск-движок проверяет лимиты по карте, скоринг по MCC, поведенческие признаки, кэш статусов авторизаций, белые и чёрные списки устройств. Решение — одобрение, отказ или *soft decline*. В бесконтактном пути *step-up* невозможен: карта не в поле, повторного `GENERATE AC` не будет, поэтому *soft decline* превращается в обычный отказ или одобрение.

Если решение положительное, HSM считает ARPC: MAC поверх ARQC и ARC (Authorisation Response Code) по схеме, согласованной с НСПК. ARPC возвращается

в Authorization Host. По отраслевым сводкам auth host укладывается в 150–300 мс; выделенные системы снижают собственную задержку до единиц миллисекунд [261].

Фаза 10. ISO 8583 0110 и обратный путь (1020–1100 мс)

Authorization Host формирует ответное сообщение MTI 0110: bitmap, тот же DE 2/DE 3/DE 4 для корреляции, DE 38 (Authorization ID Response Code), DE 39 (Response Code: `00` — одобрено), DE 55 с ARPC в теге `0x91`. Сообщение идёт обратным маршрутом: шлюз эмитента к ОПКЦ, ОПКЦ, шлюз эквайера, FEP эквайера, терминал.

Обратный путь проходит через те же физические узлы, что и прямой, и занимает около 80 мс против 130 мс прямого пути фаз 7–8. Коды отклика ISO 8583 и правила интерпретации DE 39 — раздел 6.5.

13.4 ECR, чек, ОФД: фаза 11

После того как терминал получил MTI 0110 с `Response Code 00`, остаётся кассовый участок: сообщить о результате кассе, напечатать чек и отправить фискальные данные оператору фискальных данных (ОФД).

Фаза 11. Терминал → ECR → касса → ОФД (1100–1170 мс)

Между терминалом и кассовой программой (ECR — Electronic Cash Register) работает отдельный интерфейсный протокол. В терминал не попадают корзина покупателя и артикулы, в ECR — данные EMV и ISO 8583. Между ними — один запрос-ответ по локальной шине: «сделай платёж на такую-то сумму» — «платёж сделан, RRN такой-то, код авторизации такой-то».

Такие протоколы бывают стандартизированными и проприетарными.

Стандартизированный nexo Retailer Protocol (разработан консорциумом EPAS; с 2014 года его ведёт nexo standards — независимая некоммерческая ассоциация [262]), построенный на ISO 20022 и передающий запрос/ответ как XML или JSON-сообщения [263]. Цель nexo — снизить зависимость ТСП от конкретного эквайера: одно и то же кассовое ПО совместимо с терминалами разных поставщиков и PSP. В 2021 году ПС Мир была добавлена в nexo FAST — спецификацию платёжного приложения терминала: бесконтактное ядро Мир вошло в неё [255]; для российского рынка это означает, что европейские интегрированные кассовые решения могут принимать «Мир» без отдельного драйвера эквайера.

Проприетарные протоколы PSP и поставщиков терминалов: каждый эквайер исторически имел свой бинарный или текстовый формат связи между терминалом и кассой. На российском рынке свой протокол есть у Сбера, у ВТБ, у Альфы и у локальных поставщиков («Эвотор», АТОЛ) — с интеграцией под конкретное кассовое ПО (1С, R-Keeper, iiko, Frontol).

Получив подтверждение от терминала, ECR формирует чек: сумма, маскированный PAN, последние четыре цифры, дата, время, RRN, код авторизации, имя ТСП, адрес. По Федеральному закону от 22.05.2003 № 54-ФЗ «О применении контрольно-кассовой техники» [264] к этому добавляются фискальные реквизиты — номер фискального накопителя (ФН), номер фискального документа (ФД), фискальный

признак документа (ФПД), QR-код для проверки в приложении Федеральной налоговой службы (ФНС), и всё это передаётся ОФД через интернет. ОФД пересылает данные в ФНС.

Сигнал терминала и печать чека выполняются параллельно: терминал издаёт звук сразу по получении `Response Code 00`, кассовая программа печатает несколько секунд. Для покупателя *tap-to-beep* — это около 1200 мс; *tap-to-receipt* — ещё 2–4 секунды.

13.5 Бюджет 1170 мс

Из 1170 мс типового бесконтактного бюджета 595 мс приходится на обмен карты с терминалом, 505 мс — на сеть и эмитента, 70 мс — на ECR / печать чека (см. рис. 37). Внутри карточно-терминальной половины 285 мс из 595 занимает одна `GENERATE AC` [253] — криптограмма на ограниченном CPU чипа. Внутри сетевой половины 280 мс — Authorization Host эмитента с HSM-вызовами и риск-движком.

Когда сумма ниже офлайн-лимита терминала и эмитент допускает офлайн-одобрение (*tap-and-go*), фазы 7–10 исключаются. Терминал принимает решение по правилам ядра, пока карта ещё в поле, и издаёт сигнал сразу после фазы 5. Расчёт происходит позже, через отложенное финансовое представление (*deferred capture*): эквайер собирает одобренные офлайн транзакции пакетом, отправляет их в ОПКЦ, а если на счёте держателя средств не хватит, разбирательство начнётся постфактум. Tap-to-beep сокращается вдвое, до 600 мс. Отложенную модель применяет часть транспортных валидаторов, где задержка в полсекунды на каждом пассажире превращается в очередь у двери [81]; другие турникеты требуют удерживать карту до открытия прохода [265].

В онлайн-сценарии криптография выглядит удобной целью оптимизации: ускорить HSM, поставить его в один ЦОД с auth host, сменить шифр. Но из 280 мс auth host эмитента около 270 мс занимает риск-движок — лимиты по карте, скоринг по MCC, поведенческие проверки, кэши авторизаций и списки устройств. HSM тратит на проверку ARQC и генерацию ARPC единицы миллисекунд на вызов; если HSM и auth host находятся в одном домене синхронной репликации (расстояние между ЦОДами до 50 км, ограничено скоростью света в оптике и задержкой терминирующего оборудования), один вызов укладывается в 2 мс. Размещение HSM рядом с auth host в одном ЦОДе экономит меньше 2 % общего бюджета — закон Амдала: ускорение участка в 5 мс из 280 не меняет архитектурный вывод.

Риск-движок ускоряют без криптографии: лимиты в памяти вместо запросов к БД, кэш и предрасчёт признаков клиента и устройства, асинхронные проверки там, где задержка ответа укладывается в SLA.

Карту по протоколу ускорить тоже нельзя. Фаза 5 — около 285 мс на одну `GENERATE AC` — работа MPA (Mir Payment Application, апплет на чипе) на ограниченном CPU карты. Mir Kernel, национальное L2-ядро НСПК на терминале (в EMVCo Book C не входит, действует параллельно международным Kernel 2 = M/Chip Contactless и Kernel 3 = qVSDC поверх общего EMV-фреймворка), уже использует один GENERATE AC без Issuer Script Processing. То, что Quick Chip и M/Chip Fast (см. раздел 7.10) делают для контактного dip'а на уровне терминального ядра, в бесконтактном пути заложено в сам сценарий. Сократить эти 285 мс можно только сменой поколения чипа с аппаратным криптомодулем — то есть массовым перевыпуском карт.

В сети между картой и эмитентом сэкономить можно на одном участке: прямое соединение шлюза эквайера с ОПКЦ без промежуточных интеграторов сокращает задержку на переходах на 10–30 мс.

Физику не ускорить ничем: сигнал между ЦОДами в разных регионах России идёт туда и обратно от 9 мс (Москва — Санкт-Петербург) до 100 мс и больше (Москва — Хабаровск) [260]; если эмитент — в Москве, а эквайер — во Владивостоке, авторизация выходит за минимальный бюджет. Внутрироссийский маршрут убирает межконтинентальные задержки; в домене синхронной репликации (до 50 км) расстояние между ЦОДами добавляет единицы миллисекунд, а разнесение по зонам доступности и регионам — десятки.

13.6 Что осталось за пределами этого разбора

Разобранная транзакция прошла без сбоев. Отказы, переключения *fallback* и частичные сбои реального потока остались за пределами главы:

Отказ эмитента. Если фаза 9 завершается `Response Code 05` (не обслуживать, *do not honor*), `14` (неверный номер карты, *invalid card number*) или другим кодом отказа — терминал получает короткое MTI 0110 и издаёт сигнал отказа (или показывает сообщение). Логика обработки кодов отказа и реакции эквайера — раздел 6.5.

Сервис Резервной Авторизации ОПКЦ. Если эмитент недоступен, ОПКЦ сам принимает решение по правилам Резервной Авторизации (раздел 13 Правил ПС Мир) [169]. Карта получает одобрение или отказ без участия эмитента; эмитент получает уведомление постфактум. Этот механизм выполняется целиком внутри ОПКЦ и не пересекается с Visa STIP или Mastercard stand-in.

Кобейдж Мир–UnionPay. Если карта — кобейдж Мир–UnionPay и операция проходит за рубежом, транзакция маршрутизируется не через ОПКЦ, а через сеть UnionPay International. На 2026 год эмиссия Мир–UnionPay ограничена несколькими банками, а зарубежный приём резко сужен после внесения НСПК в список SDN. Подробно — раздел 16.1.

Fallback на контактный чип. Если бесконтактный обмен не завершился (карта вышла из поля, FWT превышен), терминал переключается на контактный интерфейс: карта вставляется в слот. APDU те же, физика другая (ISO 7816 вместо ISO 14443), бюджет вырастает до 3–5 секунд — раздел 7.9.

Токен вместо PAN. Если транзакция — через Mir Pay, в DE 2 передаётся не PAN, а токен НСПК. Сервис токенизации НСПК (раздел 16.3) детокенизирует значение и передаёт эмитенту настоящий PAN; ARQC при этом считается ограниченным ключом LUK, который TSP выпускает для DPAN, а не ключом карты (раздел 8.3). Apple Pay и Google Pay для российских карт с 2022 года недоступны [266]; оплата телефоном по NFC в России — это Android: Mir Pay (HCE) и банковские сервисы SberPay и T-Pay [267, 268]; для iPhone — BLE (раздел 8.3). Подробно — гл. 9.

3-D Secure. В бесконтактной транзакции 3DS не участвует — держатель физически присутствует у терминала, и аутентификация уже выполнена через CVM / CDCVM на стороне карты или устройства. 3DS включается только в CNP-сценарии; для карт «Мир» это MirAccept, гл. 11 и раздел 16.4.

Chargeback. Если держатель оспорит операцию через несколько дней или недель, запускается отдельная процедура по правилам ПС Мир: сбор доказательств, арбитраж НСПК. Её разбирает гл. 32.

Часть III

Платёжные системы

После первых двух частей платёжная отрасль выглядит обозримой. Модель движения денег, сообщений и обязательств описана; механизмы доверия, подлинности и защиты данных разобраны; остаётся подставить названия сетей. Именно на этом шаге начинаются дорогие ошибки. Две транзакции выглядят одинаково на экране кассы, проходят через похожие стадии авторизации и используют один и тот же пластик в кошельке, но подчиняются разным правилам, с разным набором документов, разной финальностью расчёта, разной архитектурой маршрутизации и разными последствиями для банка, продавца и процессинга.

Третья часть сравнивает семейства систем: глобальные карточные сети; национальные карточные системы; A2A-системы (см. гл. 21), где платёж опирается на доступ к счёту и согласие клиента. Сравнение идёт по тому, кто владеет правилами, где источник истины, как достигается окончательность расчёта и что меняется для банка, продавца и процессинга.

Сначала — глобальные карточные сети, Visa и Mastercard. Они показывают классическую логику свода правил, авторизационной и клиринговой систем, сертификации и сетевых сервисов. Затем — Мир, UnionPay и национальные карточные сети СНГ: варианты той же карточной модели с ролью национальной инфраструктуры, локального регулирования и политической экономии платёжной сети.

СБП и открытый банкинг работают иначе: оплата опирается на банковский счёт, согласие на доступ и иную семантику окончательности расчёта, без карточного идентификатора и отдельной системы диспутов.

Глубина глав здесь намеренно асимметрична. СБП, Мир, UnionPay и открытый банкинг разобраны подробнее, чем Visa и Mastercard: книга для русскоязычного инженера, глубина пропорциональна релевантности системы. Главы о международных сетях дают опорную модель для сравнения с национальными и A2A; за исчерпывающим описанием читатель идёт в их своды правил.

Конкретное сравнение объясняет, почему системы по-разному обрабатывают диспуты, распределяют риск фрода и поддерживают подписки, требуют разной сертификации и предъявляют разные требования к внутреннему процессингу. То, что в предыдущей части выглядело общим механизмом, здесь получает имя, владельца и свод правил.

Когда своды правил, расчётные модели и системы сопоставлены, вопрос меняется: *что происходит с платёжным потоком в промышленной эксплуатации*, какая бы система за ним ни стояла. Часть IV разбирает фрод, комплаенс, подписки, сверку, диспуты и управление отказами.

14 Visa

В общей четырёхсторонней модели (см. раздел 2.1) Visa задаёт собственную сетевую архитектуру, свод правил, сервисы и требования к приёму карт.

ВАЖНО

Контекст для российского читателя. 5 марта 2022 года Visa объявила о приостановке всех операций в России [269]. Карты Visa, выпущенные российскими банками до этого момента, продолжают приниматься внутри России: внутрироссийские авторизации и клиринг по таким картам идут через операционный и платёжный клиринговый центр Национальной системы платёжных карт (ОПКЦ НСПК; см. гл. 16), минуя VisaNet — глобальную процессинговую сеть Visa, и срок действия карт российские банки продлевают самостоятельно [270]. Международный приём этих карт за пределами РФ прекращён. Глава описывает архитектуру и правила Visa, на которые российские эквайеры и эмитенты ориентируются из-за унаследованных интеграций и требований совместимости; российская специфика после 2022 года разбирается в гл. 16.

14.1 VisaNet: авторизационная сеть и расчётный бэкенд

Авторизация и клиринг разнесены по времени и характеру задачи (см. гл. 5), поэтому Visa обслуживает их в двух независимых сетях. Авторизационная сеть исторически называлась **BASE I**. В современных документах Visa она именуется **V.I.P. System** (VisaNet Integrated Payment) и включает не только BASE I (авторизации из двух сообщений, *dual-message*), но и **SMS (Single Message System)** для сценариев с одним сообщением (*single-message*), исторически — для дебетовых операций Interlink и банкоматных операций Plus [83]. Сеть отложенного клиринга и расчёта по-прежнему называется **BASE II**; денежный расчёт между участниками выполняет отдельная подсистема **VisaNet Settlement Service (VSS)**, логически отделённая от клирингового конвейера BASE II [13, 83]. V.I.P. System авторизует операции в реальном времени с жёстким таймаутом, BASE II принимает пакетные клиринговые инструкции в собственном формате.

Привязка «T+0 — авторизация, T+1 — клиринг» типична для рынка США и ряда крупных эквайеров; Visa Core Rules такой константы не задают: сроки клиринга и расчёта зависят от региона, типа продукта и участника.

Если эмитент недоступен или превышает таймаут ответа, Visa отвечает эквайеру от его имени через **Stand-In Processing (STIP)** по параметрам, согласованных с эмитентом (общий механизм — в разделе 5.1). Параллельно сетевой скоринг рисков **Visa Advanced Authorization (VAA)** оценивает запрос с помощью моделей и передаёт эмитенту оценку риска (см. раздел 14.7).

Для разработчика платёжного шлюза это две интеграции. Авторизационный запрос передаётся в реальном времени по ISO 8583 — международному стандарту сообщений карточных авторизаций (см. гл. 6). Клиринговые записи отправляются отдельным процессом по расписанию; у авторизации и клиринга разные классы ошибок и регламенты обработки.

14.2 Расчётная гарантия сети

В интервале между авторизацией и расчётом эмитент уже подтвердил обязательство заплатить, эквайер уже передал товар, но межбанковский неттинг через VSS

Рис. 38 — Авторизационная сеть BASE I и расчётный бэкенд BASE II.

пройдёт через несколько часов или суток. Если эмитент за это время становится несостоятельным, эквайер остаётся без покрытия.

Правила Visa дают гарантию на этот интервал: сеть обязуется возместить клиенту сети потери от того, что другой клиент не исполнил расчётные обязательства [271]. В годовом отчёте по Form 10-K Visa называет это возмещение потерь при расчёте (*settlement indemnification*); в отчёте за 2017 финансовый год она раскрывала методику оценки экспозиции: среднедневной объём операций по картам, умноженный на оценочное число дней до расчёта плюс защитная маржа, плюс среднее за четыре скользящих месяца по объёму chargeback, плюс остаток непогашенных дорожных чеков Visa [272]. В отчёте за 2023 финансовый год Visa приводит итог: максимальная дневная экспозиция $126{,}9$ млрд USD, средняя — $77{,}1$ млрд USD [271].

Первый уровень покрытия — обеспечение, которое сеть собирает с участников, не прошедших кредитную оценку группы Global Credit Settlement Risk: денежные депозиты в эскроу на имя Visa, заложенные ценные бумаги (хранятся у кастодиана, сеть вправе продать их при дефолте), безотзывные аккредитивы банков клиента и гарантии материнской структуры по обязательствам дочерней [271—273]. Когда обеспечения не хватает, покрытие даёт собственная ликвидность сети: Visa Global Treasury держит достаточно ликвидных активов, чтобы рассчитаться в тот же день даже при дефолте участника с наибольшей нетто-задолженностью, и ежедневно проверяет выполнение этого требования по стандартам BIS [273]. Дополнительную опору даёт собственный капитал Visa Inc.: на 30 сентября 2024 года $12{,}0$ млрд USD в денежных средствах и их эквивалентах и $5{,}4$ млрд USD в долговых ценных бумагах для продажи (Treasury и бумаги агентств правительства США) [273].

Правила Visa (VCR/VPSR) прямо запрещают одностороннюю отмену авторизованных, но ещё не рассчитанных операций даже в случае несостоятельности участника [273]. С октября 2023 года VisaNet официально отнесён Bank of Canada к системно значимым платёжным системам (Prominent Payment System) и подчинён 18 стандартам управления рисками, включая Standard 7 (финальность расчёта) и Standard 9 (правила и процедуры при дефолте участника) [273]. Отдельно от возмещения при расчёте действует соглашение о распределении убытков (*loss sharing agreement*) между Visa, Visa U.S.A., Visa International и частью банков-членов Visa U.S.A.: убытки по судебным делам U.S. covered litigation банки покрывают пропорционально доле членства [272].

У Mastercard конструкция та же: правила сети гарантируют расчёт по значительной части транзакций между клиентами, совокупный расчётный риск (*gross*

settlement exposure) на 31 марта 2024 года оценён в 73,8 млрд USD при необеспеченном риске 61,2 млрд, а участники, не проходящие стандарты управления рисками, вносят денежное обеспечение, аккредитивы или гарантии [274].

Механизм проявился в марте 2023 года при банкротствах Silicon Valley Bank и Signature Bank. На конференции Wolfe Research финансовый директор Visa Васант Прабху и директор по продуктам Mastercard Крейг Восбург подтвердили, что после перехода обоих банков под управление регуляторов расчёт через них все выходные шёл без сбоев, и согласились с описанием своих сетей как страховочной опоры (*back-stop*) для банков при сбоях в обработке платежей [275].

В ПС Мир механизм аналогичный по функции и публично оформлен: Приложение 3 к Правилам ПС Мир — «Методика определения размера гарантийного обеспечения Участника» — задаёт формулу расчёта обязательного депозита, который участник вносит в НСПК пропорционально объёму своих расчётов [276].

Карточный платёж в четырёхсторонней модели свободен от риска контрагента-эмитента: при банкротстве эмитента в интервале между авторизацией и расчётом деньги эквайеру придут из сети — сначала из обеспечения этого эмитента, затем из ликвидной позиции сети, затем из её капитала. В *push*-системах вроде СБП, Pix или FedNow конструкция другая: расчёт мгновенный и идёт в деньгах центрального банка, поэтому расчётного интервала и связанного с ним кредитного риска по отдельной транзакции там нет; вместо него возникают риск ликвидности (покрытие на корсчёте требуется в момент отправки) и операционный риск (при сбое системы платёж отклоняется немедленно: исправить нельзя) — см. гл. 19 и гл. 20.

14.3 Core Rules

При споре, сертификации или разборе инцидента отправная точка — **свод правил Visa (Visa Core Rules and Visa Product and Service Rules)**; его публичная редакция открыта всем, но Visa прямо предупреждает, что из неё исключены проприетарные сведения, коммерчески чувствительные данные и часть значимых для безопасности деталей [13].

Публикация устроена иерархически: **Visa Core Rules** задают общие требования к участию в сети, ответственности сторон и базовым процессам, а **Visa Product and Service Rules** добавляют продуктовые и региональные условия. Технические форматы сообщений, процедуры сертификации и детали сетевой обработки вынесены в отдельные руководства по внедрению (*implementation guides*), на которые правила ссылаются, но содержание которых не пересказывают [13].

За пределами публичной редакции остаются членские соглашения с конкретными банками, дополнительные технические материалы, чувствительные сетевые параметры и индивидуальные коммерческие условия — они дополняют общий свод и участнику доступны через закрытые каналы.

Публичные редакции правил выходят с фиксированной датой вступления в силу (*effective date*); в последние годы это апрельская и октябрьская редакции, и к каждой прилагается сводка изменений Summary of Changes. Оперативные обновления выходят в Visa Merchant Business News Digest: краткие сводки со ссылками на материалы Business News [13, 277]. В споре стороны ссылаются на редакцию, действовавшую на дату операции [13].

Для инженера Core Rules — рабочий документ участника: он показывает обязанности эквайера и эмитента, допустимые сроки клиринга, основания для понижения

категории interchange и момент, когда спор или инцидент становятся нарушением правил сети (см. гл. 25).

ПРАКТИКА

Читать Core Rules лучше от задачи: чтение сверху вниз быстро превращается в поверхностное знакомство. Сначала определите роль — эквайер, эмитент, VisaNet Processor (участник с прямым подключением к VisaNet, обрабатывающий трафик других членов сети) или конкретный продукт. Затем зафиксируйте редакцию документа и дату вступления в силу. После этого ищите локальную норму. Без этой привязки легко сослаться на правило, которое либо относится к другой роли, либо ещё не вступило в силу в нужном регионе.

14.4 TADG и сертификация терминалов

Visa TADG (Transaction Acceptance Device Guide) — *инженерное руководство Visa* по поведению терминала, пользовательскому интерфейсу и сетевым деталям приёма карт; оно дополняет формальные спецификации и тестовые наборы, но не заменяет их. Фраза «терминал сертифицирован под Visa» покрывает проверку аппаратной части, ядра EMV и интеграции устройства с конкретным эквайером.

Уровень 1 (L1) — физический и электрический уровень. Терминал соответствует требованиям к контактному считывателю и бесконтактному интерфейсу. Проверяются аппаратная часть и низкоуровневое взаимодействие с картой [55].

Уровень 2 (L2) — программный уровень, ядро EMV. Терминал правильно реализует логику транзакции EMV: выбор приложения, чтение данных, обработка **TVR (Terminal Verification Results)** — вектора результатов проверок терминала (см. гл. 7), генерация криптограмм. Для контактных устройств нужно одобрение консорциума EMVCo; для части бесконтактных стеков — соответствие **спецификации бесконтактных платежей Visa (Visa Contactless Payment Specification, VCPS)**. На L2 проверяют реализацию сценария приёма целиком [55].

Уровень 3 (L3) — интеграционный уровень. Связка ядра EMV с конкретной системой управления терминалом (**Terminal Management System, TMS**) эквайера и его хостом авторизации. Устройство тестируют в полевой конфигурации: конкретное терминальное приложение, параметры эквайера, маршрутизация авторизаций. На L3 проверяют, как терминал формирует авторизационное сообщение и передаёт поле данных **DE 55** (Integrated Circuit Card data, контейнер EMV-данных в сообщении ISO 8583, см. гл. 6) [55].

Отсюда практическое правило: слово «сертифицирован» обретает смысл только с указанием уровня. Устройство, не поддерживающее нужный сценарий EMV или введённое в сеть с неверной конфигурацией, лишает эквайера защиты в спорах о фроде по тому же механизму переноса ответственности (*liability shift* — перераспределение ответственности за фрод между эмитентом и эквайером в зависимости от технологии приёма), что и в разделе 7.1.

14.5 Visa Token Service

Общая модель сетевых токенов EMVCo и устройство сервиса **Visa Token Service (VTS)** описаны в гл. 9. Здесь — специфика Visa.

VTS предоставляет эмитенту группы интерфейсов: **ID&V** (*Identification & Verification* — процедуры подтверждения личности держателя при выпуске токена), **Token Inquiry** (запрос состояния токена и данных об устройстве и риске) и **Token Lifecycle** (управление жизненным циклом токена) с операциями *activate*,

resume, *suspend* и *delete* [36]. Помимо интерфейсов Visa вводит **Token Assurance Level** (уровень доверия к токену): он присваивается при выпуске по методу ID&V (от *passive* — без активной проверки, до *biometric* — с биометрическим подтверждением) и передаётся эмитенту в каждой авторизации, влияя на решение о риске наряду с **Token Domain Restriction Controls** — ограничениями по каналу, устройству и типу операции, для которых выпущенный токен пригоден (см. раздел 9.3) [36, 174].

14.6 Visa Direct

Обычная карточная покупка движется по модели «дебет у плательщика», в которой авторизация резервирует средства, а клиринг завершает списание. Visa поддерживает и обратный сценарий, когда деньги нужно доставить *держателю карты*. В Visa Direct для этого используется **исходная кредитовая транзакция (Original Credit Transaction, OCT)** — зачисление на счёт, связанный с картой получателя; **AFT (Account Funding Transaction)** при необходимости предварительно списывает средства с карты отправителя [13].

OCT покрывает переводы между физлицами, массовые выплаты, пополнение предоплаченных продуктов и платежи по кредитным картам [278].

OCT отличается от обычной авторизации покупки тем, что деньги зачисляются напрямую на счёт получателя: холда (резервирования суммы на счёте держателя карты до завершения клиринга, см. гл. 5) в OCT нет. Публичная документация Visa оговаривает, что фактическая доступность средств зависит от банка получателя и выбранного коридора. Общая норма Visa — эмитент получателя проводит OCT по счёту не позднее двух рабочих дней после получения; срок «до 30 минут» после одобрения (в США для внутренних OCT — до 60 секунд) задаёт **Fast Funds** — сервис ускоренной доставки средств, обязательный для эмитентов, которые принимают OCT как онлайн-операции [13].

Типовой сценарий — связка OCT и AFT. Если источник средств — карта отправителя, инициатор выплаты сначала выполняет AFT, затем отправляет OCT получателю. AFT и OCT — две отдельные транзакции: между ними возможна пауза в минуты, часы или больше; в это время платформа выплат может выполнять собственную проверку, ждать подтверждения источника или менять источник финансирования [279]. Помимо связки AFT→OCT Visa допускает и другие источники финансирования через Visa Direct: дебет **ACH** (Automated Clearing House — американская сеть межбанковских расчётов с отложенным неттингом) или иной банковский перевод. Такие сценарии не оформляются как AFT и подключаются по отдельным программам.

Онлайн-OCT Visa требует инициировать как Online Financial Transaction: авторизация, клиринг и расчёт проходят одним сообщением через SMS [13]. При обработке из двух сообщений клиринг по AFT и OCT передаётся отдельным потоком через BASE II; Visa Acceptance Solutions передаёт эквайеру одобренные операции в файле захвата TC 33.A для формирования клиринговых записей [280]; схема на рис. 39 отображает только авторизационный поток V.I.P. System.

Перед запуском платформа выплат фиксирует, кто финансирует AFT, какой SLA (*service-level agreement*, формальное соглашение об уровне обслуживания) установлен по OCT, как банк получателя обеспечивает доступность средств и в какой момент ответственность сети сменяется ответственностью участника программы.

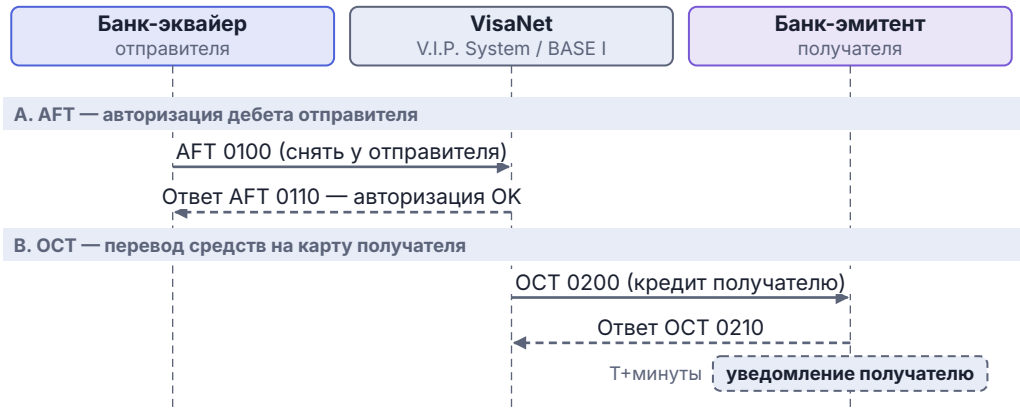


Рис. 39 — Типовой поток Visa Direct: AFT и OCT.

После марта 2022 года Visa Direct как трансграничный продукт для российских участников недоступен: Visa приостановила операции со всеми российскими банками [269], а приём и отправка OCT/AFT за пределы страны не выполняются. Внутрироссийские карточные операции по картам Visa, выпущенным до марта 2022 года, продолжают обслуживаться через НСПК (см. раздел 16.2). Переводы между своими счетами в разных российских банках обслуживают Me2Me Pull (инициирует получатель) и Me2Me Push (инициирует отправитель), выплаты от бизнеса физлицу — B2C-переводы (*business-to-consumer*) Системы быстрых платежей (СБП; см. гл. 19 и раздел 19.2).

14.7 Visa Advanced Authorization

Эмитент, принимающий решение по подозрительной операции, видит только собственный портфель: историю клиента, его поведение и баланс. Весь сетевой поток авторизаций доступен Visa, и на этом построен **сетевой скоринг рисков Visa (Visa Advanced Authorization, VAA)** [13, 281].

По каждому авторизационному запросу сеть в реальном времени рассчитывает числовой показатель риска и передаёт его эмитенту в составе авторизационного сообщения [281].

VAA работает на уровне сети: Visa получает все авторизационные запросы от эквайеров и, прежде чем запрос дойдёт до эмитента, оценивает его с помощью моделей, обученных на сетевом трафике. Модели обнаруживают шаблоны, недоступные отдельному эмитенту, — например, что по той же карте только что прошли авторизации в трёх разных городах.

В одном варианте Visa Risk Manager принимает авторизационное решение автономно, и эмитент делегирует часть логики сети. В другом сеть передаёт оценку риска и набор Risk Condition Codes (кодов выявленных рисковых условий, поясняющих, какие сигналы повлияли на оценку) в авторизационный запрос, а эмитент сам решает, как реагировать, — снизить лимит сессии, запросить дополнительную аутентификацию или одобрить операцию. Точное поле в протоколе VisaNet для этих данных в публичных материалах не раскрыто; команда с доступом к VisaNet Message Specifications сверяется по закрытому документу. Сетевая оценка встраивается в собственную **RBA** эмитента (*risk-based authentication* — адаптивная аутентификация,

при которой требования к подтверждению зависят от оценки риска операции) как ещё один сигнал наряду с историей клиента и данными устройства.

14.8 Interchange Visa: структура таблиц

Общий механизм interchange, разложение MSC и модели тарификации для продавца разобраны в разделе 2.3; ниже — специфика Visa: как организованы программы и почему одна и та же операция может квалифицироваться по разным ставкам.

Таблицы Visa сгруппированы по **программам interchange**, каждая программа — сочетание типа карты (дебетовая, кредитная, коммерческая), категории торгово-сервисного предприятия (ТСП) по **MCC** (Merchant Category Code — четырёхзначный код категории ТСП по ISO 18245) и канала транзакции (карта предъявлена, электронная коммерция, бесконтактный приём) [21]. Для ТСП с MCC 5411 действует одна ставка для дебетовых карт, другая для кредитных и третья для коммерческих; внутри этих веток заданы дополнительные квалифицирующие условия по данным и способу приёма.

Понижение программы (*downgrade*) свойственно interchange любой сети; в таблицах Visa оно выражено через явные пары программ: транзакция, удовлетворяющая условиям лучшей программы, квалифицируется как «qualified»; при недостатке данных или несоответствии сценария квалифицируется как «non-qualified» с более дорогой ставкой.

Интересы сторон в таблице interchange Visa расходятся. Эмитенту выгодна программа выше: каждая ступень дороже для эквайера и выгоднее эмитенту. Эквайеру выгодна программа ниже: правильно собранный авторизационный и клиринговый пакет данных удерживает сделку в дешёвой программе. Продавец влияет только через MCC и канал приёма, причём косвенно: MCC присваивает эквайер по Visa Merchant Data Standards Manual [43]. Региональные редакции таблиц выходят дважды в год, с фиксированной датой вступления и сводкой изменений; ставка по конкретной операции применяется на дату обработки эквайером, а не на дату покупки. Программа CPS в США и её аналоги в других регионах — это «лучшая» категория с самыми жёсткими требованиями к данным; переход в EIRF или Standard IRF (Standard Interchange Reimbursement Fee — максимальная по стоимости категория downgrade Visa для операций, не прошедших по EIRF) означает, что одно из условий не выполнено.

Допустим, ТСП с MCC 5912 (аптека, *drugstore*) принимает на рынке США чиповую дебетовую карту Visa на $100, выпущенную эмитентом, освобождённым от Regulation II ФРС США (*exempt*). Для регулируемой карты обе программы ниже дают одну ставку 0,05 % + $0,21, и понижения нет. При корректной передаче DE 55 с данными EMV транзакция квалифицируется в программе **CPS**/Retail (Custom Payment Service — группа программ interchange Visa с расширенными требованиями к данным авторизации и клиринга) со ставкой порядка 0,80 % + $0,15, и эквайер перечисляет эмитенту примерно $0,95 [21]. Если из-за ошибки терминала или хоста DE 55 не попадает в клиринговое сообщение, операция квалифицируется по категории **EIRF** (Electronic Interchange Reimbursement Fee — общая категория interchange Visa для электронных операций без квалифицирующих признаков лучших программ) с более высокой ставкой около 1,75 % + $0,20, и interchange вырастает примерно до $1,95. Разница порядка $1,00 на одной операции; при 10 000 транзакций в месяц downgrade обходится продавцу около $120 000 в год. Конкретные ставки и потолки

сверяются по актуальной редакции таблицы Visa Interchange Rates. Диагностика downgrade начинается с проверки, попал ли DE 55 в клиринговый файл. Авторизационный лог может показывать данные EMV, но если хост эквайера не передал их в BASE II, понижение всё равно произойдёт [13, 55].

Видимость downgrade в выписке зависит от тарифной модели эквайера (Interchange++, *flat rate*, *tiered*): в Interchange++ понижение программы видно сразу, в *flat rate* оно растворяется в усреднённой ставке.

ВАЖНО

Потеря контекста EMV — это и риск фрода, и фактор interchange. Таблицы Visa различают *card-present* (операция при физическом предъявлении карты на терминале), *key-entry* (ручной ввод реквизитов оператором терминала) и общие категории (EIRF, Standard IRF); операция без ожидаемых данных или вне сценария *card-present* квалифицируется дороже [21, 55].

ПРАКТИКА

Чтобы найти программу interchange для конкретной транзакции в документе Visa Interchange Rates, удобно двигаться от общего к частному. Сначала выбирают регион и дату вступления в силу таблицы. Затем определяют тип карты, категорию ТСП и канал приёма. После этого читают квалифицирующие условия рядом со ставкой — какие именно данные должны быть переданы в сообщении, нужен ли контекст EMV, есть ли отдельные условия для электронной коммерции или бесконтактного приёма.

15 Mastercard

От Visa Mastercard отличается единой сетевой архитектурой, форматами GCMS (Global Clearing Management System) и IPM (Integrated Product Messages), токенизацией через MDES (Mastercard Digital Enablement Service), механизмом DSRP (Digital Secure Remote Payments) и сервисом ABU (Automatic Billing Updater) — при общей четырёхсторонней модели (см. раздел 2.1), общем EMV и похожих таблицах interchange.

ВАЖНО

Контекст для российского читателя. С марта 2022 года Mastercard приостановила обслуживание российских банков для новых международных операций [282]. Карты Mastercard, выпущенные российскими банками до этого момента, продолжают приниматься внутри России. Авторизации и клиринг по таким картам внутри страны проходят через операционный и платёжный клиринговый центр НСПК (ОПКЦ НСПК), минуя Banknet — глобальную сеть Mastercard для авторизации, клиринга и расчёта; сроки действия продлевают российские банки-эмитенты [270]. За пределами РФ эти карты не принимаются. Унаследованная инфраструктура эквайеров в России построена по логике Mastercard, поэтому знание архитектуры и правил сети сохраняет практическую ценность; российские изменения после 2022 года разбираются в гл. 16.

15.1 Сеть Mastercard

Сеть Mastercard исторически называется Banknet (см. рис. 40) — именно через него проходят авторизация, клиринг и расчёт между участниками. У Mastercard эти три фазы разнесены во времени и в требованиях к латентности (см. гл. 5), и каждую обслуживает своя подсистема. За авторизацию отвечает Authorization Platform, за клиринг — Global Clearing Management System (GCMS), за расчёт — Settlement Account Management (SAM) [283].

Для участника это единая сеть, но интеграция с каждой подсистемой отдельная: сертификация и тестовые среды у каждой свои [15].

Подсистемы не резервируют друг друга: при недоступности Authorization Platform трафик не уходит в клиринг, и наоборот. Сбой авторизации обрабатывает механизм *stand-in*, иначе запрос получает отказ; на альтернативную сеть трафик не переключается [283]. Stand-In Processing (STIP), не отражённый на рис. 40, работает у Mastercard по той же логике, что и у Visa (см. раздел 5.1): Authorization Platform отвечает вместо эмитента по заранее согласованным параметрам [283].

Участники подключаются к Authorization Platform и GCMS не напрямую, а через региональный граничный (*edge*) узел Mastercard Interface Processor (MIP), обеспечивающий шифрование канала, маршрутизацию и базовую буферизацию обмена [283].

15.2 Dual message: IPM против TC33

Модель *dual message* разобрана в разделе 5.4. В Mastercard авторизационный диалог ведут сообщения MTI 0100/MTI 0110 (MTI — message type identifier, четырёхзначный код типа сообщения ISO 8583); на клиринговом этапе эквайер формирует для GCMS интегрированные продуктовые сообщения IPM 1240 (Integrated Product Messages). TC33 (формат пакетного клирингового файла Visa BASE II), как у Visa,

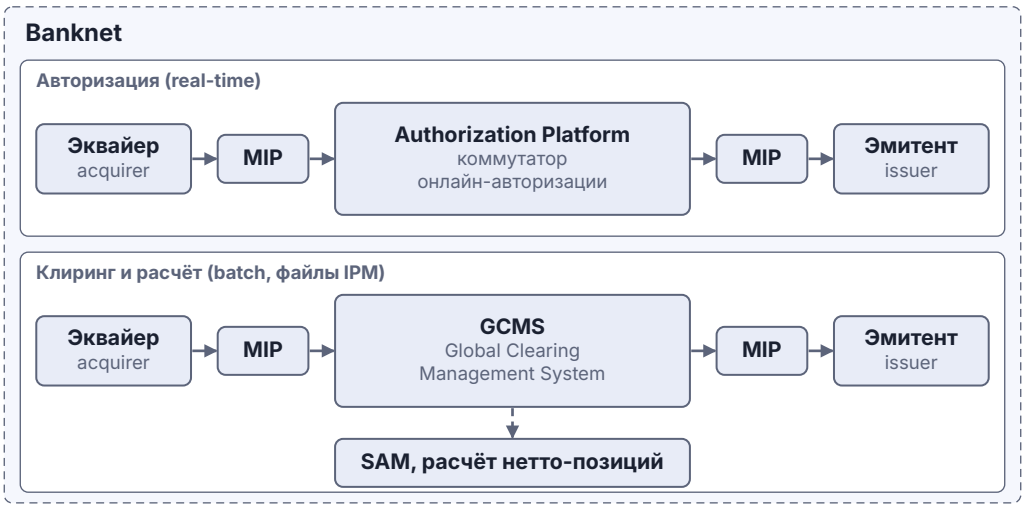


Рис. 40 — Топология логических подсистем сети Mastercard.

здесь не применяется [38]. IPM-файл собирает эквайер на основании авторизованных операций, принятых к финансовому представлению. Authorization Platform IPM не генерирует: она формирует авторизационные ответы, на которые опирается клиринг.

Наборы полей в авторизации и в клиринге различаются. IPM построен на ISO 8583:1993, и под одним номером поля там бывает другой элемент: DE25 (DE — data element, элемент данных ISO 8583 с указанным номером поля; см. гл. 6) в IPM несёт Message Reason Code, DE48 в авторизации несёт подэлементы, а в IPM — приватные подэлементы PDS [14]. DE25 и DE48 — только примеры полей с расхождением; полный набор шире и включает DE2/3/4/14/22/43/48/49/61, а также PDS-блоки (PDS — private data subelement, приватные подэлементы данных Mastercard внутри расширяемых полей IPM) внутри IPM. Данные, попавшие в *first presentment* (первое клиринговое представление операции эквайером в адрес эмитента), видны только в клиринге, в авторизационном логе их нет; по ним и проверяют клиринговый отказ [38].

ВАЖНО

В Visa и Mastercard *dual message* опирается на одну идею, но инженерная единица клиринга разная: у Visa BASE II/TC33, у Mastercard GCMS/IPM. Типичная ошибка — трактовать IPM как переименованный TC33; клиринговый конвейер Mastercard требует отдельной логики формирования и разбора ответов.

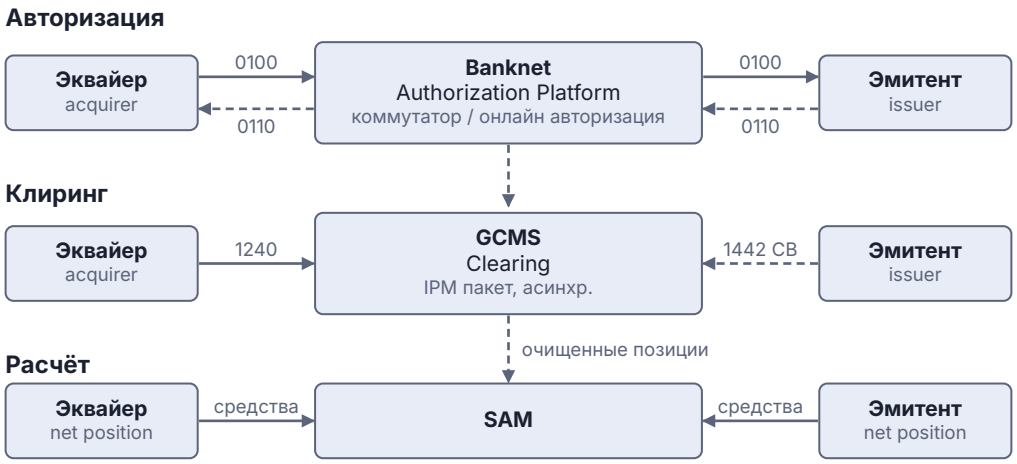


Рис. 41 — Фазы Mastercard: авторизация (Banknet), клиринг (GCMS) и расчёт (SAM).

15.3 IPM и GCMS

GCMS принимает и маршрутизирует клиринговые данные в формате IPM (интегрированные продуктовые сообщения для клиринга и связанной с ним обработки) [283].

IPM — клиринговый формат со своими типами сообщений и элементами данных [38]. Спецификация записей, подэлементов и служебных заголовков описана в документации Mastercard для участников; публичные материалы сети подтверждают формат IPM и роль GCMS, но полного атласа полей для построчного разбора не дают.

Таблица 28 — Структура обмена IPM Mastercard.

Уровень	Описание
Файл IPM	Контейнер клирингового обмена
Клиринговая запись	Единица обмена внутри файла
Message header	Служебный заголовок записи
ISO 8583 data elements	Элементы данных транзакции
Fees / adjustments	Комиссии и корректировки

First presentment в IPM использует MTI 1240 вместо привычного авторизационного 0100. IPM работает пакетно: получатель принимает файл целиком и обрабатывает содержимое асинхронно. Ответа 1250 на каждую запись 1240 нет: MTI 1644 обозначает административные сообщения — заголовок (1644-697) и концевик (1644-695) файла, подтверждения приёма и сверочные сообщения GCMS (например, Financial Position Detail 1644-685), на которых строится сверка [14].

1240 — *directed*-сообщение без смыслового ответа уровня клиринга: в обычном сценарии *first presentment* закрывается расчётом нетто-позиции через SAM. IPM 1442 *first chargeback* — не ответ на 1240, а самостоятельная инициатива эмитента при споре клиента, со своими основаниями и сроками; 1442 — тоже *directed*-сообщение, а возражение эквайера — 1240 *second presentment* с функциональным кодом 205

(полная сумма) или 282 (часть) [38, 46]. Из элементов данных IPM для разбора важнее других DE48 — дополнительные данные в виде PDS, включая данные токена, идентификатор типа транзакции и дополнительные данные ТСП, и DE63 Transaction Life Cycle ID, Trace ID которого связывает клиринговую запись с авторизацией [14]. Структуры авторизации и клиринга различаются, поэтому клиринговому разбору нужен собственный парсер.

До марта 2022 года Mastercard обслуживала внутрироссийские транзакции. Для покупки на 5 000 руб. через чиповый терминал эквайер формировал в клиринговом файле запись MTI 1240, *first presentment*; заголовок содержал Member Message Text и процедурные поля, идентифицирующие участника и цикл обработки. Затем следовали элементы данных — DE 2 с PAN, DE 4 с суммой в формате `000000500000`, DE 49 с кодом валюты 643, DE 22 Point of Service Data Code со способом ввода с чипа, DE 48 с PDS, например PDS 0208 Additional Merchant Data. DE 63 Transaction Life Cycle ID нёс Trace ID — Banknet Reference Number и дату из авторизации [14]. Отдельными записями проходили комиссии: interchange fee в валюте расчёта и assessment fee сети [38].

Если эмитент оспаривает транзакцию, он создаёт *first chargeback* (IPM 1442 в адрес эквайера), ссылающийся на тот же DE 63 Transaction Life Cycle ID и Acquirer Reference Number (ARN — уникальный идентификатор операции, присваиваемый эквайером для сверки клиринга и спора). Эквайер получает *chargeback* в следующем клиринговом файле; для *second presentment* (повторное представление эквайером после *first chargeback*) он формирует IPM 1240 с соответствующим *function code* 205 или 282 (коды цели сообщения IPM второго представления) и передаёт доказательства через Mastercard Connect — корпоративный портал Mastercard для участников сети с доступом к документации и сервисам [38].

Код рекомендации для ТСП (Merchant Advice Code, MAC) сеть передаёт в авторизационном ответе в DE 48, subelement 84 для поддерживаемых сценариев [46]. По нему ТСП или шлюз решает, повторять ли попытку, обновлять ли реквизиты или прекращать автоматические списания.

По результатам клиринга сеть рассчитывает нетто-позиции участников и передаёт их в расчётный процесс; конкретные сроки и порядок урегулирования задают правила региона и роль участника [15]. В период между авторизацией и расчётом сеть несёт расчётный риск: правила Mastercard прямо гарантируют расчёт по многим транзакциям между участниками, совокупный расчётный риск (*gross settlement exposure*) на 31 марта 2024 года оценивается в $73{,}8$ млрд USD при необеспеченном риске $61{,}2$ млрд [274]. Участники с повышенным риском вносят денежное обеспечение, аккредитивы или гарантии [274]; механизм аналогичен механизму Visa и подробнее разобран в разделе 14.2.

15.4 Собственные реализации: M/Chip и MDES

Поверх стандартов EMVCo Mastercard добавляет требования сети: M/Chip задаёт чиповое приложение на карте, MDES — токенизацию и удалённую оплату. Терминальную сторону бесконтактного приёма карт Mastercard описывает ядро Kernel 2 из EMVCo Book C-2 [108].

Семейство M/Chip поверх стандарта EMV (гл. 7) добавляет правила Mastercard для поведения приложения и отдельную процедуру сертификации [284]. В нём есть контактный и бесконтактный профили; M/Chip Contactless разобран в разделе 8.2. Каждый профиль добавляет свой набор тегов, правил офлайн-поведения и тестовых

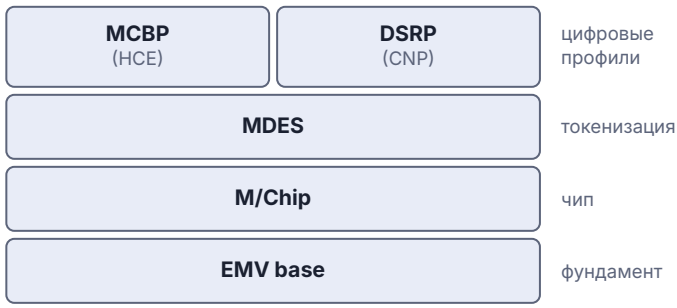


Рис. 42 — От EMV base к M/Chip и DSRP.

сценариев. Поэтому терминал с поддержкой EMV не начинает работать с Mastercard автоматически: нужны требования сети и их проверка. Матрицу профилей M/Chip сверяют через Mastercard Connect; в открытом доступе полной матрицы нет. Типичный сертификационный риск: терминал проходит EMVCo Level 2 (см. гл. 7), но проваливает тесты M/Chip из-за расхождения в обработке конкретных тегов или логике CVM (cardholder verification method).

Модель сетевого токена и MDES как Token Service Provider описана в гл. 9. В MDES у Mastercard есть встроенный механизм защищённой удалённой оплаты DSRP (Digital Secure Remote Payments): он принимает интернет-платежи и платежи в приложениях с опорой на криптографию EMV [46]. DSRP формирует криптограмму для каждой операции CNP (card-not-present, без физического предъявления карты) и даёт эмитенту более сильное подтверждение подлинности, чем обычный сценарий сохранённых реквизитов [177]. Какой именно набор криптограмм и полей пришлёт клиентский кошелёк, зависит от его реализации; Mastercard публично не фиксирует единый профиль для всех Token Requestors — зарегистрированных запрашивающих токены сторон (кошельков, эквайеров, ТСП).

В мобильных сценариях место выработки криптограммы задаёт модель кошелька: при Secure Element (SE) или Host Card Emulation с локальными ключами она формируется на самом устройстве, при облачном профиле (MCBP) ключи держателя остаются в инфраструктуре TSP (Token Service Provider), а устройство получает пакет одноразовых сессионных ключей и по ним вычисляет криптограмму само [285]. Для сети поле криптограммы выглядит одинаково, но эксплуатационные риски, требования к аттестации устройства и поведение в офлайне различаются.

Эти реализации надстраиваются над базовым EMV: M/Chip даёт чиповый профиль, MDES — сетевые токены, а поверх токенов работают цифровые профили — облачный Mastercard Cloud-Based Payments (MCBP) и удалённый DSRP (рис. 42). Схема охватывает чиповый профиль и токенизацию; CNP-сценарии Mastercard шире: аутентификация держателя при онлайн-оплате (3-D Secure 2, см. гл. 11) и Click to Pay поверх EMVCo SRC (Secure Remote Commerce — стандарт EMVCo для упрощённого онлайн-оформления заказа) на ней не показаны.

15.5 Mastercard Send

Mastercard Send — сервис выплат и переводов: он зачисляет средства получателю на карту, банковский счёт, цифровой кошелёк или иной канал, поддерживаемый конкретной программой [286].

Выплаты физлицам от бизнеса (*disbursements*) — зарплаты, страховые возмещения, выплаты ТСП маркетплейса и платформ разовой занятости (*gig*). P2P-переводы проходят между физическими лицами как внутри страны, так и в международных коридорах. В карточном сценарии платформа сначала проводит Funding Transaction (резервирует средства отправителя), а затем Payment Transaction — кредитовую операцию в адрес получателя [46].

Авторизационный запрос на выплату несёт признаки Payment Transaction: значение 28 в DE3 Processing Code вместо кода покупки, Transaction Category Code P в DE48 и Transaction Type Identifier в DE48, subelement 77; транзакция кредитует получателя, а не дебетует карту [46]. Для транзакции *Send* процессингу нужна отдельная ветка логики: парсер, настроенный только на покупки и возвраты, её не обработает.

Visa Direct использует ту же *push*-модель с парой Funding/Payment Transaction, но с другими полями и процедурами участника. Различаются источники финансирования и нормы окончательности расчёта (*finality*): в коридорах почти реального времени (*near real-time*) Mastercard Send зачисляет выплаты почти в реальном времени, тогда как фактическая доступность средств у получателя зависит от банка-получателя [286].

Для российского рынка после марта 2022 года Mastercard Send как трансграничный (*cross-border*) продукт для участников из РФ недоступен. Внутренние операции по картам Mastercard, выпущенным российскими банками до марта 2022 года, продолжают обслуживаться через НСПК (см. раздел 16.2). В РФ 2026 года для выплат на карту физлицу доступны B2C-переводы (от бизнеса физлицу) Системы быстрых платежей (СБП; см. гл. 19); для переводов между своими счетами — Me2Me Pull (банк-получатель запрашивает средства со счёта в другом банке) и Me2Me Push (отправитель переводит средства на свой счёт в другом банке; см. раздел 19.2).

ПРАКТИКА

Формулировка *near real-time* в маркетинге Mastercard Send не гарантирует фактической доступности средств получателю: сверяйте конкретный коридор и SLA банка или провайдера-получателя.

15.6 ABU: автоматическое обновление данных карты

Модель обновления реквизитов после перевыпуска карты, обе модели интеграции (пакетная и через API в реальном времени), сетевые токены как альтернатива и аналог Visa Account Updater (VAU) разобраны в разделе 30.5. Automatic Billing Updater (ABU) у Mastercard отличается ограничениями охвата. Правила обязывают эмитента участвовать в ABU, но выводят из обязательного охвата неперезаряжаемые предоплаченные карты, одноразовые счета для удалённых операций и коммерческие карты, кроме карт малого бизнеса; региональные модификации правил меняют этот перечень [46, 287]. Нормативные технические требования Mastercard (Transaction Processing Rules, TPR), на которые ссылаются этот и следующие разделы, доступны участникам сети через Mastercard Connect [46].

Платформа, работающая и в Visa, и в Mastercard, поддерживает оба сервиса отдельно: процедуры ABU и VAU не совпадают по форматам файлов, SLA и правилам отклика эмитента.

Альтернатива ABU — сетевые токены MDES: сам токен (DPAN) остаётся стабильным, а его привязку к базовому PAN (FPAN) при перевыпуске карты обновляет TSP. В рекуррентных сценариях с сохранёнными токенами рассылка обновлений эквайерам и ТСП через ABU не нужна.

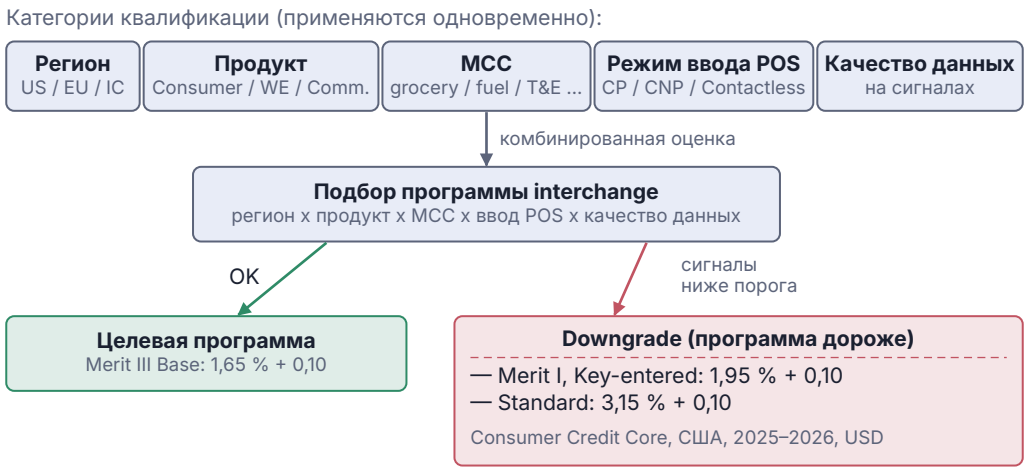


Рис. 43 — Дерево квалификации interchange: от региона до downgrade.

15.7 Interchange Mastercard

Схема квалификации interchange (регион → продукт → MCC → канал → квалифицирующие условия → downgrade), MSC и тарифные модели для ТСП разобраны в разделе 2.3 и применимы к Mastercard без изменений [22]. Своё у Mastercard здесь семейство требований *Data Quality*, ступенчатый downgrade и правила о *fallback* на магнитную полосу.

Признаки, по которым сеть квалифицирует транзакцию, Mastercard объединяет под именем *Data Quality*: ECI (electronic commerce indicator)/CVV2 (Card Verification Value 2)/ AVS (Address Verification Service) для CNP (см. гл. 11), сроки авторизации и клиринга, POS Entry Mode и результат CVM (cardholder verification method) для card-present, признаки card-on-file (сохранённые у ТСП реквизиты для повторных списаний; см. гл. 9) и сетевого токена. Нарушение обязательного для программы признака смещает транзакцию в менее выгодную программу [22].

Downgrade возникает, когда транзакции не хватает квалифицирующих признаков для целевой программы. Среди причин downgrade — отсутствие ECI, неполные данные в DE48, пропущенная проверка AVS или позднее представление в клиринг (*late presentment* — позже сроков, заданных правилами сети). Downgrade применяется ступенчато: каждый пропущенный признак опускает транзакцию на одну ступень по шкале ставок, в предельном случае — в программу Standard (3,15 % + 0,10 USD по consumer credit в США), самую дорогую из общих программ [76].

Для аудита downgrade нужны клиринговые данные: квалификация происходит на этапе клиринга, и в файле IPM видно, какую программу присвоила сеть и каких признаков не хватило [22].

С 1 апреля 2026 года Mastercard взимает с эквайеров в США сбор Fallback Avoidance по картам Mastercard core (основной кредитно-дебетовый бренд) и Maestro (исторический дебетовый бренд Mastercard) — 0,10 % от суммы за авторизованный *fallback* на магнитную полосу, когда карту с чипом принимает чиповый терминал [288, 289].

Ставки Mastercard и Visa сравнимы только с привязкой к рынку, дате публикации и публичной региональной таблице: соотношение зависит от рыночных правил, частных договорённостей и редакции тарифов. Тезис, что премиальный продукт

Mastercard *всегда* дороже сопоставимого продукта Visa, без такой привязки не проверяется. Для рынка США Mastercard публикует отдельные таблицы ставок и критериев interchange, и любой численный пример ссылается на конкретную таблицу [22].

15.8 Отличия от Visa

Различия между Mastercard и Visa делятся на терминологические, исторические и инженерные. Первые два типа влияют на словарь и контекст; инженерные определяют, какой код придётся переписать при переносе системы с одной сети на другую. Сравнение Mastercard, Visa и UnionPay по компонентам сведено в таблицу 29 в гл. 17.

Для переноса кода ключевые различия — клиринговая модель и формат обмена. При переносе обработки клиринга с одной сети на другую переименованием полей не обойтись: IPM и TC33 требуют отдельного парсинга и отдельной диагностики отказов. Токенизация затрагивает кошельки и интернет-платёжные интеграции; ABU и VAU — платформы рекуррентных платежей.

Термин «dual message» применяют и к Visa, и к Mastercard, и формула «авторизация и клиринг разделены во времени» верна для обеих сетей, но детали разделения и техническая реализация у них расходятся.

TSP у Mastercard — это MDES с криптограммой DSRP поверх EMV, а у Visa — VTS с Token Assurance Level; эквайер и кошелёк поддерживают две независимые интеграции и две процедуры регистрации Token Requestor. Платформа, работающая в обеих сетях, проходит две сертификации и ведёт два процесса эксплуатации: правила сетей публикуются в разной форме, графики релизов расходятся, и команда отслеживает обновления Mastercard Connect и Visa Online (VOL, корпоративный портал Visa для участников сети) параллельно.

ПРАКТИКА

Для диагностики отказов Mastercard нужно проверять код отказа и Merchant Advice Code в авторизационном ответе (DE 48, SE 84), а не в клиринговых сообщениях IPM: MAC показывает, допустимы ли повторы и нужно ли обновлять сохранённые реквизиты [46].

16 Мир

Внутрироссийские транзакции по картам «Мир» остаются внутри страны, а криптография опирается на отечественные алгоритмы. Из этих условий следуют маршрутизация через ОПКЦ, ГОСТ-криптография на чипе и собственный TSP в Mir Pay.

16.1 История НСПК

Весной 2014 года санкции против ряда российских банков отрезали их карты от процессинга Visa и Mastercard. Внутрироссийский карточный оборот оказался в прямой зависимости от внешних операторов [5, 17].

НСПК (Национальная система платёжных карт) — оператор платёжной системы «Мир»; через её операционную и платёжную клиринговую систему проходят внутрироссийские карточные операции всех платёжных систем. НСПК создана 23 июля 2014 года. С 2015 года внутрироссийские операции по картам международных платёжных систем начали проходить через ОПКЦ (операционный и платёжный клиринговый центр; см. раздел 16.2) НСПК: соглашение с Mastercard о переводе внутрироссийского процессинга подписано 30 декабря 2014 года, операционный переход банков завершился к 1 апреля 2015 года; для Visa полный переход завершён 27 мая 2015 года [290, 291]. Платёжная система «Мир» запущена 15 декабря 2015 года; первые карты представили семь банков [17, 292].

С 2018 года карты «Мир» вышли в массовый оборот [292]. Закон обязал использовать их для ряда бюджетных выплат, а крупные торгово-сервисные предприятия — принимать [1, 293, 294].

Название «Мир» относится к разным сущностям. Мир — платёжная система. НСПК — её оператор и ОПКЦ. Банк России — расчётный центр для операций между российскими участниками; для иностранных участников расчёты ведёт Банк ВТБ или иные кредитные организации, привлечённые оператором (см. раздел 1.3.2 Правил ПС Мир) [1, 17, 169].

Кобейдж: Мир–UnionPay и Мир–JCB

Кобейдж связывает внутренний маршрут системы Мир с внешним маршрутом партнёрской системы там, где инфраструктура Мир не подключена. НСПК выпускала кобейдж с UnionPay и JCB (Japan Credit Bureau, японская международная карточная сеть); первая карта Мир–JCB вышла в августе 2016 года [103, 295]. С 14 марта 2022 года JCB International приостановила обслуживание российских карт за рубежом, и выпуск Мир–JCB российскими банками прекратился [296].

Внутри России кобейдж обрабатывается через сеть Мир, за пределами — через сеть партнёра, если этот маршрут подключён конкретным эквайером и эмитентом. Страна приёма не задаёт маршрут сама по себе: приоритет определяет процедура выбора приложения (Combination Selection по EMV Contactless Book B [254]; для контактного интерфейса — Application Selection по EMV Book 1 [91]; см. гл. 8) по AID (application identifier — идентификатор платёжного приложения на чипе по ISO/IEC 7816 [132]), затем терминал учитывает поддерживаемые ядра (kernel — компонент терминала, реализующий специфичную для сети логику бесконтактного

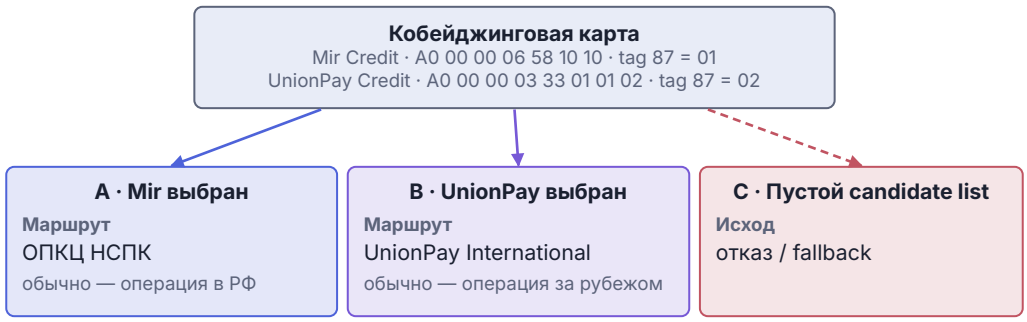


Рис. 44 — Исходы кобейджа Мир–UnionPay: ОПКЦ НСПК, UnionPay International, пустой список приложений.

EMV; см. гл. 7), валюта операции и MCC (merchant category code). Возможен *третий исход* на стадии выбора приложения — пустой список приложений (*candidate list*): терминал не поддерживает ни Mir Kernel, ни UICS (UnionPay International Chip Specification — чиповая спецификация UnionPay), AID-наборы не пересекаются, и операция отклоняется до GPO либо терминал выполняет *fallback* по своей конфигурации. Отказ по BIN-диапазону (bank identification number, старшие цифры PAN; ISO/IEC 7812) при блокировке российских эмитентов UnionPay International или иностранным эквайером — отдельный шаг: BIN читается из Track 2 Equivalent Data только после READ RECORD (штатный EMV-сценарий) или сразу из трека при *fallback*; решение принимает эквайер либо сеть UnionPay, а не процедура Combination Selection. Раздел 17.7 отдельно разбирает устройство Мир–UnionPay: сценарии отказа, маршрутизацию по AID и тестирование комбинации «карта × терминал × страна × канал».

На 2025 год эмиссия Мир–UnionPay ограничена несколькими банками, а международный приём резко сузился: 23 февраля 2024 года OFAC внёс НСПК в список SDN [252], и зарубежные эквайеры стали отказывать в обслуживании карт российских эмитентов независимо от бренда на лицевой стороне.

16.2 ОПКЦ

ОПКЦ (операционный и платёжный клиринговый центр) — инфраструктурный узел, через который проходят внутрироссийские карточные транзакции. С 2015 года через ОПКЦ маршрутизируются и внутрироссийские транзакции по картам иностранных сетей: бренд остаётся на лицевой стороне карты, операционная обработка идёт через НСПК [5, 17]. После приостановки операций Visa и Mastercard в марте 2022 года карты этих сетей, выпущенные российскими банками, работают только внутри страны, через НСПК [138].

Терминал отправляет авторизационный запрос в эквайера, тот направляет его в ОПКЦ. ОПКЦ идентифицирует эмитента по BIN (старшим цифрам PAN, primary account number; см. ISO/IEC 7812 [54]), маршрутизирует запрос в эмитента и возвращает ответ тем же путём к терминалу. После авторизации ОПКЦ собирает клиринговую информацию. В аббревиатуре ОПКЦ соединены операционная функция (маршрутизация авторизационных сообщений в реальном времени) и платёжно-клиринговая (формирование клиринговых позиций участников). На рис. 45 обе функции совмещены в одном узле. ОПКЦ НСПК ведёт операционный и платёжный клиринг, а расчёт по операциям между российскими участниками завершает Банк

России; для иностранных участников расчётным центром выступает Банк ВТБ либо иные кредитные организации, привлечённые оператором (раздел 1.3.2 Правил ПС Мир) [1, 7, 169].

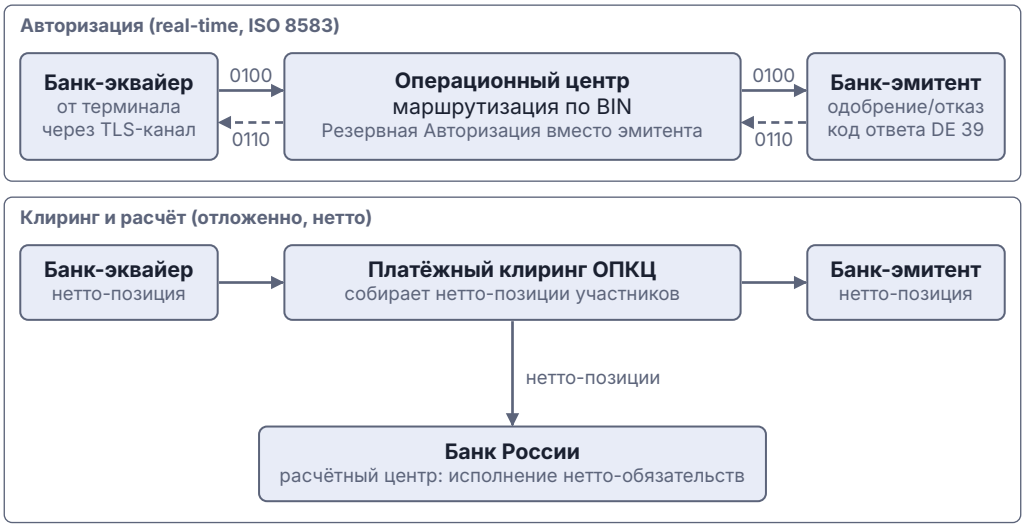


Рис. 45 — Маршрут карточной транзакции через ОПКЦ НСПК: эквайер, обработка, эмитент, расчётный центр.

Протокол обмена между ОПКЦ и участниками основан на ISO 8583 (международный стандарт сообщений карточных авторизаций [74]); состав и интерпретацию полей задаёт собственный профиль сообщений НСПК.

Держатель прикладывает карту Мир к POS-терминалу. Терминал выбирает платёжное приложение Мир по AID из RID (registered application provider identifier, первые пять байт AID) НСПК `0xA000000658` [132, 297], считывает чиповые данные и формирует авторизационный запрос.[1] Эквайер заполняет сообщение MTI 0100 (message type indicator — тип сообщения ISO 8583) по профилю НСПК через нумерованные поля DE (data element [74]): DE 2 (PAN, primary account number, из диапазона 2200–2204 по ISO/IEC 7812 [54]), DE 4 (сумма), DE 22 (POS Entry Mode — способ ввода реквизитов карты на терминале), DE 55 (EMV data, включая криптограмму по правилам платёжного приложения Мир). Эквайер передаёт сообщение в ОПКЦ по выделенному каналу. ОПКЦ ищет эмитента по BIN в собственной таблице маршрутизации и пересылает запрос на хост эмитента. HSM (hardware security module — аппаратный модуль безопасности; см. гл. 10) эмитента верифицирует криптограмму по согласованной с НСПК схеме ключей, хост принимает решение и возвращает MTI 0110 с кодом DE 39 через ОПКЦ обратно эквайеру [1, 17].

Хостовый модуль банка, работавшего с Visa или Mastercard до 2022 года, требует адаптации под ОПКЦ: профили полей, коды ответов и правила заполнения отличаются. Подключение хоста к ОПКЦ оформляется отдельно, с собственными ключами, тестовой средой и сертификацией.

Когда эмитент недоступен, ОПКЦ принимает решение об авторизации вместо него по параметрам, которые эмитент заранее согласовал с НСПК. В Правилах ПС Мир этот механизм называется *Сервисом Резервной Авторизации* (раздел 13) [169];

[1] Поля и значения ниже описывают типичный профиль ISO 8583; полная спецификация полей НСПК и коды расширений — закрытая документация для участников.

международный аналог — *stand-in*. Эмитент задаёт лимит на сумму одной операции, накопительные лимиты сумм и количества операций по карте за заданный период; устаревшие параметры порождают отказы, которые трудно диагностировать. Резервная Авторизация в ОПКЦ замкнута внутри российской системы: ни Visa STIP, ни Mastercard *stand-in* processing к ней отношения не имеют. Набор разрешённых сценариев определяют правила платёжной системы «Мир» [75, 169].

Клиринг в ОПКЦ работает по расписанию, зафиксированному в правилах платёжной системы [75]. Авторизации, накопленные за операционный день, формируют клиринговую позицию, а расчёт между участниками завершает Банк России [1, 7]. Продавцу и PSP нужно различать авторизацию и расчёт: обещанный срок зачисления отсчитывается от клирингового цикла, в который попала транзакция, а не от одобрения.

16.3 Mir Pay после 2022 года

После 2022 года мобильная оплата по картам «Мир» работает через Mir Pay — приложение для устройств под управлением Android с NFC [37, 298]. Для держателя это обычная оплата телефоном; внутри — сервис токенизации НСПК, который выпускает одноразовые платёжные данные в привязке к устройству, опираясь на криптографию НСПК (вместо VTS или MDES; общая модель сетевой токенизации — в разделе 9.5).

НСПК потребовался собственный TSP (token service provider — провайдер сетевой токенизации; см. гл. 9): внешние варианты либо закрыты для Мир, либо сохраняют зависимость от Visa и Mastercard. Apple не открывает Secure Element iPhone сторонним платёжным системам: Apple Pay работает только с TSP, которые Apple интегрировала сама — VTS, MDES и ограниченный набор локальных провайдеров [141]. После приостановки Apple Pay для российских карт в 2022 году канал SE на iPhone стал для Мир недоступен. Использование VTS или MDES сохраняло бы зависимость внутреннего рынка от Visa и Mastercard, которую НСПК должна была устранить. Mir Pay работает через HCE (Host Card Emulation) на Android и не требует доступа к аппаратному SE [37, 298].

Mir Pay распространяется как Android-приложение для смартфонов с NFC; минимально поддерживаемая версия Android и каналы дистрибуции меняются вслед за политикой НСПК и магазинов приложений. Карту можно добавить, только если эмитент подключён к сервису [298]. Wear OS Mir Pay не поддерживает; из часов поддержаны Huawei Watch 5 и Watch Ultimate 2 на HarmonyOS 5.0 и новее [298].

Для банка Mir Pay — отдельное направление работ: интеграция с сервисом токенизации НСПК, выпуск и сопровождение токенов, согласование антифрода и подготовка службы поддержки к отклонённым операциям, проблемам при добавлении кошелька, перевыпуску карты, отзыву токена.

16.4 MirAccept: 3DS-аутентификация в системе Мир

MirAccept — сервис аутентификации держателя карты для операций без присутствия карты (CNP), который НСПК эксплуатирует как Directory Server и инфраструктурную часть 3-D Secure для системы «Мир» (см. гл. 11) [299].[1] По архитектуре MirAccept повторяет общую модель EMV 3DS (см. раздел 11.2): Directory Server поддерживает НСПК, Access Control Server (ACS) — эмитент, 3DS Server (компонент, отправляющий запросы аутентификации) — продавец или его PSP (payment service provider — провайдер платёжных услуг).

Чтобы получить корректный 3DS-результат по карте «Мир», продавец и его PSP должны быть зарегистрированы в MirAccept и поддерживать актуальную версию протокола EMV 3DS. Перенос ответственности (*liability shift* — переход финансовой ответственности за спорную CNP-операцию с эквайера на эмитента) при успешной 3DS-аутентификации действует по правилам платёжной системы «Мир». Сценарии *frictionless* (аутентификация без взаимодействия с держателем), *challenge* (с интерактивной проверкой) и *attempts response* (формальный ответ при невозможности полноценной аутентификации) сохраняются; условия их применения и матрицу ответственности фиксирует НСПК. Mir Pay и токенизованные операции через TSP НСПК встраиваются в ту же схему 3DS. При оплате токеном продавец получает результат аутентификации в том же формате, что и для нетокенизированной карты.

В подключении MirAccept повторяются сбои: 3DS-результат «not enrolled» или «unable to verify» там, где ожидался успешный *challenge*; отсутствие переноса ответственности при формально успешной аутентификации; несоответствие версий протокола между 3DS Server продавца и ACS эмитента. Каждый из них требует сверки конфигурации с НСПК; альтернативного маршрута для карт «Мир» нет.

16.5 Interchange и тарифы системы Мир

Тарифную модель платёжной системы «Мир» устанавливает оператор — НСПК, и она зафиксирована в Правилах платёжной системы и публикуемых тарифных планах [75, 300].[2] В отличие от Visa и Mastercard, которые публикуют глобальные таблицы interchange с десятками региональных переменных отдельно от правил сети (у Mastercard — Transaction Processing Rules, TPR) [22, 46], тарифы Мир образуют единую структуру для российского рынка.

Interchange (в Стандарте Системы — *межбанковское вознаграждение*) — плата, которая входит в клиринговую позицию участника по итогам клиринга. Плательщик зависит от типа операции: при оплате товаров и переводе с карты на карту платит эквайер, при выдаче наличных, возврате, запросе баланса и смене ПИН-кода — эмитент (раздел 2.1 Стандарта «Межбанковские вознаграждения») [301]. Ставка зависит от типа карты (Дебетовая, Классическая, Привилегия, Премиальная, Мир Суприм и др.), от MCC ТСП и канала совершения операции. **Плата за операционные, авторизационные, платежные клиринговые и прочие услуги** — собственная плата оператора (раздел 2 Тарифов, Приложение 4 к Правилам), не относится к interchange; участник платит её НСПК как оператору. **Плата за услуги Расчётного центра** — отдельная компонента (раздел 3 тех же Тарифов) [302]. **Торговая уступка**, MSC

[1] Актуальная версия протокола, поддерживаемая MirAccept, относится к семейству EMV 3DS 2.x; матрица переноса ответственности между эмитентом и эквайером фиксируется правилами платёжной системы и сверяется по официальной документации НСПК.

[2] Конкретные ставки interchange и комиссии операционных и клиринговых услуг НСПК изменяются; актуальные значения см. в действующей публичной редакции тарифов.

(merchant service charge), — итоговая комиссия эквайера с продавца; рассчитывается с учётом interchange и плат НСПК, согласуется в договоре эквайринга и в Правилах ПС Мир не регулируется.

Бюджетные карты «Мир» (в Стандарте «Межбанковские вознаграждения», далее — Стандарте МБВ [301], отнесённые к продуктовым категориям *Дебетовая* и *Предоплаченная*) выпускаются массово из-за обязательной эмиссии и получают особый тариф: в отдельных тарифных строках пониженная ставка межбанковского вознаграждения сочетает 0,3–0,4 % от суммы небольших операций и фиксированные 3–4 руб. за операции выше порогового значения. Для социально значимых MCC (ЖКХ, бюджетные платежи, медицина, образование) ставка дополнительно ограничена сверху по остальным продуктам; банк получает заранее ограниченное вознаграждение за операции пенсионеров и получателей социальных выплат [294, 301].

Социально значимые категории и тарифные ограничения

Во время пандемии и в последующие годы в России неоднократно вводились временные и постоянные ограничения на максимальный размер MSC для отдельных категорий ТСП — социально значимых: продукты питания, аптеки, медицинские услуги, услуги ЖКХ, образование, транспорт. Основание для этих ограничений — сочетание решений Банка России, рекомендаций ФАС (Федеральной антимонопольной службы) и параметров государственных программ поддержки малого и среднего бизнеса; пример — программа возмещения комиссии при оплате через СБП (Систему быстрых платежей; см. гл. 19) [303].

Эквайер тарифицирует обычное ТСП по рыночной ставке, ТСП из социально значимой категории — по ограниченной; эмитент получает по таким операциям уменьшенный interchange. В процессинге тариф определяют MCC и дополнительные атрибуты ТСП в реестре эквайера, признак самой карты это ограничение не включает: продуктовая категория карты задаёт лишь базовую тарифную строку. Один и тот же эмитент в течение дня получает по одной и той же бюджетной карте разный interchange — в зависимости от того, в каком ТСП прошла покупка.

Классификация MCC в Мир

Кодификация ТСП в системе «Мир» опирается на тот же международный стандарт ISO 18245 (международный реестр кодов категорий ТСП), что и в Visa, Mastercard, UnionPay [16]. Сами коды MCC — четырёхзначные значения от 0742 до 9950, и они совпадают с кодами международных систем: аптеки — 5912, продукты — 5411, заправки — 5541, авиаперевозки — 4511. Различия задаёт НСПК: она фиксирует, какие MCC относятся к социально значимым категориям для целей тарифных ограничений, какие MCC требуют дополнительной антифрод-проверки (например, азартные игры и обналичивание) и какие учитываются в государственных программах субсидирования комиссий. При подключении ТСП в Мир код MCC напрямую влияет на тариф и на состав обязательных проверок.

16.6 Обязательная эмиссия и эквайринг

161-ФЗ (ст. 30.5) [1] и разъяснения Банка России обязывают банки выпускать карту «Мир» для ряда бюджетных выплат [294], а Закон РФ «О защите прав потребителей» (ст. 16.1) — крупные торгово-сервисные предприятия принимать её [293].

Если банк обслуживает пенсии, социальные выплаты или зарплату работников государственных и муниципальных учреждений, он обязан выпускать и сопровождать карту Мир [294].

Выпуск карты требует полного сопровождения: мобильного банка, колл-центра, разбора спорных операций, карточных лимитов, поддержки Mir Pay, маршрутизации внутрироссийского трафика и управления кобейджем.

Для торгово-сервисных предприятий с годовой выручкой свыше 20 млн рублей приём карт «Мир» обязателен (ст. 16.1 Закона РФ «О защите прав потребителей») [293, 294]. Для крупной торговой сети, общая выручка которой превышает этот порог, обязанность распространяется и на отдельные точки сети с выручкой свыше 5 млн рублей в год; санкция за нарушение — административный штраф по ч. 4 ст. 14.8 КоАП РФ (надзор Роспотребнадзора) [304].

Эквайер и PSP проверяют, что терминальная сеть и интернет-эквайринг не отфильтровывают BIN-диапазоны карт Мир, что в TMS (terminal management system — системе централизованного управления терминальным парком) развёрнуты правильные параметры, что подключение ТСП учитывает обязательный приём, а у службы поддержки в инструкциях разделены отказ продавца «не хотим включать ещё один бренд» и нарушение обязательного правила приёма.

В больших распределённых сетях ТСП требование обязательного приёма должно быть отражено в кассовом ПО, параметрах терминального парка, интернет-эквайринге и процедурах внутреннего контроля инцидентов. Иначе одна и та же компания формально принимает Мир, но не проводит операции на части точек или в части каналов.

16.7 Платёжное приложение Мир, SDK, сертификация

EMV-апплет карты Мир в методологии НСПК называется **MPA (MIR Payment Application)**. Низкоуровневый профиль MPA НСПК раскрывает только в документации для участников.

Мир использует собственную мобильную и терминальную инфраструктуру. НСПК публикует Mir HCE SDK (software development kit — набор средств разработки) для токенизации и платежей по NFC, Mir Kernel SDK для бесконтактного эквайринга на POS-терминалах и MIR CIT Mobile (MIR Certification Integration Terminal — клиентское приложение системы сертификационного интеграционного тестирования) для проверки эквайринговой сети [37].

Криптографические профили MPA, привязка к алгоритмам и сертификационная матрица описаны в закрытой документации НСПК. Нормативную базу задают стандарты ГОСТ 34.10–2018 (электронная подпись), ГОСТ 34.11–2018 (функция хэширования Стрибог), ГОСТ 34.12–2018 (блочные шифры Кузнечик и Магма) и ГОСТ 34.13–2018 (режимы работы блочных шифров) [190, 219—221]; применение блочных шифров для формирования проверочного параметра платёжной карты и проверочного значения PIN задаёт Р 1323565.1.007–2017 (рекомендации по стандартизации) [305].

Участие банка или процессинга в Мир начинается с допуска по Правилам ПС Мир. НСПК публикует сами Правила, форму заявления на присоединение и методику расчёта гарантийного обеспечения [75].

Далее банк или процессинг настраивает маршрутизацию, обмен ключами, тестовые среды и обработку сообщений по правилам НСПК. Подключение к ОПКЦ, график обмена и обработка инцидентов требуют отдельного плана работ.

Доработки в маршрутизации, терминальном стеке или мобильном сценарии проверяются в тестовой среде НСПК: тестовые BIN, тестовые ключи, тестовые ТСП и сценарии *stand-in* — собственные.

Эти работы распределены между командами и выполняются с разной скоростью. За правила и договоры отвечают продуктовые подразделения и служба комплаенса, за хостовую сертификацию — процессинг, за терминальные и карточные профили — эмиссия, поставщики карт и эквайринговая сеть. Если их не свести в один план, участие оказывается формально оформленным и технически неполным: хостовый канал подключён, а терминалы или персонализация чипа всё ещё не готовы к промышленной эксплуатации —недооценка любого направления приводит к задержкам из-за ключей, тестовых сертификатов, терминальных ядер, параметров TMS или расписания обязательного внедрения.

17 UnionPay

В международном приёме UnionPay объединяет инфраструктуру UnionPay International (UPI, не путать с индийской Unified Payments Interface) [306], правила конкретной юрисдикции [307] и маршруты кобейджа, где путь операции выбирается по правилам соответствующей платёжной системы.

17.1 Процессинговая архитектура UnionPay

Внутренняя расчётная и процессинговая инфраструктура China UnionPay (CUP) обрабатывает авторизацию, клиринг и расчёт карточных транзакций внутри Китая и выполняет в UnionPay роль, сопоставимую с VisaNet у Visa. UPI не публикует подробного открытого описания этой инфраструктуры; в отраслевых материалах используется обобщённая аббревиатура CUP, иногда с уточнением назначения подсистем: процессинг, клиринг, расчёт [307].

Авторизация и клиринг разнесены во времени и по требованиям к задержкам так же, как у Visa и Mastercard (см. гл. 5); внутренняя инфраструктура UnionPay маршрутизирует авторизационные запросы к эмитенту, а клиринговая обработка собирает исходящие реестры за период, рассчитывает нетто-позиции и передаёт их в расчётный центр [307].

Опубликованные правила UnionPay в России задают регламент обработки: авторизации работают круглосуточно; исходящие реестры и отчётность поступают до 09:00 МСК дня T; реестр нетто-позиций направляется в расчётный центр до 12:00 МСК дня T+1; расчёты между участниками завершаются до 13:00 МСК дня T+1 [307].[2]

Правила UnionPay в России называют и исполнителей: операционным и платёжным клиринговым центром служит НСПК (ОПКЦ, см. раздел 16.2), как того требует ч. 4 ст. 30.6 161-ФЗ [1], расчётным центром — Банк России [307]. UPI остаётся правообладателем товарного знака и получает нетто-позиции по трансграничной части через свой расчётный центр, а внутренний клиринг между российскими участниками проходит через ОПКЦ. Регламент 09:00/12:00/13:00 МСК из правил UnionPay действует с поправкой: в части функций ОПКЦ приоритет у правил НСПК [307], и участник сверяет оба документа одновременно. При расхождении между расчётным днём UPI и операционным днём НСПК для российских участников действует календарь НСПК, для внешнего участника — календарь UPI.

ВАЖНО

За пределами материкового Китая операции проходят через инфраструктуру UnionPay International — связующее звено между участником в стране приёма и внутренней инфраструктурой UnionPay в Китае. Каждая юрисдикция применяет собственную редакцию правил и регламента; сроки обработки и форматы файлов проверяются отдельно по каждой стране.

[2] Внутрироссийские операции по картам международных платёжных систем по ч. 4 ст. 30.6 161-ФЗ обрабатываются через операционный и платёжный клиринговый центр НСПК [1]; значения сверяются по актуальной редакции правил.

17.2 Операционный цикл и расчётный регламент

Открытые правила UnionPay в России описывают двухэтапную карточную схему. Эквайер направляет эмитенту авторизационный запрос через операционный центр; после одобрения эквайер отправляет исходящий клиринговый файл; платёжный клиринговый центр рассчитывает нетто-позиции; расчётный центр исполняет их по счетам участников [307]. В этих правилах базовая схема обрабатывает транзакцию двумя сообщениями (*dual-message*), а не одним (*single-message*).

В отличие от Visa BASE II и Mastercard GCMS, расчётный цикл UnionPay изначально строился под внутрикитайский рынок, а зарубежный приём обслуживается через UnionPay International. Внутри Китая инфраструктура UnionPay обрабатывает транзакции с расчётами T+1 по умолчанию; для международных операций схема зависит от соглашения между эквайером и эмитентом через UPI. Сроки расчёта по одной и той же карте UnionPay в разных юрисдикциях сверяются по актуальной редакции правил соответствующей расчётной системы [307].

Операции *single-message* занимают в UnionPay более важное место, чем в Visa или Mastercard. UnionPay вырос из дебетового и банкоматного рынка Китая 2002–2010 годов, где транзакция сводилась к снятию наличных в банкомате и покупке с моментальным списанием. Для дебетовой карты, где нет кредитного лимита и нет промежутка между авторизацией и расчётом, *single-message* естественнее: одно сообщение содержит и авторизацию, и финансовый факт. Visa и Mastercard, напротив, развивались из кредитной модели, где холд, подтверждение и расчёт разнесены во времени (раздел 5.4). Схема *dual-message* появилась у UnionPay позже — по мере роста кредитной эмиссии, международного расширения и сценариев с отложенным подтверждением (гостиницы, аренда) [307].

UnionPay поддерживает обе схемы. В сценарии *offline-single-message* карта одобряет транзакцию офлайн и накапливает записи для последующей передачи [86]; такой сценарий применяется для небольших сумм и ряда автоматических POS-терминалов. В схеме *single-message* второго клирингового файла нет, поэтому коннектор эквайера обрабатывает транзакцию иначе, чем в *dual-message*.

Сценарии с отложенным подтверждением продавец сверяет по продукту и рынку отдельно. *Pre-auth* (предварительное резервирование суммы на карте без её немедленного списания; финальное предъявление выполняет отдельная операция *completion*) в гостиничном канале работает как партнёрская функция. IHG (InterContinental Hotels Group, международная гостиничная группа) описывает запуск приёма бронирований UnionPay с *pre-auth* без предъявления карты для своих прямых каналов в Большом Китае [308]; параметры *pre-auth*, *completion* и последующих изменений суммы у каждого партнёра свои.

17.3 QuickPass: ядро и протокольный стек

Официальные материалы UPI определяют QuickPass как сервис на базе NFC (near-field communication — бесконтактная связь малой дальности на 13,56 МГц) и токенизации, который поддерживает бесконтактную офлайн-оплату, оплату по QR и платежи внутри приложения, включая мобильные телефоны, HCE (host card emulation — программная эмуляция карты в ОС телефона) и носимые устройства, если они соответствуют спецификациям EMVCo (отраслевой консорциум — владелец спецификаций EMV: контактный/бесконтактный чип, токенизация, 3-D Secure [86]) [309].

Физический уровень здесь тот же, что у Visa payWave и Mastercard PayPass[1]: ISO/IEC 14443 (стандарт *proximity*-карт и физический уровень NFC на 13,56 МГц) [124]. Один считыватель на аппаратном уровне обслуживает несколько бесконтактных сетей, если в нём установлены соответствующие ядра приложений (*kernels* — программные компоненты терминала, реализующие правила EMV-обработки бесконтактной транзакции для каждой платёжной сети).

У каждой платёжной сети собственное ядро бесконтактной обработки. У Visa это VCPS (Visa Contactless Payment Specification), у Mastercard — PayPass/M/Chip Contactless, у UnionPay — отдельное QuickPass-ядро. Каждое ядро реализует правила своей сети для выбора приложения (AID, application identifier — идентификатор EMV-приложения на карте; см. гл. 7), набор команд APDU (application protocol data unit — формат команд и ответов между терминалом и чипом по ISO/IEC 7816-4 [102]), криптографические параметры и поведение терминала при различных условиях транзакции. Терминал с одним только ядром VCPS обнаружит карту UnionPay на физическом уровне, но не проведёт транзакцию: логики обмена с этим приложением у него нет.

Выбор приложения EMV через список AID на карте и в терминале (механика и определение AID — раздел 7.3) открывает транзакцию. Карта UnionPay содержит собственный AID из диапазона, зарегистрированного за China UnionPay. Терминал без этого AID с привязанным QuickPass-ядром приложение не выберет, и транзакция не начнётся.

UPI публикует отдельные списки рекомендованных точек приёма QuickPass и указывает, что фактический приём отличается от списков и сверяется по знаку QuickPass в точке оплаты [310]. Эквайер и интегратор проверяют поддержку бесконтактного интерфейса и наличие QuickPass-ядра в терминальной конфигурации.

Сценарий QR в QuickPass устроен иначе, чем NFC: обе схемы — MPM (merchant-presented mode — QR показывает продавец, сканирует покупатель) и CPM (consumer-presented mode — QR показывает покупатель, сканирует продавец) — работают на прикладном уровне, не через EMV APDU (таксономия QR и различия между MPM и CPM — раздел 22.2). Подключение QuickPass QR — отдельная интеграция через API, не связанная с настройкой ядра NFC на терминале.

17.4 Карточные продукты и interchange

В отличие от Visa и Mastercard, UnionPay не публикует единой мировой таблицы interchange. Для части рынков UPI публикует таблицы в открытом доступе на странице Interchange Rate Fees: на момент сверки в апреле 2026 года это EEA (European Economic Area — Европейская экономическая зона), Великобритания, Швейцария, Япония, Канада, Малайзия, Казахстан и ряд других юрисдикций; актуальный перечень рынков сверяется по странице IRF [311]. Для остальных юрисдикций, в том числе для самого Китая, условия определяются договорами с участниками и зависят от типа продукта, географии и роли участника в расчётной системе.

Продуктовая линейка UnionPay делится на уровни: UnionPay Standard, UnionPay Gold, UnionPay Platinum, UnionPay Diamond и несколько специализированных продуктов (UnionPay Business Card, UnionPay Prepaid). Как у Visa и Mastercard, тип

[1] Visa payWave и Mastercard PayPass — исторические маркетинговые бренды; с 2016 года Mastercard перевела продукт на бренд «Mastercard Contactless» (ядро M/Chip Contactless), а Visa к концу 2010-х в маркетинге перешла на термин «Visa Contactless». В технической документации и сертификационных материалах исторические названия продолжают использоваться.

продукта влияет на маршрутизацию, на правила управления рисками и (там, где условия определены) на стоимость обработки.

UnionPay появился как сеть с тесной связью между эмитентом, процессингом и расчётом. Внутри Китая большинство транзакций проходит через внутреннюю инфраструктуру UnionPay напрямую, без промежуточных звеньев. За пределами Китая операции проходят через инфраструктуру UPI, и до подключения команда определяет, кто именно участник и какая редакция правил действует в конкретной юрисдикции.

ТСП, принимающее карты UnionPay через интернет, аутентифицирует транзакции без физического присутствия карты (*card-not-present*, CNP) механизмом UPI: UnionPay 3DS, сертифицированный по спецификации EMVCo 3DS [312], или UPI SecurePlus — протокол поверх API с SMS-аутентификацией и токенизацией, доступный за пределами материкового Китая [313].[1] Если эмитент поддерживает один из протоколов, ответственность в случае спора переносится (логика та же, что в разделе 11.6); оба протокола относятся к UnionPay и требуют отдельной интеграции.

17.5 UnionPay International и правила участия

За пределами материкового Китая карту обслуживает UnionPay International. В собственном профиле компания называет себя дочерней структурой China UnionPay, отвечающей за международный бизнес; участие оформляется через партнёрские организации [306].

Местные правила UnionPay построены на актуальной редакции UnionPay International Operating Regulations с учётом местного законодательства [307]. Те же правила задают критерии участия для прямых и косвенных участников, обязанности эквайера и эмитента, требования к управлению рисками и информационному обмену [307].

Подключение к UnionPay начинается с описания модели участия: через какого участника принимаются операции, какие договоры и лицензии оформляют участие, кто отвечает за досье на ТСП и управление рисками, как оформлены расчёты [307].

Открытые правила описывают расчётный механизм: нетто-клиринг, передачу реестра нетто-позиций в расчётный центр, дебетование и кредитование счетов участников, а также конкретные сроки обработки по дням T и T+1 [307].

17.6 Расчётная валюта и конвертация

Внутри Китая расчёты между участниками внутренней инфраструктуры UnionPay проводятся в юанях (CNY — буквенный код китайского юаня по ISO 4217 [84]). За пределами Китая UPI рассчитывает участников в CNY или в согласованной валюте расчётной системы; выбор валюты зависит от двусторонних договорённостей с UPI и региональной редакции правил участия [307].

Карточная транзакция включает несколько конвертаций валюты на разных этапах. Покупатель платит в местной валюте (в рублях или тайских батах), эквайер выставляет транзакцию в валюте транзакции, а расчёт между участниками выполняется в расчётной валюте системы с конвертацией по курсу момента клиринга,

[1] SecurePlus пришёл на смену более раннему UPI SecurePay с HPP (*hosted payment page*) и редиректом покупателя на страницу UnionPay; SecurePlus встроен в *checkout* эквайера и не требует редиректа [313].

а не момента авторизации. Курс зачисления продавцу отличается от курса на терминале. Правила UnionPay в России привязывают конвертацию к курсу Банка России: п. 6.2.3 — на момент совершения операции, п. 6.9.4 — при расчёте рублёвой клиринговой позиции на дату расчёта [307].

Общий механизм DCC (dynamic currency conversion — конвертация на терминале по предложенному эквайером или его DCC-провайдером курсу с раскрытием суммы покупателю) разобран в разделе 36.3 [314]. У UnionPay механика та же, но китайский держатель карты ожидает сумму в CNY, и эквайер показывает её через стороннего провайдера DCC в обход официального канала UPI; курс DCC по картам UnionPay менее выгоден, чем сетевой. Для продавца, работающего с китайскими туристами, это типичный источник жалоб и спорных операций.

Отдельный случай — межвалютные расчёты по двусторонним соглашениям UPI с центральными банками. В ряде юрисдикций UPI согласовал расчёты в валюте страны без промежуточной конвертации через CNY. Условия сверяются по актуальной редакции правил участия [307].

17.7 Кобейдж Мир/UnionPay: маршрутизация и выбор банка

UPI и НСПК в официальных материалах совместно продвигают выпуск дебетовых карт Мир–UnionPay банками-участниками НСПК [315]; такая карта обрабатывается через сеть Мир в России и через сеть UnionPay за её пределами [315]. Действующие правила UnionPay в России дополнительно уточняют: для эмиссии совместной карты эмитент должен участвовать в обеих платёжных системах, а операции, маршрутизируемые через платёжную систему UnionPay, регулируются её правилами [307].

Карта Мир–UnionPay содержит приложение Мир с AID национального диапазона и приложение UnionPay с AID китайского диапазона. Терминал при выборе приложения получает оба AID и применяет приоритет из конфигурации. В России терминальная конфигурация отдаёт приоритет Мир; за рубежом доступно только приложение UnionPay либо оба, в зависимости от настроек эквайера и конфигурации терминала.

Маршрут карты Мир–UnionPay выбирается не один раз при выпуске, а при каждой транзакции. Сначала терминал формирует список взаимно поддерживаемых AID (пересечение списка карты и списка терминала). Затем эквайер или хост переопределяет приоритет через параметры TMS (terminal management system — система централизованного управления парком терминалов: их конфигурацией, ключами и прошивками), например выставляет приоритет UnionPay выше Мир на международных терминалах. Если эмитент настроил маршрутизацию по типу операции или по сумме, разные транзакции одной и той же карты маршрутизируются в разные сети.

Кобейдж тестируют по полной комбинации «карта × терминал × страна × канал». Авторизацию за рубежом выполняет банк-эмитент через инфраструктуру UnionPay (минуя НСПК); решение о риске и логику отказа формируют правила UnionPay.

Если эквайер или ТСП рассчитывает на карту «Мир–UnionPay» как на универсальный международный способ оплаты, доступность маршрута проверяется по странам, банкам и точкам приёма [315].

17.8 Сценарии отказа по кобейджу

Кобейдж добавляет к стандартным причинам отказа отдельный класс: отказ по маршрутизации, помимо отказа по состоянию счёта держателя карты. Для команды поддержки и аналитики жалоба «карта не прошла за рубежом» разбирается по сценариям.

Первый сценарий: **AID не найден**. Терминал не содержит QuickPass-ядра или AID UnionPay не входит в конфигурацию, и приложение не выбрано. Держатель карты видит отказ ещё до авторизационного запроса и воспринимает его как «карта не работает»; хост такой транзакции не видит. Диагноз: проблема на терминальной стороне эквайера, не на стороне эмитента.

Второй сценарий: **авторизационный отказ по коду**. Запрос поступил эмитенту через сеть UnionPay, но эмитент вернул отказ. Используются те же коды ISO 8583 (стандарт формата сообщений карточных авторизаций; см. [74]), что и в других сетях: 05 (Do not honor), 57 (Transaction not permitted to cardholder), 62 (Restricted card). Типичная причина кода 62 у карт UnionPay — эмитент не включил этот диапазон BIN (bank identification number — первые цифры PAN, идентифицирующие эмитента и продуктовый диапазон) или тип операции в разрешённый международный маршрут. Карта физически выпущена, но не настроена на работу через UPI.

Третий сценарий: **недоступность маршрута**. Сеть UnionPay между эквайером и эмитентом недоступна: нет договора между эквайером и UPI, нет корреспондентских связей, или канал временно недоступен. Терминал получает таймаут или технический отказ (96, 91). Если терминал поддерживает *fallback* (резервный сценарий обработки — переключение на альтернативное приложение, сеть или способ ввода, когда основной путь недоступен) на альтернативную сеть и на карте есть другое приложение, например национальная сеть страны эквайера, *fallback* возможен. Для Мир/UnionPay за рубежом *fallback* на Мир возможен только там, где эквайер принимает Мир, а таких стран немного и в большинстве из них приём ограничен (раздел 18.7).

Четвёртый сценарий: **интернет-платёж (транзакция CNP)**. Терминала и выбора AID здесь нет; процессинг решает, по какому маршруту направить транзакцию, опираясь на BIN и договорную конфигурацию. Если маршрут UnionPay не настроен для этого BIN, транзакция либо отклоняется с кодом «неверный маршрут», либо не создаётся: шлюз отбрасывает карту на этапе валидации формы ввода.

ПРАКТИКА

При диагностике отказов по кобейджу проверяют по порядку: был ли авторизационный запрос (или отказ на стороне терминала), какой код ответа вернул эмитент, направлена ли транзакция через UnionPay или через Мир, и соответствует ли конфигурация BIN на стороне эквайера ожидаемому маршруту.

17.9 Санкции и операционные риски

Санкционные ограничения определяют, в каких юрисдикциях и при каких условиях карта UnionPay фактически работает, независимо от того, есть ли технический маршрут.

Позиция UnionPay. После февраля 2022 года UnionPay International приостановил переговоры о новых продуктах с российскими банками, а ряду банков отказано

в подключении к сети UPI[1]. Отраслевые источники называли причиной риск вторичных санкций США и Евросоюза. UPI — китайская компания: напрямую она не подпадает под санкции OFAC (Office of Foreign Assets Control — управление Министерства финансов США, администрирующее санкционные программы) и не включена в список SDN (Specially Designated Nationals and Blocked Persons List — санкционный список заблокированных лиц и организаций), но вторичные санкции создают риск для любой компании, проводящей транзакции с лицами или организациями из списка SDN [316].

Вторичные санкции как механизм. Вторичные санкции США по Executive Order 14024 в редакции Executive Order 14114 [317] грозят блокирующими санкциями или ограничением корреспондентских счетов в США иностранным финансовым организациям, проводящим значительные операции с военно-промышленной базой России; с 12.06.2024 OFAC относит к ней всех лиц, заблокированных по Executive Order 14024 и включённых в список SDN [318]. Даже технически возможная транзакция через инфраструктуру UPI создаёт для UnionPay риск вторичных санкций, включая отключение от долларовых корреспондентских счетов и американских рынков капитала. Прямого запрета нет [319]; риск создаёт вторичный механизм.

Наблюдаемая картина. Часть российских банков сохранила выпуск и обслуживание карт UnionPay; это банки, не попавшие под SDN и не входящие в секторальные санкционные категории. По сообщениям деловых СМИ карты работают в странах, не присоединившихся к западным санкционным пакетам (Китай, ОАЭ, Турция, страны АСЕАН, часть африканских рынков); UPI не публиковала официальный перечень поддерживаемых стран. В государствах, применяющих санкции ЕС и США, эквайер либо блокирует диапазоны BIN российских карт на входе, либо получает отказ от банков-корреспондентов при попытке рассчитать операцию.

Операционный риск для эмитента. Для российского банка, выпускающего карты UnionPay, основной риск договорной: UPI может в одностороннем порядке приостановить или прекратить участие банка в сети, если санкционный периметр вокруг банка изменится. Обещание клиенту «карта работает за рубежом» создаёт операционный риск, который остаётся при любых технических мерах; снижают его мониторинг санкционного статуса и прямое предупреждение держателя карты об ограничениях.

Операционный риск для ТСП и эквайера. ТСП или PSP (payment service provider — провайдер платёжных услуг, агрегирующий приём для ТСП на стороне эквайера), подключающий UnionPay, проводит скрининг транзакций по санкционным спискам OFAC: для лиц под юрисдикцией США это прямая обязанность [320], для остальных — требование договоров с эквайером и банками-корреспондентами и защита от риска вторичных санкций. Поскольку значительная доля держателей карт — граждане КНР, политическое напряжение между США и Китаем остаётся долгосрочным фактором риска.

Проверка по первоисточнику Санкционный периметр вокруг UnionPay меняется быстрее, чем печатная книга успевает его фиксировать. Актуальный список SDN и SSI поддерживается OFAC [316]; позиция конкретного банка проверяется по текущей редакции санкционных листов; состояние на дату публикации этой книги ориентиром не служит.

[1] Официальных пресс-релизов UPI по этому вопросу в открытом доступе опубликовано не было; описание поведения системы основано на отраслевых сообщениях 2022 года и на наблюдаемом поведении сети.

17.10 Отличия от Visa и Mastercard

При общей карточной модели UnionPay расходится с Visa и Mastercard по процессинговой инфраструктуре, формату клиринга, бесконтактному ядру, токенизации, интернет-аутентификации, выплатам, обновлению реквизитов и публикации interchange. Таблица 29 сопоставляет все три сети; пару Mastercard и Visa разбирает раздел 15.8, который опирается на эту же таблицу.

Таблица 29 — Архитектурные отличия UnionPay, Visa и Mastercard.

Компонент	UnionPay	Visa	Mastercard
Процессинговая инфр.	внутренняя инфраструктура UnionPay (Китай), UPI (международно)	VisaNet (BASE I + BASE II)	Единый периметр (Authorization Platform + GCMS)
Клиринговый формат	Реестры через инфраструктуру UnionPay/UPI	TC33 через BASE II	IPM через GCMS
Бесконтактное ядро	QuickPass-ядро (отдельное для UnionPay)	VCPS	PayPass/M/Chip Contactless
Токенизация	UPI Token Service	VTS + Token Assurance Level	MDES + DSRP
Интернет-аутентификация	UnionPay 3DS (EMVCo) + SecurePlus (SMS/токен)	Visa Secure (3DS)	Mastercard Identity Check (3DS)
Выплаты	UnionPay MoneyExpress [321]	Visa Direct	Mastercard Send
Обновление реквизитов	Нет публичного аналога VAU/ABU	Visa Account Updater (VAU)	Automatic Billing Updater (ABU)
Таблицы interchange	Публикуются для части рынков (EEA, UK, JP, CA и др. — двухбуквенные коды стран по ISO 3166-1 [322]); для остальных договорные	Публикуются по регионам	Публикуются по регионам

Бесконтактное ядро: терминал с VCPS или PayPass требует отдельного QuickPass-ядра для приёма карт UnionPay, даже если физический уровень NFC одинаковый.

Закрытые условия interchange: команда, которая строила ценообразование по публичным таблицам Visa и Mastercard, не сможет применить ту же методику к UnionPay — условия она получает по договору с участником [307].

ПРАКТИКА

При добавлении UnionPay в таблицу маршрутизации заранее разделите вопросы: редакция правил и участник/расчётная система в вашей юрисдикции; поддерживаемый продукт и маршрут кобейджа (QuickPass, QR, Мир–UnionPay); отдельно — интернет-аутентификация через UPI SecurePlus.

18 Национальные карточные сети СНГ

Банку или поставщику платёжных услуг (*payment service provider*, PSP) при выходе в соседнюю страну недостаточно терминала с EMV, хоста с ISO 8583 и знакомого логотипа на карте. Логотип не показывает, кто управляет внутренним трафиком, где завершается расчёт, обязателен ли внутренний приём и как кобейдж (выпуск карты с двумя платёжными приложениями двух разных сетей; разбор см. в разделе 17.7) открывает внешний путь карты за пределами страны.

18.1 Мотивация национальных сетей

Суверенный контроль над правилами сети и непрерывностью операций требует маршрутизации внутреннего трафика силами собственного оператора. Маршрутизация через внешнюю сеть ставит весь внутренний оборот в зависимость от остановки, санкционного давления или единоличного решения её владельца. Регулятору нужна инфраструктура, которая работает независимо от решений внешних участников.

Национальная сеть и процессинг убирают зависимость от чужой валютной и расчётной инфраструктуры. Расчёты в национальной валюте между участниками не требуют прохождения через корреспондентскую сеть (систему счетов, которые банки держат друг у друга для исполнения межбанковских переводов) или зарубежный клиринг. Порог входа ниже, чем у глобальной сети. Прямое членство (статус участника сети, который даёт прямое подключение к сети и обязанности по правилам, в отличие от косвенного участия через спонсора) в глобальной сети требует капитала, технической сертификации и инфраструктуры сопровождения, которой у небольшого регионального банка может не быть.

Мир создавался под санкционным давлением. После того как Visa и Mastercard в 2014 году приостановили обслуживание ряда российских банков, основана Национальная система платёжных карт (НСПК; см. гл. 16) [17] и в 2015 году запущена карта Мир. В марте 2022 года Visa и Mastercard полностью прекратили операции в России, и Мир остался основной внутренней карточной сетью. Иранская сеть Shetab появилась раньше, в 2002 году, как проект унификации фрагментированной карточной инфраструктуры страны. Санкции отрезали Иран от международных сетей позднее, превратив Shetab в единственную доступную внутреннюю инфраструктуру. UnionPay в Китае выросла из задачи обслуживать национальный розничный рынок — задолго до того, как международные карты заняли там значимую долю.

Транзакции через собственную сеть приносят interchange и процессинговые комиссии, которые остаются в национальной экономике, а не перечисляются иностранному оператору. Тарифы и правила операций устанавливает оператор расчётной системы внутри страны.

С 2024 года к этому добавился санкционный механизм: включение оператора чужой сети в список SDN переносит риск на эмитентов в стране-партнёре. Банк, выпустивший карту сети X, после санкций против X выбирает между нарушением правил сети и риском для корреспондентских отношений в валютах третьих стран; разбор см. в разделе 18.7. Собственная сеть устраняет этот риск по построению: суверен сам определяет применение санкций внутри страны и не подчинён внешним спискам SDN.

У Белкарт, HUMO и ЭЛКАРТ собственный стандарт карточного приложения, собственные данные авторизационного сообщения и собственные правила отклонения. Сам факт карточной эмиссии совместимости со стеком EMV не гарантирует, поэтому точкой отсчёта перед интеграцией служит документация национальной сети.

18.2 Критерии сравнения

Инженерное сравнение национальных сетей ведётся по параметрам: оператор и физическое размещение процессинга; обязательность внутреннего приёма (*domestic acceptance*); устройство расчётной системы и условия участия; необходимость кобейджа для внешнего использования; степень совпадения с привычным стеком EMV/ISO 8583 из гл. 7 и 5.

Формат сообщения и чип не определяют ни географию приёма, ни обязательность эквайринга, ни распределение рисков работы сети. Различия проявляются в операторской модели — кто владеет сетью и выпускает правила; в размещении процессинга и расчёта — внутренняя обработка идёт через собственный узел, и тот же оператор завершает урегулирование; в модели приёма — обязательная внутри страны или добровольная; во внешнем пути карты — самостоятельном или открываемом через кобейдж.

Пока неизвестно, где находится расчётная система, как оформляется участие и обязателен ли внутренний приём, решение о поддержке сети преждевременно: главные ограничения коренятся в организационной модели, а транспортный формат сообщения вторичен.

18.3 Белкарт и ArCa

Белкарт — национальная сеть с собственной внутренней инфраструктурой, оформленной как бренд и набор правил для участников. Оператор системы — ОАО «Банковский процессинговый центр»; правила системы охватывают эмиссию, эквайринг, процессинг и расчёты по операциям с карточками Белкарт [323].

Среди продуктов Белкарт есть кобейдж Белкарт–Maestro (Maestro — дебетовый бренд Mastercard, выпуск которого сворачивается поэтапно по регионам: в Европе с 1 июля 2023 года [324]) для операций в Беларуси и за рубежом [325]; кобейдж Белкарт–Мир выпускается с января 2020 года, а после того как в марте 2022 года белорусские карты Visa и Mastercard перестали работать в России, стал для держателей способом платить в России [326].

ArCa с самого начала работает на инфраструктуре процессора, который обслуживает и международные сети. Armenian Card описывает себя как оператора и процессинговый центр национальной платёжной системы ArCa: её инфраструктура обрабатывает транзакции и проводит клиринг, а банки-участники, помимо Mastercard, Visa, American Express, DCI (Diners Club International), Мир и JCB (*Japan Credit Bureau* — японская международная карточная сеть), выпускают и обслуживают карты ArCa [327].

Процессинг разделяет логотип на карте и инфраструктуру расчёта. Даже компактные сети вроде Белкарт и ArCa требуют отдельного проекта, если банк встраивает их в процессинг с поддержкой нескольких сетей: операторская модель и обязательный внутренний приём задают требования, специфичные для конкретной страны, а группа, работающая сразу в нескольких юрисдикциях региона, ведёт отдельный набор правил подключения и сопровождения по каждой сети.

18.4 HUMO, UzCard и ЭЛКАРТ

Официальный FAQ называет HUMO национальной платёжной картой и связывает появление системы с президентским указом о создании National Interbank Processing Centre (NIPC, Узбекистан — отдельная организация, не путать с одноимённым по смыслу IPC в Кыргызстане, см. ниже). Международные карты внутри Узбекистана могут обрабатываться через HUMO в роли второго процессора, а за рубежом принимаются в сети той системы, с которой карта была выпущена [328].

UzCard на своём официальном сайте называет себя ведущим национальным платёжным оператором Республики Узбекистан. В сообщении 2025 года UzCard и UnionPay объявили о планах расширять выпуск кобейдж-карт и обеспечивать совместимость QR-кодов между сетями [329]. Интеграция банкоматных сетей HUMO и UzCard прошла летом 2023 года: после постановления Президента от 9 марта 2023 года [330] к концу июля сети объединили [331]. В ноябрьском сообщении HUMO сказано, что число банкоматов, доступных населению, выросло вдвое [332]. Пара HUMO и UzCard задаёт интегратору отдельную задачу интероперабельности: поддержать обе карты и отделить участки, где инфраструктура уже объединена, от участков, где правила операторов различаются.

Официальный сайт ЭЛКАРТ выделяет среди базовых продуктов «Социальные выплаты» и «Пенсионную карту»; описание пенсионной карты прямо связывает её с получением пенсий, пособий и компенсаций [333]. Там же сказано, что ЭЛКАРТ — национальная платёжная карточная система под управлением Interbank Processing Center (IPC — оператор национальной платёжной системы Кыргызстана «ЭЛКАРТ»; не путать с узбекским NIPC выше), а в роли эмитента участвует и Центральное казначейство Министерства финансов Кыргызстана [333]. Страница IPC подтверждает, что компания — оператор национальной платёжной системы «ЭЛКАРТ» и одновременно оказывает услуги по обработке платежей и проведению расчётов в международных платёжных системах, действующих на рынке страны [334]. Помимо кобейджа с UnionPay у ЭЛКАРТ существовал и кобейдж с Мир — продукт «ELCARD MIR NFC», выпускавшийся, в частности, Кыргызско-Швейцарским банком. С 5 апреля 2024 года оператор ЭЛКАРТ из-за риска вторичных санкций прекратил обслуживание карт Мир в своей сети, а карты ЭЛКАРТ перестали обслуживаться в сети Мир [335].

HUMO использует собственные правила эмиссии и расчёта; UzCard делит национальный рынок с HUMO и подключается к ней в части банкоматной сети; ЭЛКАРТ опирается на государственные и социальные сценарии. Выбор локальной сети задаёт интегратору параметризацию терминала, маршрутизацию на стороне хоста, подключение ТСП, собственный список проверок релиза и отдельную поддержку операций.

18.5 Азербайджан: AzeriCard и MilliKart

В Азербайджане локальная инфраструктура сосредоточена в процессинговых центрах без собственного карточного бренда. Таких центров два, AzeriCard и MilliKart, и они не зависят друг от друга.

AzeriCard работает с 1997 года при International Bank of Azerbaijan, обрабатывает операции двух десятков банков в Азербайджане и за рубежом и сертифицирован Visa, Mastercard, American Express, Diners Club, UnionPay и JCB [336]. MilliKart основан Центральным банком Азербайджана в 2006 году, с октября того же года работает

как ООО с 17 банками-участниками и ЕБРР в капитале и имеет лицензии полного членства (*full membership*) Mastercard, Visa и UnionPay [337].

Клиент держит карту с международным логотипом; внутренняя транзакция проходит через азербайджанский процессинговый центр и не передаётся зарубежному сервису; внешний путь карты работает по правилам Visa, Mastercard или UnionPay без отдельного кобейджа. Для интегратора это снижает требования к хосту — сертификация ISO 8583-сообщения у процессора уже покрывает международные сети — и одновременно повышает зависимость от их правил: своей карточной сети, к которой можно было бы переключиться при санкционном давлении, у такой модели нет.

В 2024 году AzeriCard подключил приём Apple Pay и Google Pay через шлюз Akurateco: шлюз проверяет и расшифровывает платёжные токены кошельков и передаёт данные существующему процессинговому вендору AzeriCard [338]. Это эквайринговая сторона интеграции: процессор не эмитирует карты, и токенизация карт банков-участников в Visa Token Service и Mastercard Digital Enablement Service в этом проекте не описана.

18.6 Казахстан без национальной карточной сети

В Казахстане место национальной сети заняла частная платёжная экосистема Kaspi.kz. По данным Нацбанка РК, в январе–мае 2026 года на Kaspi пришлось 83 % безналичных операций в стране по количеству и около 75 % по объёму [339]; платёжной платформой Kaspi во втором квартале 2026 года пользовались 14,8 млн активных клиентов [340]. На 1 августа 2026 года в Казахстане в обращении 84,0 млн платёжных карт; 81,6 % дебетовые, 15,5 % кредитные, 2,8 % дебетовые с кредитным лимитом и предоплаченные (*prepaid*) [341]. Банки выпускают карты международных систем и локальной системы Kaspi.kz [341]; государственного карточного бренда страна не создала.

Нацбанк РК в 2024 году объявил о запуске универсальной межбанковской QR-инфраструктуры с приёмом в любом банке страны; срок интеграции банков — 19 июля 2026 года [339]. Опережая её запуск, Kaspi в сентябре 2024 года открыл собственную платёжную сеть для клиентов Home Credit Bank и Altyn Bank, до этого работавших только с картами своих эмитентов [342]. Аргументация повторяет логику национальной сети: контроль над внутренней маршрутизацией, независимость от международных операторов, собственные правила приёма. Отличается субъект: задачу решает частная компания вместо государственного оператора расчётной системы.

Для интегратора, выходящего в Казахстан, выбор идёт между Kaspi через её API и банками через QR-сервис Нацбанка. При такой доле Kaspi подключают обязательно; универсальный QR-сервис Нацбанка связывает QR-приём всех банков, включая терминалы Kaspi, и обеспечивает регуляторное равенство участников. Место национальной сети в платёжном суверенитете здесь занимает монополия местной частной экосистемы, согласовавшей с регулятором правила доступа третьих сторон.

Когда доля одного провайдера превышает половину розничных платежей, регулятор сталкивается с теми же задачами, что и центральный банк страны без собственной сети: контроль непрерывности операций, санкционная политика, тарификация. Разница в субъекте отчётности: в национальной сети оператор подотчётен регулятору, в частной экосистеме — акционерам и биржевому рынку. Регуляторный ответ Нацбанка РК (универсальная QR-инфраструктура, межбанковский доступ)

повторяет шаги, которые десятилетие назад привели к созданию НСПК и Белкарта; стимулом здесь стал частный провайдер, а не санкционное давление.

18.7 Кобейдж после внесения НСПК в список SDN

23 февраля 2024 года Минфин США внёс АО НСПК в список SDN [252]. Для национальных сетей кобейдж с Мир из канала внешнего использования превратился в источник санкционного риска. Армянская ArCa свернула продукт ArCa–Мир к 30 марта 2024 года (см. таблицу 30); зарубежные эмитенты, у которых кобейдж с Мир оставался активным, пересматривали набор карточных продуктов из-за риска вторичных санкций для своих банков-корреспондентов.

К 2025 году Мир принимается, по открытым заявлениям ЦБ РФ, в 13 странах; в девяти — с ограничениями (Армения, Венесуэла, Вьетнам, Казахстан, Лаос, Молдова, Мьянма, Таджикистан, Никарагуа) [343]. В мае 2025 года ЦБ Ирана объявил о запуске второго этапа интеграции с Мир: иранские продавцы принимают карты Мир через Android-приложение MirPay [344]. Список стран и условия приёма пересматриваются чаще, чем выходит печатное издание; интегратор сверяется с актуальными ограничениями национального оператора-партнёра, а не с общим списком стран.

После февраля 2024 года решение по кобейджу начинается с санкционной оценки; продуктовая экономика идёт следом. Для зарубежного эмитента, выпустившего карту X–Мир, судьбу продукта определяют оценка риска по OFAC и требования банков-корреспондентов. Для эмитента в стране, где обязательный приём собственной национальной сети требует кобейджа для внешнего пути, остаётся разрабатывать альтернативный маршрут через UnionPay либо JCB или отказываться от внешнего использования вовсе. Активный кобейдж с Мир после февраля 2024 года теряет смысл для банков, сохраняющих корреспондентские отношения в долларах и евро.

Кобейдж с UnionPay сохраняет внешнее использование в Китае, странах ASEAN, на Ближнем Востоке и в ряде европейских юрисдикций, но требует сертификации по правилам UnionPay International и подключения к CIPS (*Cross-Border Interbank Payment System*) для межбанковского клиринга в юанях. Кобейдж с JCB даёт приём в Японии и Юго-Восточной Азии, но эквайринговая сеть там заметно уже, чем у UnionPay. Национальная сеть, обязательная к приёму внутри страны, продолжает работать независимо от внешнего кобейджа: санкционный риск кобейджа внутренний поток к оператору сети не затрагивает.

Параллельная инфраструктура — СПФС Банка России для межбанковских сообщений в рублях и национальных валютах стран-партнёров — к 2025 году расширилась до зарубежных участников из стран СНГ, Ирана и ряда юрисдикций Ближнего Востока и Юго-Восточной Азии [12]. СПФС работает на межбанковском уровне и карточную маршрутизацию с розничным приёмом Visa или Mastercard не заменяет: она даёт корреспондентский канал для межбанковского клиринга, независимый от SWIFT и доступный участникам в условиях санкционных ограничений. Поэтому после свёртывания кобейджа с Мир расчётные связи операторов национальных сетей СНГ с российскими банками сохраняются: рублёвый и национальный поток идёт через СПФС, минуя карточную инфраструктуру.

Таблица 30 — Параметры национальных карточных сетей СНГ.

Сеть	Диапазон BIN	Внутренний interchange	Обязательный приём	Внешний путь
Мир	2200–2204	По таблицам НСПК	Да (ТСП свыше 20 млн руб./год)	Кобейдж с UnionPay
Белкарт	требует сверки	По правилам оператора	Да (по ряду категорий ТСП)	Кобейдж с Мир и Maestro
HUMO	требует сверки	По правилам NIPC	Да (внутри Узбекистана)	Кобейдж с UnionPay
UzCard	требует сверки	По правилам UzCard	Да (внутри Узбекистана)	Кобейдж с UnionPay [329]
ArCa	требует сверки	По правилам ЦБ Армении	Да (внутри Армении)	Кобейдж с UnionPay и Mastercard анонсирован [345]; ArCa–Мир — до 30 марта 2024
ЭЛКАРТ	требует сверки	По правилам оператора	Да (внутри Кыргызстана)	Кобейдж с UnionPay; с Мир — до 5 апреля 2024

18.8 Последствия для интегратора

Техническая совместимость с EMV из гл. 7 и знакомый карточный жизненный цикл из гл. 5 оставляют банку, процессингу и шлюзу открытыми вопросы: кто задаёт правила сети, где обязателен приём, как устроен кобейдж и насколько широк охват внешнего использования.

Продавец сталкивается с той же асимметрией: в одной стране национальная сеть обязательна для приёма, в другой это дополнительный внутренний канал, важный для отдельных категорий клиентов или выплат. От этого зависят витрина оплаты, приоритет брендов в интерфейсе, формулировки приёма в договоре и запасные сценарии службы поддержки.

В сводной таблице 30 BIN-диапазоны (*bank identification number*; в ISO/IEC 7812 — стандарте нумерации идентификаторов эмитентов — обозначается как *issuer identification number*, IIN) для всех сетей, кроме Мир, требуют сверки по реестру IIN ISO/IEC 7812 [54] и публичной документации операторов: в открытых источниках встречаются устаревшие значения локального внутреннего распределения, не зарегистрированные в ISO.

Поддержка национальной карты — это согласие на её внутреннюю платёжную систему целиком: операторскую модель, требования сертификации, обязательность приёма и санкционный риск кобейджа.

ПРАКТИКА

Минимальный список проверок для интегратора по национальной сети: где находится оператор и расчётная система, обязателен ли приём внутри страны, нужен ли отдельный путь через кобейдж для внешнего использования, какие сертификации терминала и хоста требуются и кто отвечает за международный приём. Если хотя бы один пункт остаётся неясным, интеграция не завершена, даже если лабораторный платёж по карте уже проходит.

Банковская группа с дочерними банками в нескольких странах СНГ ведёт пять или шесть параллельных интеграций с национальными сетями. У Белкарт, HUMO,

UzCard, ArCa и ЭЛКАРТ собственное EMV-приложение (AID) и собственное терминальное ядро: параметры терминала, профиль EMV-приложения, структура авторизационного сообщения и правила отклонения у каждой сети свои. Расчётный день и формат сводных файлов клиринга тоже различаются; единого расчётного календаря у группы не будет. Унификация достигается собственной шиной процессинга: один формат входящего сообщения и маршрутизация по диапазону BIN на подключение нужного оператора. То же распределение действует для производства и персонализации карт (раздел 7.11): профиль приложения готовится отдельно под каждую сеть, а скрипты подготовки данных и договор с производителем карточных заготовок остаются общими. Экономика такой группы строится на отделении общей инфраструктуры процессинга от локальной специфики каждой сети; расчёт на унификацию стандартов в этой группе не работает.

19 СБП

Система быстрых платежей (СБП) — сервис Банка России и НСПК для онлайн-переводов и платежей между счетами в банках-участниках. За кнопкой «карта» стоит сеть с авторизацией, клирингом и отдельным расчётом; за кнопкой «СБП» — перевод со счёта на счёт, окончательный почти сразу.

19.1 Архитектура системы

СБП собрана из звеньев, и карточных ролей в ней нет: ни эмитента с кредитным лимитом, ни эквайера с карточным риском продавца, ни двухтактной логики авторизации и клиринга.

Первое звено — Банк России: через его платёжную систему (ПС БР) проходит окончательный расчёт между банками-участниками [5]. Второе — Национальная система платёжных карт (НСПК; см. гл. 16), она ведёт операционную инфраструктуру СБП, на её основе работают клиентские сервисы системы и действуют правила Операционного и платёжного клирингового центра СБП (ОПКЦ СБП) [346, 347]. Третье звено — банки-участники, через которые клиент отправляет и получает перевод.

Далее в главе используются типовые направления денежных потоков: C2C между физическими лицами, C2B от покупателя продавцу, B2C от бизнеса физическому лицу, B2B между юридическими лицами, Me2Me между своими счетами одного клиента в разных банках.

У типичного C2B-платежа последовательность шагов отличается от карточной. Продавец создаёт платёжную сессию (объект на стороне продавца или банка, связывающий заказ, попытку оплаты и итоговый статус) и показывает динамический QR-код (*Quick Response*; см. гл. 22), кнопку или ссылку. Покупатель переходит в банковское приложение или SBPay и подтверждает списание с выбранного счёта. Банк плательщика передаёт операцию в операционную инфраструктуру СБП, перевод проходит расчётную систему Банка России, банк получателя зачисляет деньги, а продавец получает итоговый статус операции [5, 347—349].

В карточной сети между одобрением и деньгами проходит отдельная стадия клиринга. В СБП этот промежуток короче, но экранное подтверждение не заменяет исполненный перевод. До зачисления денег и финального статуса заказ остаётся в ожидании оплаты.

C2B-перевод может завершиться отказом в банке плательщика, ОПКЦ СБП или банке получателя. Банк плательщика отказывает на этапе подтверждения при нехватке средств, срабатывании антифрода, приостановке по Федеральному закону от 24.07.2023 № 369-ФЗ «О защите клиентов от переводов без согласия» [350], а также при срабатывании ограничений по суммам и лимитам. ОПКЦ СБП возвращает таймаут или ошибку маршрутизации, когда банк получателя недоступен или когда QR-код либо платёжная ссылка недействительны: нарушена структура, не пройдены проверки, одноразовую ссылку уже оплатили. Продавца в C2B адресуют зашитые в QR реквизиты и его идентификатор в СБП, а не привязка счёта к номеру телефона — это механика C2C и возвратов. Банк получателя отказывает в зачислении при закрытом счёте, блокировке по 115-ФЗ [351] или внутренних ограничениях получателя. В любом из этих случаев операция получает финальный статус отказа, и средства не списываются: расчёт между корреспондентскими счетами в Банке России идёт

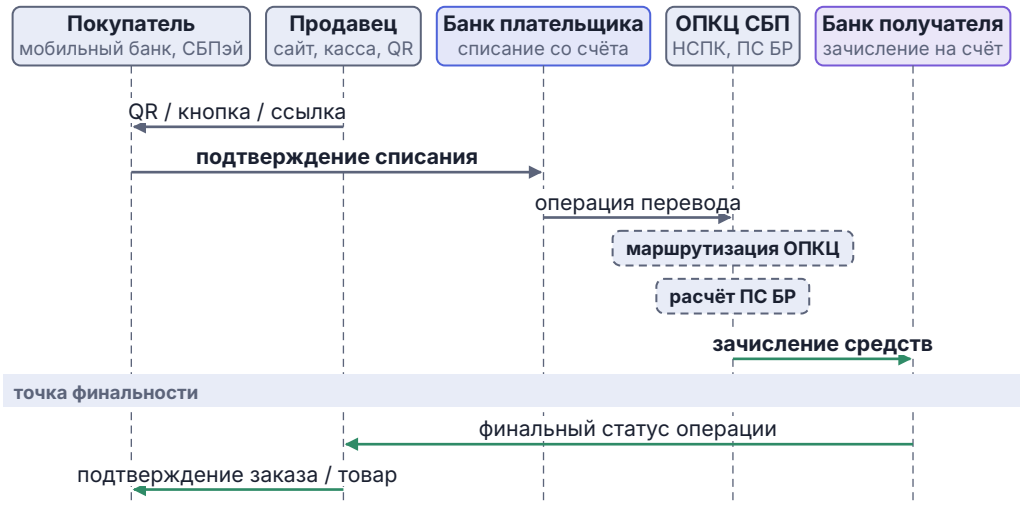


Рис. 46 — C2B-платёж по СБП: от QR до зачисления.

только после готовности банка получателя, поэтому отказ означает несостоявшийся перевод, а не списание с последующим возвратом. Возврат — отдельная операция, и она возможна лишь по уже исполненному переводу [347, 348].

Карточная система работает по схеме «сначала авторизация, потом клиринг»; в СБП центральное событие — подтверждение исполнения самого перевода. Доменной модели нужен другой набор состояний: инициация, ожидание результата, исполнение, отказ и отдельная операция возврата.

При оплате картой продавец получает обещание эмитента, окончательный расчёт приходит позже. При оплате через СБП источник истины о платеже смещается от авторизационного ответа к факту межбанковского зачисления.

Если пользовательский интерфейс обновляется быстрее учётной системы и заказ помечен как оплаченный раньше, чем перевод подтверждён, сверка фиксирует расхождение.

19.2 Сценарии платежей

Сценарии СБП различаются тем, кто инициирует перевод, какие данные требуются при инициации и где будет проходить сверка. Способ инициации — номер телефона, QR-код, ссылка или корпоративные реквизиты — для архитектора вторичен [346].

Протокол C2C в СБП охватывает перевод другому человеку и переводы самому себе между банками. В него входят сценарии: C2C Push (другому человеку, по инициативе отправителя), Me2Me Push и Me2Me Pull (себе, по инициативе отправителя и получателя соответственно). C2C Push требует номера телефона, суммы и выбора банка получателя. Один номер бывает привязан к счетам в нескольких банках: если получатель назначил банк по умолчанию, ОПКЦ СБП возвращает его как предпочтительный; если нет, банк отправителя просит клиента выбрать банк. Банк отправителя передаёт в ОПКЦ выбор клиента; список банков получателя ему не раскрывается. После выбора банк отправителя через ОПКЦ СБП запрашивает у банка получателя

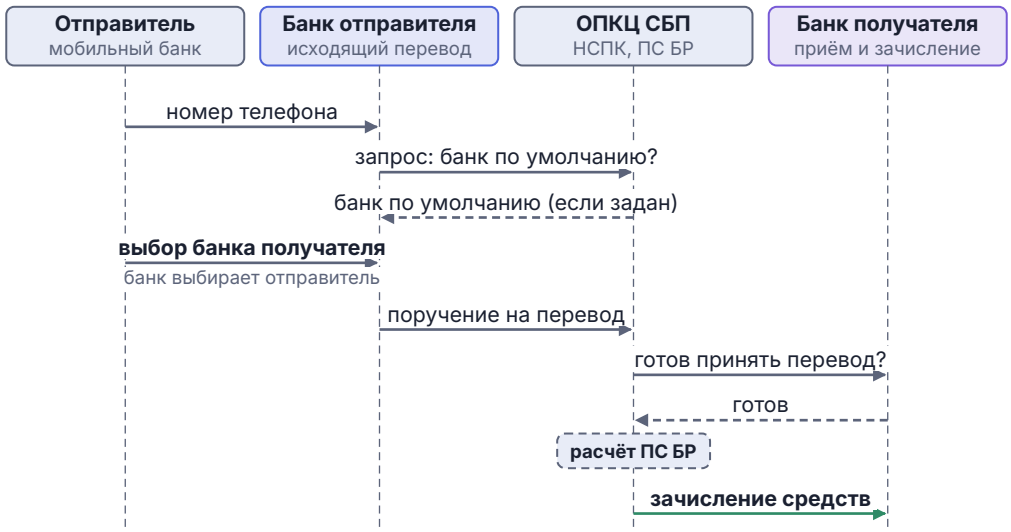


Рис. 47 — Сценарий C2C Push: выбор банка получателя и подтверждение готовности через ОПКЦ СБП.

готовность принять перевод на эту сумму и только затем инициирует расчёт. Ключевое условие адресации: получатель заранее подключил приём переводов по СБП в своём банке [352].

Два других сценария протокола C2C — переводы самому себе на счёт в другом банке. **Me2Me Push** инициирует отправитель: из приложения банка-отправителя он отправляет средства на свой счёт в банке-получателе — так пополняют вклад, брокерский счёт, гасят кредит. **Me2Me Pull** инициирует получатель, но согласие на списание клиент даёт в банке-отправителе: именно он распоряжается исходящим переводом. По первому запросу банк-отправитель присылает уведомление со ссылкой, клиент выбирает счёт списания и подтверждает операцию; согласие бывает разовым или постоянным — на последующие переводы без подтверждения [353]. В международной карточной практике перевод себе реализуют связкой AFT+OCT (*Account Funding Transaction* — списание с карты-источника, *Original Credit Transaction* — зачисление на карту-получателя) через Visa Direct или Mastercard Send (см. разделы 14.6, 15.5); после марта 2022 года эти продукты недоступны российским участникам.

Платёж от клиента к бизнесу (C2B) принимается по QR-коду или платёжной ссылке. Динамический (кассовый) QR-код — сценарий `C2BQRD` — создают на конкретную покупку: сумма в нём обязательна, код одноразовый. Статический QR-код (наклейка, `C2BQRS`) печатают один раз и используют для множества переводов; он бывает с суммой или без, и при пустой сумме покупатель указывает её по договорённости с продавцом. Кассовая ссылка СБП — подтип статического QR: сама ссылка многоразовая, но сумму и прочие реквизиты каждого платежа задаёт получатель из кассового ПО. Отдельные сценарии — оплата по ссылке на устройство плательщика (`C2BMcom`) и возврат (`C2BRfnd`) [348, 354].

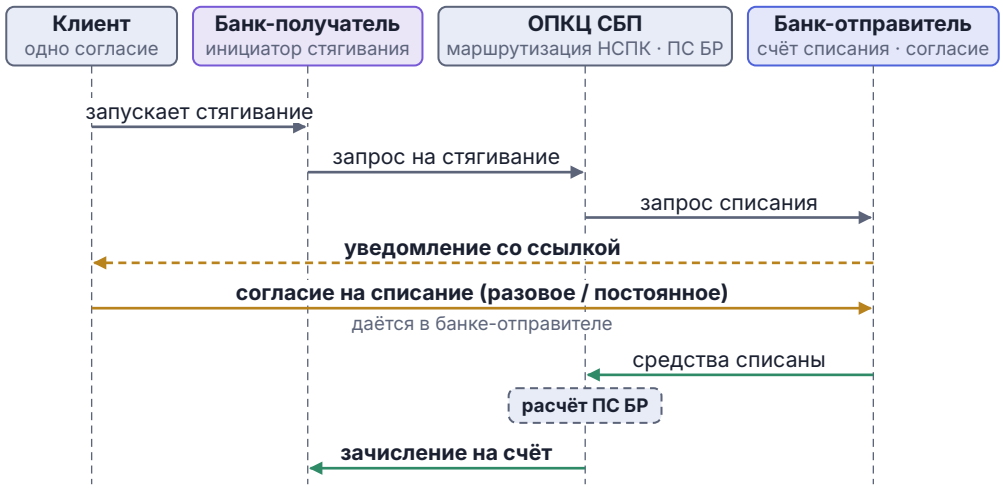


Рис. 48 — Me2Me Pull: согласие на списание — в банке-отправителе.

Главное различие для продавца — способ сверки. Статический QR требует сопоставлять поступивший перевод с заказом по сумме, времени, кассе или дополнительному идентификатору уже после факта оплаты. В интернет-магазине и кассовом ПО динамический QR создаётся под конкретную покупку и связывает заказ и перевод [348].

У маркетплейса один и тот же C2B-платёж по СБП обслуживает две модели исполнения заказа. В FBO (*Fulfillment by Operator*) товар хранится на складе площадки, и она сама готовит заказ к доставке. В FBS (*Fulfillment by Seller*) товар хранится у продавца, он сам собирает заказ и передаёт маркетплейсу для доставки [355, 356]. Для платёжной системы FBO и FBS не отличаются: перевод остаётся C2B-платежом с мгновенным зачислением и отдельной операцией возврата [348]. Для продуктовой логики различие сохраняется: разные жизненные циклы заказа порождают разные правила сверки одной и той же оплаты.

СБП подходит и для выплат от бизнеса физическому лицу (B2C, протокол `B2COther`): возвраты, кешбэк, вознаграждения, выплаты подрядчикам [354]. В III квартале 2025 года в СБП было совершено 63 млн переводов юридических лиц гражданам на сумму 531 млрд рублей [357].

Массовые B2C-выплаты требуют загрузки реестра, отдельного статуса по каждой строке, повторной отправки ошибочных записей и контроля идемпотентности (свойства, при котором повторная отправка операции с тем же идентификатором не приводит к повторному эффекту). Единица управления здесь — реестр выплат целиком.

B2B-сценарий работает в корпоративной среде и требует формальных реквизитов, назначения платежа и интеграции с учётной системой. Банк России отдельно публикует тарифы для переводов юридических лиц и индивидуальных предпринимателей (ИП) в пользу юридических лиц и ИП, а НСПК описывает B2B-платежи как круглосуточные онлайн-расчёты с мгновенным зачислением средств получателю [5, 358].

Таблица 31 — Сценарии СБП и их параметры сверки.

Сценарий	Что нужно на старте	Что подтверждает успех	Что нужно сверять
C2C	Номер телефона, сумма и выбранный банк получателя (или его банк по умолчанию)	Исполненный перевод на счёт получателя	Выбранный банк и подключённый получателем приём по СБП
Me2Me Pull	Согласие на списание в банке-отправителе (разовое или постоянное)	Исполненный перевод на свой счёт в банке-получателе	Действительность согласия и доступность счёта-источника
Me2Me Push	Перевод себе на счёт в другом банке из приложения банка-отправителя (на уровне СБП — операция C2C Push)	Исполненный перевод на свой счёт в банке-получателе	Принадлежность обоих счетов одному клиенту
C2B	QR-код, кнопка, ссылка или привязанный счёт	Исполненный перевод в пользу продавца	Связку платёжной сессии и заказа, а также возврат как отдельную операцию
B2C	Реестр получателей и суммы выплат	Реестр исполненных выплат по каждой строке	Идемпотентность, частичные ошибки и повторную отправку
B2B	Корпоративные реквизиты и назначение платежа	Исполненный перевод и зачисление получателю	Связку с договором, счётом и бухгалтерской системой

19.3 SBPay: мобильный сценарий оплаты

SBPay (СБПэй) — отдельное мобильное приложение для оплаты через СБП с привязанного банковского счёта [349].

Пользователь скачивает приложение, выбирает свой банк и привязывает счёт через приложение банка или, если банк это поддерживает, вручную вводя номер телефона и номер счёта [349]. После этого через SBPay можно оплачивать покупки по QR-коду, табличке NFC (*Near Field Communication* — ближнепольная радиосвязь), кнопке на сайте или платёжной ссылке.

Банк нужен только для привязки счёта и части проверок, а само приложение работает параллельно банковскому. В мобильной интеграции заранее выбирают сценарий: кнопку СБП в банковском приложении, отдельное приложение SBPay или оба сразу.

В сценарии с кнопкой, ссылкой или NFC пользователь переходит во внешнее приложение, а затем возвращается к продавцу или дожидается фонового обновления статуса. Такой переход не должен закрывать платёжную сессию: продавец сохраняет её открытой, повторно запрашивает итог операции и не помечает заказ оплаченным по факту перехода в SBPay или в банковское приложение [349, 359].

ПРАКТИКА

Для электронной коммерции базовый набор — динамический QR, кнопка СБП и платёжная ссылка: они работают внутри сайта или приложения продавца. SBPay нужен, если отдельный мобильный платёжный интерфейс поверх СБП важнее встроенного сценария.

19.4 Привязка счёта и повторные покупки

Публично описанный сценарий повторной оплаты в СБП основан на привязке счёта. Пользователь один раз выбирает опцию «Привязать счёт СБП», переходит в приложение банка и связывает счёт с продавцом. После этого можно платить с привязанного счёта без повторного ввода реквизитов [359].

Первая онлайн-покупка одновременно оплачивает заказ и устанавливает привязку между продавцом и счётом клиента. Следующая покупка начинается с выбора оплаты по СБП на сайте или в мобильном приложении продавца [359].

В продукте привязка счёта должна быть самостоятельным объектом согласия между продавцом и счётом клиента, отделённым от первой успешной покупки. У такой привязки собственный жизненный цикл: запрошена, подтверждена, отозвана, повторная оплата инициирована. Оплата не должна неявно следовать из самой привязки. Иначе первая же отвязка счёта или отклонение повторной операции приведут к смешению состояния согласия и денежного события.

Внешне это напоминает *card-on-file* (сценарий повторных оплат с заранее сохранёнными карточными реквизитами), но техническая основа иная. Продавец не работает с PAN (*Primary Account Number*, номер карты), карточным токеном и сроком действия карты; в публично описанной модели СБП он использует ранее привязанный счёт, а новую оплату подтверждает пользователь. Карточные термины MIT (*Merchant-Initiated Transaction*, операция, инициированная мерчантом) и CIT (*Customer-Initiated Transaction*, операция, инициированная клиентом) плохо переносятся в СБП: здесь важнее различать момент привязки счёта, момент оплаты и обработку результата.

Публичные материалы СБП подтверждают саму схему привязки и оплату с уже привязанного счёта, но не раскрывают весь протокол обмена между продавцом, банком и НСПК [359]. Для проектирования достаточно моделировать привязку и повторную оплату как два события, каждое со своим подтверждением.

Модель СБП ближе к открытому банкингу (*open banking* — когда сторонние сервисы по согласию клиента инициируют переводы напрямую с банковского счёта клиента) и к переводам со счёта на счёт (*account-to-account*, A2A), чем к картам. Ключевой объект в обеих моделях — право инициировать перевод со счёта клиента без карточного реквизита.

19.5 Универсальный QR

Универсальный QR — инициатива НСПК, объединяющая в одном QR-коде сразу несколько способов оплаты (по СБП, банковским сервисом мгновенной оплаты конкретного банка, цифровым рублём) [360]. Для покупателя он выглядит как обычный QR-код: после сканирования банковское приложение предлагает доступные способы оплаты, а пользователь выбирает удобный. По 248-ФЗ с 1 сентября 2026 года все банки обязаны поддерживать универсальный QR; через него же проходит оплата цифровым рублём (см. раздел 24.2), а НСПК предоставляет банкам сам код бесплатно [361, 362].

Для продавца Универсальный QR упрощает приём оплат: вместо нескольких кодов и кнопок на кассе достаточно одного. Для сверки это вносит неопределённость: способ оплаты конкретной покупки продавец узнаёт только после неё. Учётная система получает итоговый идентификатор способа оплаты в уведомлении после оплаты и сверяет движение денег с поправкой на источник перевода.

19.6 Подписочные платежи СБП

Помимо привязки счёта, НСПК выделяет отдельный сервис «Подписка СБП». Однократно полученное согласие клиента позволяет продавцу инициировать последующие списания в пределах согласованных параметров (сумма, периодичность, срок действия согласия), без участия пользователя в каждой повторной операции [363]. Для пользователя сервис похож на *card-on-file* в подписочном бизнесе; у продавца вместо токена карты хранится идентификатор согласия СБП с привязанным счётом клиента.

Для подписочного продукта эта схема явнее разделяет согласие и первую оплату, чем обычная привязка счёта. У согласия собственный жизненный цикл (выдано, активно, отозвано, истекло); объект «связь со счётом» задан явно и прослеживается по состоянию согласия.

19.7 Протокол ОПКЦ СБП и OpenAPI

Взаимодействие банка-участника и продавца с СБП проходит через OpenAPI (публичный REST-интерфейс, описанный в формате OpenAPI Specification) ОПКЦ СБП на стороне НСПК [364].[1] Ключевые свойства протокола: асинхронный обмен сообщениями (создание платёжной сессии и получение итогового статуса разделены во времени), обязательная идемпотентность операций по идентификатору запроса, формализованный набор статусов операции (`NTST` — не начата, `RCVD` — в обработке, `ACWP` — исполнена, `RJCT` — отклонена) и явные поля для связки покупки и перевода [364].

В C2B-сессии сверка опирается на идентификаторы ОПКЦ: `qrcId` как идентификатор QR-кода или платёжной ссылки, `trxId` как идентификатор конкретной операции СБП, отдельный идентификатор запроса на возврат (`opkcRefundRequestId`). Возврат привязывается именно к `trxId` исходного платежа, а не к идентификатору заказа продавца: один заказ может породить несколько попыток оплаты, и для корректного частичного или полного возврата нужно знать, какой именно перевод возвращается. Идентификатор кассы и идентификатор заказа продавца передаются как пользовательские поля и не заменяют идентификаторы ОПКЦ при сверке.

Интеграция различается для банка-участника и продавца. Банк-участник подключается к ОПКЦ СБП напрямую: набор операций задают Правила ОПКЦ СБП и операционные бюллетени НСПК, единые для всех участников, а доработки сверяют с документами на портале поддержки НСПК [347, 365]. Продавец или агент ТСП интегрируется через банк: ему доступна та часть операций, которую открыл банк-партнёр, поэтому сначала изучают её, затем по документации НСПК разбирают семантику статусов и правила идемпотентности и только после этого проектируют учётные сценарии в продукте.

[1] Полная техническая спецификация ОПКЦ СБП доступна банкам-участникам и агентам ТСП (юридическим лицам, действующим от имени торгово-сервисного предприятия в части приёма платежей по СБП) через портал `support.nspk.ru` после подключения; публично доступны правила ИТ-взаимодействия агента ТСП, банка и НСПК по QR-кодам СБП, версия 4.0 от 12.09.2024.

19.8 Финальность, возвраты и антифрод

После исполнения перевод по СБП финален: ни банк-отправитель, ни НСПК не могут отменить его в одностороннем порядке. Банковский интерфейс лишь показывает уже наступивший расчётный результат [1]. Если отправитель ошибся в сумме или номере телефона, вернуть деньги он сможет с согласия получателя и его банка [352]. В C2B-сценарии возврат идёт как новая операция: продавец инициирует полный или частичный возврат через свой банк, и деньги поступают покупателю моментально [348]. Встроенного карточного chargeback в СБП нет; устройство споров и отличия от карточного цикла подробно разобраны в разделе 32.8.

Учётной системе нужна более строгая машина состояний: платёжная попытка переходит в подтверждение исполнения, оттуда — в состояние «оплачено»; возврат — отдельная операция со своими статусами. Одного двоичного признака «оплачено/возвращено» недостаточно.

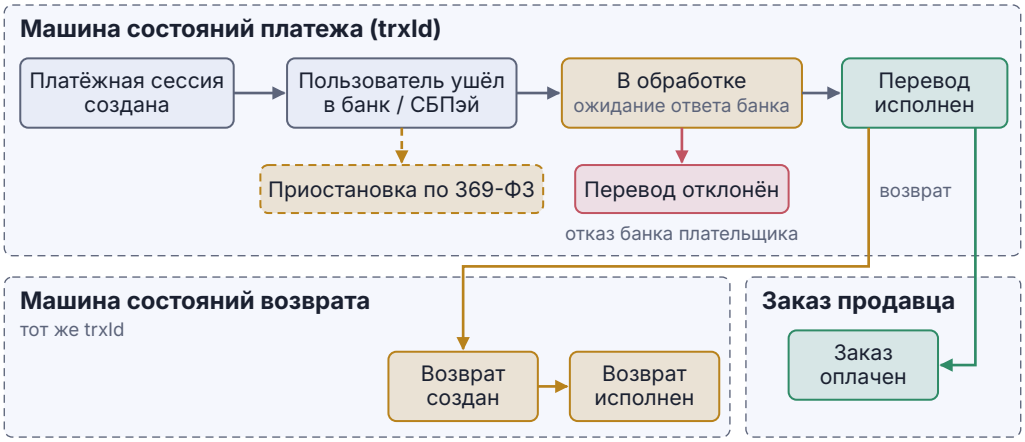


Рис. 49 — Состояния платежа и возврата в СБП.

Антифрод в СБП должен сработать до подтверждения плательщиком: после исполнения перевод финален. По разъяснению Банка России, при наличии сведений о получателе в базе данных о переводах без добровольного согласия клиента банк обязан на два дня приостановить перевод или отказать в повторной операции, в том числе по СБП. Если по истечении этой двухдневной паузы клиент не отказался от перевода или повторил его на те же реквизиты и сумму, банк обязан его исполнить; при соблюдении этой процедуры он не возвращает деньги за перевод на счёт злоумышленника [350, 366].

19.9 Отличия от карточных сетей

Карта даёт продавцу обещание эмитента и отложенный расчёт; СБП — исполненный перевод со счёта на счёт. Инженерные различия двух систем сведены в таблице 32.

Продавцу, у которого большинство чеков укладывается в лимит одного перевода, СБП даёт клиенту более простой сценарий оплаты и меньшую нагрузку на внутреннюю сверку [352, 367]. Платой за эту простоту становится иная архитектура

Таблица 32 — Инженерные различия СБП и карт.

Параметр	Карты	СБП
Реквизит на старте	PAN (номер карты), карта или сетевой токен	Номер телефона, QR-код, ссылка, кнопка или привязанный счёт
Источник истины о платеже	Авторизационный ответ, затем клиринг и расчёт	Исполненный перевод и подтверждение результата
Финальность денег	После отдельного расчёта	Почти сразу после исполнения перевода
Возврат и спор	Возврат, chargeback, сетевые процедуры	Возврат как новая операция, встроенного chargeback нет
Резервирование средств	Возможны холд (резервирование суммы на счёте плательщика до завершения клиринга) и предавторизация	Естественного аналога карточному холду нет
Повторные покупки	*stored credential* (сохранённые карточные реквизиты) и правила MIT/CIT	Привязанный счёт и отдельное подтверждение результата
География	Международная	Внутрироссийская
Предельная сумма	Зависит от карты, банка и сценария	Меньше 1 млн рублей за перевод или платёж
Комиссия для бизнеса	Определяется договором эквайринга	Не более 0,2 %, 0,4 % или 0,7 %

возвратов и собственный процесс разрешения конфликтов вместо карточных сетевых процедур.

Карту имеет смысл применять там, где деньги сначала резервируются, а уже потом переводятся: гостиница, прокат автомобиля, депозит, предавторизация на АЗС. СБП выигрывает там, где деньги должны быстро оказаться у получателя, а заказ закрывается после подтверждённого перевода.

19.10 Тарифы, лимиты и подключение банков

Тарифы СБП ниже карточных и заранее известны. Для переводов между разными банками комиссия для физического лица отсутствует до 100 тыс. рублей в месяц, для переводов между своими счетами (Me2Me) лимит — 30 млн рублей в месяц [352]. Сумма одного перевода или платежа в СБП должна быть меньше 1 млн рублей, банк вправе устанавливать и более низкие внутренние лимиты [352].

Эти лимиты относятся к переводам между счетами. Оплата по QR-коду или по кнопке СБП не расходует лимит на бесплатные переводы: в FAQ системы оплата и переводы описаны как разные операции [352]. Для продуктовой команды слово «лимит» здесь объединяет разные ограничения: системный потолок на одну операцию, тарифное правило для переводов и внутренние ограничения самого банка по риску и пользовательскому сценарию.

Для приёма платежей бизнеса от физических лиц (C2B) ставка зависит от категории операции: ЖКХ — 0,2 % и не более 10 руб. за операцию; прочие социально значимые категории — 0,4 %; остальные операции — 0,7 % при потолке 1 500 руб. [367]. Ставки и состав социально значимых категорий C2B-операций устанавливает и пересматривает Совет директоров Банка России отдельными решениями; Положение 876-П задаёт устройство самой платёжной системы [7, 368].

Покупатель оплачивает заказ на 3 000 руб. в интернет-магазине электроники. При оплате по СБП (несоциально значимая категория) комиссия для бизнеса — не более 0,7 %: $3\,000 \times 0{,}007 = 21$ руб. При оплате картой через эквайринг типичная ставка для интернет-торговли — 1,5–2,5 %. При ставке 2,0 % это $3\,000 \times 0{,}02 = 60$ руб. Разница 39 руб. с одной транзакции; при 50 000 операций в месяц переход на СБП экономит 1,95 млн руб. в месяц или 23,4 млн руб. в год [367]. Для социально значимых категорий (аптеки, продукты) потолок 0,4 % снижает комиссию до 12 руб., увеличивая экономию на транзакцию до 48 руб.

Число банков-участников СБП публикуется на сайте системы: по данным FAQ, в СБП участвуют 220 банков [346]. Для банка-участника подключение к СБП формализовано: дополнительное соглашение к договору корреспондентского счёта, присоединение к правилам ОПКЦ СБП и тестовые испытания в инфраструктуре НСПК [347]. Для бизнеса подключение проще: достаточно обратиться в банк-участник, поддерживающий оплату по QR-коду, и заключить договор на приём платежей через СБП; отдельных соглашений с НСПК и Банком России бизнес не подписывает [348].

Интегратор выбирает между готовым сценарием и собственной координацией. Готовый сценарий от банка или провайдера уже включает QR-код, кнопку, ссылку или оплату с привязанного счёта. При собственной координации интегратор создаёт динамический QR, связывает заказ с платёжной сессией, принимает обратное уведомление, проверяет поступление и отдельно запускает возврат, если он нужен. Готовый сценарий быстрее подключить; собственная координация даёт больше контроля над учётной логикой и сверкой.

19.11 Цифровой рубль и СБП: разделение функций

Цифровой рубль похож на СБП по интерфейсу: QR-код, банковское приложение, почти мгновенный результат. По устройству это другая часть денежной системы. СБП переводит безналичные деньги между счетами в коммерческих банках; цифровой рубль — отдельная форма денег, учитываемая на платформе Банка России (см. раздел 24.1). При оплате через СБП продавец ждёт перевод между банковскими счетами, при оплате цифровым рублём — движение внутри платформы Банка России. Одинаковый QR на экране не делает операции одинаковыми для реестра обязательств, сверки и правового анализа [369].

Роль Банка России в двух системах разная. В СБП он — оператор системы: устанавливает правила и проводит расчёт, операционную инфраструктуру ведёт НСПК (см. раздел 19.1), но деньги остаются обязательствами коммерческих банков. В цифровом рубле он — эмитент денежной формы и оператор реестра кошельков: обязательство принадлежит Банку России непосредственно, банки лишь обслуживают клиентский интерфейс. Параллель «обе системы — от Банка России» верна для управления инфраструктурой, но неверна для обязательства: в СБП движутся обязательства банков, в цифровом рубле — обязательство Банка России.

20 Мгновенные платежи в мире: Pix, UPI, FedNow, SEPA Instant

СБП из предыдущей главы — одна из национальных систем мгновенных безотзывных переводов между банковскими счетами 24/7/365. Такие же системы работают в Бразилии (Pix), Индии (UPI), США (FedNow) и еврозоне (SEPA Instant Credit Transfer). Для держателя они похожи, но различаются тем, кто оператор расчёта; задаёт ли сама схема способ инициации платежа и формат QR; какое место у небанковских участников; есть ли в схеме встроенный антифрод. Эти различия сохраняются в банковской обработке: сверка, разбор диспутов и хранение доказательств у каждой системы свои.

20.1 Pix (Бразилия)

Pix — платёжная схема, оператором которой является центральный банк Бразилии (Banco Central do Brasil, BCB). Pix запущен 16 ноября 2020 года; участие обязательно для всех финансовых институтов, у которых более 500 тыс. активных счетов клиентов [370, 371].

Расчёт проходит через выделенную RTGS-инфраструктуру под управлением BCB — систему мгновенных платежей SPI (Sistema de Pagamentos Instantâneos). При RTGS (real-time gross settlement, валовой расчёт в реальном времени) каждый перевод исполняется индивидуально и окончательно, без сведения в нетто-позицию и без расчётных окон, в отличие от карточного клиринга, где сотни тысяч операций между парой участников сводятся в одну нетто-позицию в конце дня (см. раздел 31.3). Каждый участник держит в SPI отдельный расчётный счёт; финальность наступает в момент дебета счёта плательщика и кредита счёта получателя [372]. Частного клиринга между участниками нет.

Ключи и DICT

Pix отправляется не по номеру счёта напрямую, а по ключу: номеру мобильного телефона, адресу электронной почты, CPF (идентификационный номер физлица), CNPJ (идентификатор юрлица) или случайному ключу (EVP), который BCB выдаёт как UUID по RFC 4122. Директория DICT (Diretório de Identificadores de Contas Transacionais) под управлением BCB отображает ключ в реквизиты счёта и участника. Перед отправкой банк плательщика обращается к DICT, получает реквизиты получателя и формирует расчётную инструкцию в SPI.

Инициация: QR-код и платёжная строка

BCB определяет форматы инициации Pix в отдельном регламенте [373]. Статический QR-код многоразовый, содержит ключ получателя и опционально сумму. Динамический QR одноразовый, генерируется под конкретную транзакцию и содержит ссылку на платёжную сессию у PSP (payment service provider — поставщик платёжных услуг) получателя; кассовое ПО получает обратный вызов после исполнения. Помимо сканирования, тот же набор полей передаётся как текстовая

платёжная строка, которую копируют в буфер обмена и вставляют в банковское приложение [374]. Платёжная строка нужна, когда PSP-приложение и источник кода открыты на одном устройстве и сканировать QR камерой невозможно.

EMVCo-совместимый формат QR-кода *BR Code* определяет сама схема, поэтому приложения разных банков читают один и тот же код, а подтверждение плательщика в любом канале порождает одно и то же сообщение в SPI.

Сроки и SLA

BCB регулирует сроки Pix отдельным регламентом, периодически пересматривая разрешённые длительности стадий [375]. Документ задаёт максимальные интервалы на отдельные этапы — от запроса к DICT до завершения расчёта — и делает SLA (service-level agreement — соглашение об уровне сервиса) обязательным. Сообщения между участниками и SPI идут по защищённому каналу с подписями по сертификатам ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira — национальная инфраструктура открытых ключей); требования к подписи и каналу прописаны в отдельном регламенте по безопасности [376].

Возвраты и MED

Pix — *push*-перевод (платёж, инициируемый и подтверждаемый со стороны плательщика; противопоставлен *pull*-сценарию карточного списания, см. гл. 21) с немедленной финальностью — той же RTGS-финальностью *в пределах секунд*, что описана в СБП формулировкой «почти сразу» (см. раздел 19.8): разные термины, один механизм. Поэтому обычный возврат идёт как новая, обратная по направлению, операция Pix. Сценарий «я отправил не туда» в Pix урегулирован отдельно: получатель обязан рассмотреть запрос на возврат, но согласие на него остаётся за получателем, если иное не установлено законом или судом.

Для случаев фрода BCB ввёл специальный механизм возврата MED (Mecanismo Especial de Devolução): когда у банка-отправителя есть фактические основания считать операцию фродом, банк через инфраструктуру Pix инициирует запрос на блокировку и возврат суммы у получателя. Регламент исполнения Pix описывает MED как отдельную процедуру схемы [377]. Для плательщика итог функционально близок к карточному *chargeback*: это канал восстановления средств при фроде. Основания и распределение рисков у MED другие: получателя не дебетуют принудительно по решению схемы, а проверяют операцию и могут вернуть средства, если они ещё доступны на счёте.

MED первой редакции (запуск — 2021 год) блокировал и возвращал средства только на первом счёте-получателе; при типичной схеме обналичивания, когда мошенник за секунды распределяет сумму по последовательности счетов-дропов, в 2025 году MED возвращал в среднем 9,3 % оспоренной суммы [378]. С 02 февраля 2026 года BCB сделал обязательной редакцию MED 2.0, регламентированную резолюциями BCB № 493 и № 546 [378]: добровольное подключение открыто с 23 ноября 2025 года, до 10 мая 2026 года действует переходный период без санкций. MED 2.0 заменяет одноразовую блокировку первого счёта процедурой «восстановления средств» (recuperação de valores): директория DICT по запросу банка-отправителя выстраивает граф последующих переводов глубиной до пяти уровней, рассылает уведомления о нарушении участникам по найденному маршруту денег, и каждый из них блокирует остаток на своём счёте до разбора. В MED 2.0 запрос на оспаривание подаётся не через кол-центр, а через обязательную кнопку внутри банковского

приложения; банк плательщика обязан уведомить банк получателя в течение 30 минут, целевой срок возврата по подтверждённой цепочке фрода — 11 дней с момента оспаривания.

20.2 UPI (Индия)

UPI запущен NPCI (National Payments Corporation of India — национальная корпорация платежей Индии) в апреле 2016 года и работает поверх IMPS (Immediate Payment Service) — более раннего сервиса 24/7-переводов. Систему регулирует Резервный банк Индии (RBI) по закону о платёжных и расчётных системах 2007 года [379]. UPI — набор открытых API для банков и небанковских приложений, а также центральный коммутатор NPCI, который маршрутизирует запросы и участвует в клиринге.

VPA и четырёхсторонняя модель

Реквизит платежа в UPI — виртуальный платёжный адрес VPA формата `name@psp` (например, `abhishek@okaxis`). VPA отображается на конкретный банковский счёт без раскрытия номера счёта плательщику. Как ключ Pix в DICT, VPA заменяет пользователю банковские реквизиты.

В отличие от карточной четырёхсторонней схемы (см. раздел 2.1, где сторонами выступают эмитент, эквайер, держатель карты и ТСП), в UPI участвуют стороны других типов: банк-плательщик, банк-получатель, PSP-банк (банк-спонсор, который заключил договор с NPCI и отвечает за TPAP-приложение) и TPAP (Third-Party Application Provider — поставщик стороннего приложения с клиентским интерфейсом). PhonePe, Google Pay, Paytm — крупнейшие TPAP; PSP-банк отвечает перед регулятором за работу этих приложений. NPCI как центральный коммутатор маршрутизирует запросы, идентифицирует участников через VPA, ведёт клиринг и расчёт.

Антифрод и рыночные ограничения

Чтобы ограничить концентрацию, NPCI установил лимит: один TPAP не может превышать 30 % объёма транзакций UPI; доля считается скользящим итогом за предшествующие три месяца. Процедура мониторинга закреплена отдельным циркуляром [380]: при превышении NPCI обязан вводить ограничения для новых пользователей TPAP до возврата доли под порог. Для действующих TPAP срок соблюдения лимита NPCI переносил неоднократно, последний раз до 31 декабря 2026 года [381]. Это рыночное ограничение поверх технического протокола; ничего подобного в правилах СБП, Pix, FedNow или SEPA Instant нет.

В 2025 году NPCI ужесточил требования к использованию UPI-API [382, 383]. Действующий циркуляр ограничивает частоту вызова вспомогательных API: проверка баланса — не более 50 раз в сутки на пользователя в одном приложении, запрос списка счетов — не более 25, мандат *AutoPay* исполняется одной попыткой и не более чем тремя повторами, только вне пиковых часов. Обязательны ежегодный аудит систем у аудитора, аккредитованного CERT-In (национальной группой реагирования на компьютерные инциденты Индии), и письменное обязательство PSP перед NPCI о сдерживании системных вызовов. Эти правила задаёт регулирование

поверх протокола UPI; они сдерживают избыточную нагрузку на банковские системы со стороны массовых TPAP и смягчают эффект, близкий к DDoS (distributed denial of service), при всплесках обращений.

Сценарии и отличие от Pix

UPI поддерживает *push* («я плачу») и *collect* (запрос на оплату: получатель формирует требование, плательщик подтверждает списание). QR-инфраструктура в UPI стандартизирована (Bharat QR / UPI QR), но конкуренция между приложениями смещает массовый сценарий в сторону набора VPA и *deep-link* (URL, открывающего нужный экран мобильного приложения с предзаполненными реквизитами). В Pix оплата проходит через банковские приложения по правилам BCB. В UPI центральный коммутатор принадлежит NPCI, а клиентскую часть собирают конкурирующие TPAP-приложения.

20.3 FedNow (США)

FedNow запущен 20 июля 2023 года и эксплуатируется Федеральными резервными банками [384, 385]. До его появления розничный американский рынок делили Fedwire (межбанковский RTGS для крупных сумм, не 24/7), ACH (Automated Clearing House — пакетные межбанковские переводы, T+1) и частный RTP (Real-Time Payments) The Clearing House (мгновенный, с 2017 года, но не центробанковский). FedNow добавляет центробанковский сервис, доступный всем держателям мастер-счёта в ФРС (master account — расчётный счёт банка непосредственно в Федеральной резервной системе, через который проходят расчёты в деньгах центрального банка).

Правовая основа

FedNow регулируется Subpart C 12 CFR (Code of Federal Regulations) Part 210 [386] и Operating Circular 8 [387]. Платёжная инструкция в FedNow определена как сообщение, переданное через сервис; правила Subpart C вытесняют противоречащие им положения Article 4A UCC (Uniform Commercial Code — единообразный торговый кодекс США). FedNow напрямую подпадает под федеральное регулирование — нормативный акт Совета управляющих ФРС; ответственность участников жёстче, чем у частного RTP, который работает по правилам собственной системы.

Operating Procedures [388] задают требования к работе: 24-часовой операционный день, 7/365, без плановых перерывов. Отдельного закрытия дня у FedNow нет: суточная сверка отделена от расчётного цикла и проходит параллельно сервису.

ISO 20022 как родной формат

В отличие от UPI и СБП с их собственными протоколами, FedNow с момента запуска построен поверх ISO 20022 (международного стандарта финансовых сообщений, подробно разобранного в разделе 21.7). Банк-плательщик передаёт `pacs.008` (Payments Clearing and Settlement — клиентский кредитовый перевод от банка-отправителя к банку-получателю) в FedNow; FedNow дебетует счёт банка-плательщика в ФРС, кредитует счёт банка-получателя; банк-получатель зачисляет средства клиенту. Подтверждение возвращается через `pacs.002` (статус исполнения соответствующего pacs.008), а банк-корреспондент получает через

`camt.054` (Cash Management — уведомление о зачислении или списании) сведения о расчётах своих респондентов по мастер-счёту [389]. Руководство по внедрению и песочница для тестирования сообщений размещены на платформе документирования сообщений MyStandards (SWIFT — Society for Worldwide Interbank Financial Telecommunication) [390].

Расчёт и ликвидность

Расчёт в FedNow валовой, в деньгах центрального банка, через мастер-счёт участника в ФРС. Сетевой расчётный риск (риск дефолта расчётчика/контрагента в системе нетто-расчёта до момента финального расчёта) здесь отсутствует: расчётчиком является ФРС, и дефолт расчётчика невозможен (в отличие от частного RTP). У участника возникает другая задача — поддерживать на мастер-счёте достаточно ликвидности круглосуточно, включая ночи и выходные. Дисконтное окно (*discount window* — краткосрочное обеспеченное кредитование банков центральным банком) вне стандартных часов не открывается, внутридневной кредит (*intraday credit*) доступен в пределах расчётного дня FedNow. Ночью и в выходные участник перераспределяет ликвидность между мастер-счетами переводами управления ликвидностью (*liquidity management transfer*, LMT) внутри самого FedNow [391].

Инициация и антифрод

Своего QR-кода у FedNow нет: в правилах схемы нет ни ссылки для оплаты, ни форматов QR. Запрос на оплату схема определяет как необязательную функцию: участник, включивший её, принимает `pain.013`, показывает запрос клиенту и отвечает `pain.014`, а отправитель запроса гарантирует его законную цель [388]. Остальная инициация оставлена рынку — банковским ядрам, приложениям финтеха, маркетплейсам.

Антифрод FedNow предлагает участнику как набор настраиваемых проверок: лимит суммы одного перевода, негативный список пар «маршрутный номер + счёт», пороги по числу и сумме переводов за период. Эти проверки дополняют собственный антифрод банка и отклоняют сообщение ещё на стороне сервиса [388].

20.4 SEPA Instant Credit Transfer (еврозона)

SCT Inst (SEPA Instant Credit Transfer) — мгновенный кредитовый перевод в евро внутри SEPA (Single Euro Payments Area, единой зоны платежей в евро), определённый правилами Европейского платёжного совета (European Payments Council, EPC). Целевое сквозное время — 10 секунд, 24/7/365 [392]. В еврозоне работают расчётные платформы: центробанковская TIPS (TARGET Instant Payment Settlement, оператор Eurosystem — ECB и национальные центробанки еврозоны) [393] и частная RT1 (Real-Time 1, оператор EBA Clearing — инфраструктурный дочерний оператор Euro Banking Association). Каждый PSP подключается к одной из них; между ними настроена взаимная достижимость (reachability — возможность достичь любого участника другой платформы без отдельного подключения к ней).

IPR: обязательность через регулирование

До 2024 года участие в SCT Inst было добровольным; за шесть лет после запуска (ноябрь 2017 года) часть PSP осталась вне схемы. Обязательным его сделал Regulation (EU) 2024/886 — регламент о мгновенных платежах (Instant Payments Regulation, IPR) [394, 395]. Регламент опубликован в Официальном журнале ЕС 19 марта 2024 года, вступил в силу 8 апреля 2024 года и ввёл сроки обязательной реализации:

- 9 января 2025 года — PSP в еврозоне обязаны принимать SCT Inst и соблюдать тарифную нейтральность (комиссия за SCT Inst не выше, чем за обычный SCT);
- 9 октября 2025 года — PSP в еврозоне обязаны отправлять SCT Inst и предоставлять услугу проверки получателя (Verification of Payee, VOP);
- 9 января 2027 года — PSP вне еврозоны обязаны принимать и соблюдать тарифную нейтральность;
- 9 апреля 2027 года — платёжные институты и институты электронных денег обязаны принимать, в еврозоне также отправлять;
- 9 июля 2027 года — PSP вне еврозоны обязаны отправлять и предоставлять VOP;
- 9 июня 2028 года — PSP вне еврозоны обязаны отправлять SCT Inst со счетов в национальной валюте и в часы, когда обычные переводы в евро не обрабатываются.

IPR отменяет разрешённую ранее наценку за SCT Inst поверх обычного SCT и открывает прямой доступ к платёжным системам для лицензированных небанковских PSP.

Правила SCT Inst 2025

EPC опубликовал свод правил SCT Inst 2025 v1.0 в ноябре 2024 года, а 5 октября 2025 года, за четыре дня до основной волны обязательств IPR, в силу вступила уточнённая редакция v1.1 [392]. Поля, сроки и обработка отказов в своде приведены в соответствие с IPR. Прежнее ограничение по сумме на одну операцию (100 000 EUR) IPR отменяет — лимит определяется правилами расчётной системы и PSP.

Проверка получателя (VOP)

Параллельно с основным сводом EPC ввёл отдельную схему проверки получателя (VOP). Перед инициированием SCT/SCT Inst PSP плательщика спрашивает PSP получателя, соответствует ли указанное имя получателя реквизитам IBAN (International Bank Account Number — международный номер банковского счёта). Ответ — *совпадение*, *близкое совпадение* (с предложенным именем), *нет совпадения* или *проверка невозможна* — передаётся плательщику до подтверждения платежа [396]. Правила EPC ограничивают время от отправки запроса до получения ответа пятью секундами, предпочтительно — не более одной; без ответа за пять секунд плательщик видит *проверка невозможна*. Центральный каталог EPC Directory Service (EDS) хранит данные об участниках схемы и адреса, по которым PSP плательщика направляет VOP-запрос отвечающему PSP.

VOP — обязательная по регулированию мера антифрода: IPR требует от PSP её реализации с 9 октября 2025 года. Клиентский интерфейс A2A-платежа (account-to-account, прямой перевод со счёта на счёт; см. раздел 21.6) в еврозоне обязан явно показывать результат VOP перед подтверждением, а PSP плательщика отвечает за корректное поведение, если плательщик настаивает на отправке при ответе «нет совпадения».

Таблица 33 — Сравнение СБП, Pix, UPI, FedNow и SCT Inst.

	СБП	Pix	UPI	FedNow	SCT Inst
Оператор	НСПК (Банк России)	BCB	NPCI (под RBI)	Федеральные резервные банки	TIPS (Eurosystem) и RT1 (EBA Clearing)
Расчёт	ЦБ через ОПКЦ	BCB через SPI	коммутатор NPCI и банки-расчётчики	мастер-счёт в ФРС	TIPS — деньги ЦБ; RT1 — расчёт через ЦБ по итогам
Запуск	2019	ноябрь 2020	апрель 2016	20 июля 2023	ноябрь 2017
Протокол	ОПКЦ OpenAPI	проприетарный с подписями по сертификатам ICP-Brasil	UPI API NPCI	ISO 20022 (pacs.008)	ISO 20022 (pacs.008)
QR в правилах схемы	да (НСПК)	да (BR Code, BCB)	да (UPI QR, NPCI)	нет	нет
Обязательность	добровольная для банков, обязательная для крупных в ряде сценариев	обязательная с 500 тыс. счетов	регулируется RBI и NPCI	добровольная	обязательная по IPR: в еврозоне с 2025, вне еврозоны с 2027
Антифрод схемы	приостановка по 369-ФЗ	MED	лимит доли 30 %, лимит частоты API	лимит суммы, негативный список, пороги активности	VOP (IBAN + имя)
Возврат	новая операция и процедура у банка	новая операция, MED для фрода	новая операция, диспут через PSP	новая операция, запрос возврата camt.056	новая операция, плюс отзыв по правилам схемы

20.5 Сравнение систем мгновенных платежей

Таблица 33 сопоставляет СБП (гл. 19) с четырьмя разобранными системами.

20.6 Чему учат эти системы

ISO 20022 распространён, но не универсален: у UPI собственный API NPCI, у Pix — собственный протокол с подписями по сертификатам ICP-Brasil, в СБП — ОПКЦ OpenAPI; FedNow и SCT Inst построены прямо на ISO 20022.

Кто оператор расчёта. В Pix и СБП оператором является центральный банк страны с собственной инфраструктурой расчёта. FedNow эксплуатируется самими Федеральными резервными банками. SCT Inst работает на двух платформах (центробанковской TIPS и частной RT1), между которыми настроена взаимная достижимость. В UPI центральный коммутатор принадлежит NPCI, расчёт между банками идёт под надзором RBI. Расчёт в деньгах центрального банка устраняет сетевой расчётный риск, но обязывает регулятора поддерживать круглосуточный сервис и отвечать за любые сбои инфраструктуры.

Где задаётся инициация. Pix и UPI определяют форматы QR-кода и эквивалентов (платёжная строка в Pix, *deep-link* в UPI) в правилах самой схемы. СБП — аналогично, через НСПК. FedNow и SCT Inst оставляют инициацию рынку: схема получает финальную инструкцию pacs.008, а FedNow добавляет к ней лишь необязательный запрос на оплату pain.013. Когда клиентский интерфейс встроен в правила схемы, у плательщиков разных PSP одинаковый сценарий оплаты; когда оставлен рынку, PSP конкурируют интерфейсами, но совместимость становится отдельной задачей рынка.

Роль небанковских участников. UPI ввёл отдельный класс TPAP и ограничил его 30 % объёма [380], чтобы клиентские приложения оставались конкурентными. IPR в еврозоне открывает прямой доступ к платёжным системам лицензированным небанковским PSP. В Pix платёжные институты с разрешением BCB участвуют в схеме наравне с банками, в том числе прямыми участниками SPI [397]. В СБП и FedNow небанковские приложения работают через банк-спонсор, и отдельного класса участника схемы у них нет.

Антифрод как часть схемы. VOP в SCT Inst работает *до* инициации (предотвращение), MED в Pix — *после* (восстановление). В СБП банк обязан на два дня приостановить перевод, если получатель числится в базе Банка России о переводах без согласия. В UPI ограничения вводят регуляторные циркуляры [382]: лимит частоты вызова API, лимит доли объёма для одного TPAP, обязательные аудиты. FedNow даёт участнику настраиваемые проверки (лимит суммы, негативный список, пороги активности), но решение о переводе и ответственность остаются за банком-отправителем и банком-получателем.

Участник нескольких систем мгновенных платежей настраивает сверку, разбор диспутов, клиентский интерфейс и хранение доказательств под каждую систему отдельно: у них различаются сами правовые конструкции возврата, лимитов и антифрода.

21 Открытый банкинг, A2A и ISO 20022

В платеже без PAN объектами модели становятся банковский счёт, право доступа к нему, API для инициации операции и согласие клиента. Здесь и далее **A2A** (*account-to-account*) — класс расчётной модели, в которой деньги переводятся напрямую между банковскими счетами, минуя карточные сети.

21.1 PSD2 и SCA

ВАЖНО

Применимость к РФ. Российское право использует иную модель: платёжные услуги регулирует 161-ФЗ, а доступ к счёту через открытые API развивается через стандарты Банка России и АФТ. В карточном канале функцию усиленной аутентификации выполняют 3-D Secure и механизмы противодействия фроду у эмитента (см. гл. 11). Базовый акт надзора за платёжными услугами — 161-ФЗ [1] (см. гл. 25). Глава описывает PSD2 как систему, чтобы объяснить логику открытого банкинга и ISO 20022; российская инфраструктура требует отдельного анализа.

PSD2 (Payment Services Directive 2, Directive (EU) 2015/2366) перевела доступ к счёту из частного банковского канала в регулируемый интерфейс. Директива описывает платёж как денежное событие и отдельно — роли, через которые он инициируется. В её словаре есть **PSU (payment service user)** — клиент, дающий согласие; **ASPSP (account servicing payment service provider)** — банк или другой провайдер, ведущий счёт; **AISP** (*account information service provider*) — лицензируемая сторона для доступа к данным счёта; **PISP** (*payment initiation service provider*) — лицензируемая сторона для инициирования платежа [225]. Совокупно AISP и PISP называют **TPP** (*third-party provider*) — сторонним поставщиком услуг по PSD2.

Согласие (*consent*) в открытом банкинге — самостоятельный объект: документированное волеизъявление PSU, фиксирующее объём, срок и условия доступа TPP к данным счёта или к инициации платежа. У согласия собственный жизненный цикл, отдельные статусы и отдельный идентификатор, отличный от идентификатора платёжной операции.

Если платёж инициирован через PISP, директива требует от него сразу после инициации передать плательщику подтверждение и ссылочный идентификатор операции. Банку счёта PISP должен передать ссылочный идентификатор этой же операции [225]. Объект «инициация платежа» с самого начала получает собственный идентификатор и сохраняет отдельный жизненный цикл.

SCA (*Strong Customer Authentication*, усиленная аутентификация клиента) добавляет к этой схеме инициации платежа отдельный этап контроля. Банк счёта проверяет, что плательщик подтверждает доступ к счёту или платёж как минимум двумя независимыми элементами из трёх категорий: знание, владение, биометрия [233]. В карточном канале смежную задачу решают 3-D Secure и собственные механизмы противодействия фроду у эмитента. В расчётах со счёта SCA — базовое условие доступа.

Для удалённого электронного платежа RTS (*Regulatory Technical Standards* EBA, Европейской банковской службы, по SCA и общим безопасным каналам связи — EBA RTS on SCA and CSC) добавляют динамическое связывание (*dynamic linking*): до подтверждения плательщик видит сумму и получателя, код аутентификации привязан именно к этой сумме и этому получателю, любое изменение одного из двух

параметров аннулирует ранее сгенерированный код [233]. Клиент подтверждает конкретную операцию с конкретными денежными атрибутами.

SCA связывает между собой согласие клиента, банк счёта и сам платёж. Экран продукта и экран банковского подтверждения должны показывать один набор денежных атрибутов: счёт, получателя и сумму. При расхождении этих атрибутов результат SCA для продукта недостоверен.

RTS одновременно задают основания для упрощения SCA: малая сумма, доверенный получатель, повторяющаяся операция на одну и ту же сумму одному и тому же получателю, перевод между собственными счетами у одного провайдера и анализ транзакционного риска (TRA). Операции, инициированные продавцом, регулируются отдельно от этого перечня [233]. Обязательное подтверждение и упрощение по запросу — разные процедуры. Решение по исключению принимает ASPSP: третья сторона запрашивает упрощённый сценарий, а банк счёта решает, применять ли исключение.

PSD2 и RTS задают распределение ответственности: аутентификация, согласие и окончательное решение по операции остаются за банком счёта. В карточной системе продавец работает через эквайера и PSP. В открытом банкинге ASPSP становится явным участником продуктовой архитектуры: он управляет экраном согласия, проводит SCA и возвращает допуск или отказ; оба исхода предусмотрены протоколом.

Банки сопротивлялись PSD2 по экономической причине: директива сокращала их монополию на клиентский интерфейс. До PSD2 банк контролировал и счёт, и интерфейс доступа к нему. Каждый платёж через интернет-банк или мобильное приложение генерировал данные, которые банк мог монетизировать (допродажи (*cross-sell*), кредитный скоринг, аналитика). PISP переносит инициацию платежа в свой интерфейс, AISP — доступ к данным счёта. Банк продолжает вести счёт и нести расчётный риск, а контакт с клиентом в момент платежа и эксклюзивность данных переходят к агрегатору. Добровольная модель API до PSD2 ограничила массовый доступ компаний финтеха; Еврокомиссия выбрала регуляторное принуждение как способ создать конкурентный рынок [225].

21.2 Открытый банкинг: AISP, PISP и поток согласия

Когда счёт становится доступным через регулируемый интерфейс, **AISP** и **PISP** различаются в доменной модели. AISP работает с доступом к данным счёта и истории операций, тогда как PISP отвечает за инициацию конкретного платежа [225]. В карточном платеже PSP объединяет эти функции в продуктовой модели; в открытом банкинге AISP и PISP проектируются как раздельные сущности.

Масштабируемой интеграции нужен общий профиль API для банков-участников. В Великобритании такой профиль задают стандарты Open Banking UK, в континентальной Европе — Berlin Group NextGenPSD2 [398, 399]. Open Banking UK публикует профили Read/Write API, профиль безопасности и рекомендации к пользовательскому опыту. Berlin Group описывает интерфейс XS2A с моделями согласий, вариантами SCA и перечнем платёжных продуктов. От выбора профиля зависит, где проверять поведение банка — в профиле API, профиле безопасности или документе о пользовательском потоке.

Типовой PISP-поток для одиночного платежа внутри страны в Open Banking UK (*single domestic payment* — так этот класс операций называет спецификация; рис. 50) разделяет шаги по двум фазам жизненного цикла согласия на платёж (`payment-consent` в терминах API). На фазе создания PSU даёт явное согласие

через ASPSP, выполняется SCA по Article 97 PSD2 [225], согласие переходит в статус `Authorised` [400]. На фазе инициации PISP создаёт платёжный ресурс через `POST /domestic-payments` по выданному `access_token`, ASPSP исполняет перевод и доводит статус до `AcceptedSettlementCompleted` или `Rejected`. Каждый одиночный платёж требует собственного согласия с собственной SCA. Серия последующих списаний по сохранённому мандату, аналогичная карточному *card-on-file* MIT, выносится в другой класс операций.

Регулярные списания с одной SCA в Open Banking UK выделены в отдельный профиль Variable Recurring Payments (VRP) [401]. TPP создаёт один объект VRP-согласия (`vrp-consent`) с параметрами лимита (сумма, частота, длительность), пользователь даёт SCA один раз, а последующие платежи VRP (`vrp-payment`) используют это согласие — по исключению SCA-RTS Article 13 (*trusted beneficiaries*) [233] либо через *delegated SCA* от PISP.

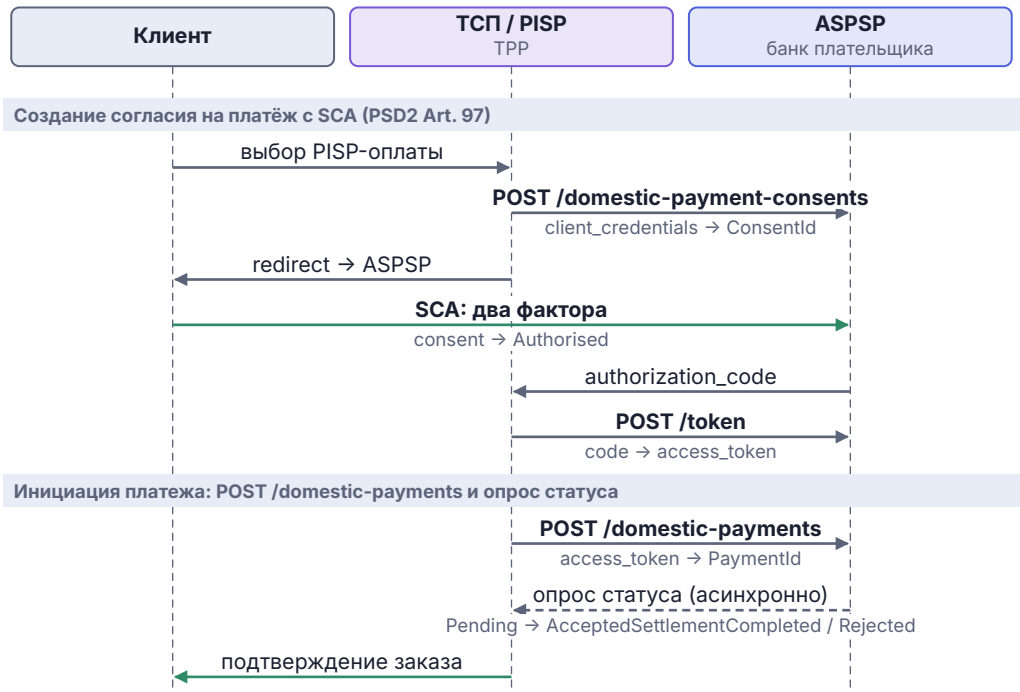


Рис. 50 — Типовой поток PISP в OB UK: создание согласия на платёж с SCA и инициация одиночного платежа внутри страны.

В этих API согласие и платёж описаны как разные ресурсы. На стороне AISP типовой поток начинается с создания ресурса согласия. В Open Banking UK AISP создаёт `account-access-consent` по потоку клиентских учётных данных (*client credentials grant*; поток OAuth 2.0, в котором клиент аутентифицируется перед сервером сам, без участия пользователя), получает `ConsentId` и начальный статус `AwaitingAuthorisation`. После аутентификации пользователя у банка статус меняется на `Authorised` или `Rejected`. Состояние `Revoked` применяется только к ресурсам, созданным до v3.1.4; для более новых ресурсов отзыв согласия оформляется удалением ресурса у ASPSP (`DELETE`) [402, 403].

У PISP разделение видно по статусам согласия и платежа. В типовом потоке Open Banking UK PISP сначала создаёт ресурс `payment-consent` и получает `ConsentId`,

после чего пользователь перенаправляется в ASPSP для аутентификации и подтверждения, и только после этого PISP создаёт платёжный ресурс. Для ресурса согласия в Open Banking UK заданы статусы `AwaitingAuthorisation`, `Rejected`, `Authorised` и `Consumed`; `Consumed` означает только использование согласия для создания платёжного ресурса. Окончательное зачисление получателю подтверждает отдельный статус платежа у ASPSP [400, 404]. Команда, которая ориентируется только на экранное «платёж подтверждён», смешивает эти статусы.

Жизненный цикл `domestic-payment-consent` (рис. 51) уточняет правила перехода. После `Authorised` переход `Revoke` закрыт (PSD2 Art. 80): платёжное согласие краткоживущее, статуса `Revoked` и метода `DELETE` у него нет. `account-access-consent` AISP удаляет через `DELETE` и после авторизации [402, 404].

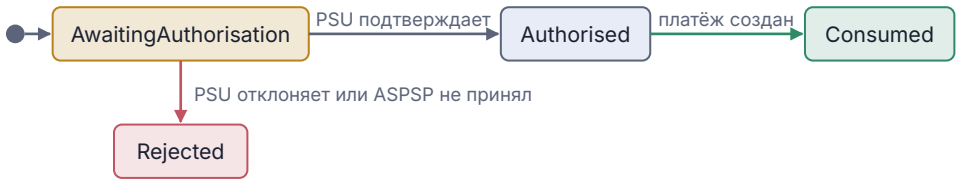


Рис. 51 — Жизненный цикл `domestic-payment-consent` (PISP) в Open Banking UK.

Для аутентификации Open Banking UK поддерживает редирект (*redirect*) и подход *decoupled*, при котором подтверждение выполняется не на том устройстве или не в том канале, откуда отправлен исходный запрос. Редирект требует того же устройства, того же канала и полноценного браузера; телефония, POS и устройства с ограниченным экраном требуют сценария *decoupled*. В потоке *decoupled* SCA выполняет банк, а пользователь подтверждает операцию в отдельном клиенте [405]. Платёжный продукт должен поддерживать смену канала и асинхронный возврат результата; редирект покрывает только один вариант потока.

Поэтому продукт явно хранит как минимум `consent_id`, `payment_id`, локальный идентификатор сессии редиректа, срок жизни токена доступа, идентификатор операции у банка, итоговый статус платёжного ресурса и момент окончания повторного использования согласия или токена. При объединении этих идентификаторов и состояний система присваивает разным причинам один ярлык «обрыв возврата пользователя»: просроченный `access_token`, отклонённое согласие, отменённая у банка операция или отложенный финальный статус.

На карточной странице оплаты (*checkout*) продавец или его PSP управляет взаимодействием до ответа авторизации. В открытом банкинге пользователь подтверждает операцию в интерфейсе банка, а продукт получает результат только через редирект, обратный вызов (*callback*) или повторный запрос статуса. Корректная модель содержит отдельный автомат состояний для согласия, платёжного ресурса и финального результата.

21.3 Промышленные платформы открытого банкинга: ЕС и США

В ЕС правила задаёт PSD2, в США — рыночная инициатива; в обоих случаях интеграция банковских счетов с приложениями сформировала отдельный класс

продуктов — платформы-агрегаторы, которые лицензируются как TPP и подключают сотни банков под единым API. Их API используют большинство потребительских сервисов финтеха.

Plaid [406] — крупнейший агрегатор в США: к его API подключено большинство известных потребительских приложений (Robinhood, Venmo, Coinbase, Affirm). В январе 2020 года Visa объявила о приобретении Plaid за $5,3 млрд; в ноябре того же года Антимонопольное управление Минюста США подало иск о блокировке сделки, и в январе 2021 года стороны её прекратили [407]. TrueLayer [408] — европейский PISP/AISP по PSD2: авторизация FCA, паспортизация в ЕС, продукты Pay-by-Bank. Tink [409] работает на европейском рынке агрегации открытого банкинга (*open banking aggregation*): в марте 2022 года Visa завершила покупку Tink за 1,8 млрд евро (около $2,1 млрд) — для Visa это была вторая попытка войти в сегмент после провала сделки с Plaid. Yodlee [410] — старейший игрок рынка, основан в 1999 году в США, в 2015 году куплен Envestnet за $660 млн, а в 2025 году продан частной инвестиционной компании STG.

Архитектурный контраст с российской моделью: в ЕС и США существуют независимые лицензируемые TPP, которые работают с банковскими данными десятков и сотен банков-партнёров и предоставляют продавцу единый API поверх фрагментированной сети счетов; в России 161-ФЗ [1] закрепляет другую модель. Функцию платформы-агрегатора выполняют сами банки и НСПК через инфраструктуру СБП.

21.4 Открытый банкинг в России

Российский открытый банкинг использует собственную модель внедрения. В ЕС доступ к счёту задан директивой, обязательной для банков; в России он развивается как поэтапная инициатива Банка России и сообщества финтеха со стандартизацией открытых API и переходом от рекомендации к обязательству для определённых сегментов рынка [411, 412].

Концепция открытых API. 9 ноября 2022 года Банк России опубликовал «Концепцию внедрения Открытых API на финансовом рынке»: документ описывает целевую модель со стандартизированными API для обмена данными и инициирования операций со счетами, едиными правилами информационной безопасности и поэтапным расширением круга участников и сценариев [413].

Стандартизация и роль АФТ. Технические стандарты открытых API в России разрабатываются при участии Ассоциации развития финансовых технологий (АФТ) «ФинТех» — профессионального сообщества, объединяющего банки, компании финтеха и Банк России. АФТ публикует рекомендованные стандарты OpenAPI для разных сценариев: получение баланса и выписки, инициирование платежа, аутентификация клиента [412].[1]

Связь с СБП и SBPay. В отличие от европейской модели, где PSD2 и SEPA Instant — две отдельные инициативы с разной логикой развития, российский открытый банкинг изначально проектируется в связке с СБП. Платёжная инициация через открытый API означает запуск перевода через СБП с уже полученным согласием клиента; сервис SBPay (раздел 19.3) — ранний пример продуктовой реализации этой модели для розничных сценариев.

[1] По состоянию на декабрь 2025 года Банк России опубликовал десять стандартов открытых API, разработанных на площадке АФТ; они носят рекомендательный характер. Переход пилотных участников на утверждённые версии спецификаций по счетам физических и юридических лиц намечен на 1 октября 2026 года [414].

Различие моделей. PSD2 в ЕС — регуляторное обязательство банков предоставить доступ к счёту по запросу TPP (с авторизацией клиента). В российской модели внедрение обязательных API поэтапное: сначала добровольное участие банков, потом обязательное — для определённых типов API и определённых участников. Право клиента отказать в доступе сохраняется в обоих подходах, а архитектура внедрения различается по степени регуляторного давления и по темпу.

ВАЖНО

Европейская терминология AISP и PISP применима к российской модели как описание функций. Российская регуляторика закрепляет другую конструкцию: право инициировать платёж и читать данные по счёту возникает из договора участника с банком, стандартизированного механизма согласия и участия в информационном обмене по Открытым API.

21.5 ФАПИ.СЕК: российский профиль безопасности открытых API

Концепция Банка России задаёт регуляторную модель; протокольная часть состоит из FAPI и ФАПИ.СЕК. FAPI (Financial-grade API) — международный профиль безопасности, на котором построены открытый банкинг Великобритании и часть европейских внедрений. ФАПИ.СЕК — российская адаптация FAPI к требованиям информационной безопасности Банка России и отечественной криптографии [415].

FAPI как профиль безопасности

Базовый OAuth 2.0 (*Open Authorization* — фреймворк делегированной авторизации, RFC 6749) проектировался для авторизации доступа к произвольным API. В финансовом сценарии опасны слабые места базового протокола: параметры запроса передаются в URL, ответ авторизационного эндпоинта возвращается неподписанным, токен доступа отвязан от ключа клиента и TLS-сессии. В базовом OAuth 2.0 одни и те же механизмы работают и для входа на новостной сайт через Google, и для авторизации платежа со счёта клиента. Финансовому рынку требуется более строгий профиль.

Профиль FAPI разрабатывает рабочая группа OpenID Foundation. Он расширяет базовый OAuth 2.0 и OpenID Connect (OIDC — уровень идентификации поверх OAuth 2.0) до уровня, пригодного для операций с деньгами. **FAPI 1.0 Part 2: Advanced** (утверждён 12 марта 2021 года) обязал использовать подписанный *request object* [416] (JSON Web Token — JWT, RFC 7519 — с параметрами авторизационного запроса, подписанный закрытым ключом клиента; семейство стандартов JOSE: JWS — JSON Web Signature, JWE — JSON Web Encryption, JWK — JSON Web Key) вместо параметров в URL, токены, ограниченные отправителем (*sender-constrained*; токен доступа, который использует только клиент, доказавший владение конкретным криптоключом или TLS-сертификатом) через mTLS (*Mutual TLS* — взаимная TLS-аутентификация, RFC 8705), защиту ответа авторизации ID-токеном как отделённой подписью либо через JARM (*JWT Secured Authorization Response Mode* — подписанный JWT-ответ авторизационного эндпоинта) и аутентификацию клиента через `tls_client_auth` или `private_key_jwt`. PKCE (*Proof Key for Code Exchange*, RFC 7636 [417]) с алгоритмом S256 (вариант *code challenge* на SHA-256) профиль требует только для предварительно переданных запросов авторизации (PAR). Профиль рассчитан на конфиденциальных клиентов [418].

FAPI 2.0 Security Profile (утверждён 19 февраля 2025 года) ужесточил профиль. Pushed Authorization Requests (PAR, RFC 9126 [419]) стал обязательным: авторизационный запрос переносится из URL на отдельный эндпоинт авторизационного сервера, который возвращает короткий `request_uri`. Токены, ограниченные отправителем, остались обязательными, но к mTLS добавилась альтернатива в виде DPoP (*Demonstrating Proof of Possession* — привязка токена к закрытому ключу клиента через подписанное доказательство, RFC 9449 [420]) для сценариев со сложной инфраструктурой взаимного TLS. PKCE S256 и TLS 1.2+ остались обязательными [421].

FAPI 2.0 Message Signing (утверждён 26 сентября 2025 года) дополнил профиль обязательной подписью самих сообщений запроса и ответа к ресурсу; подпись на этапе авторизации покрывает только часть доказательной последовательности. Подпись сообщений нужна для неотказуемости (*non-repudiation*) в сценариях, где финансовый институт обязан доказать содержание операции спустя длительное время после её исполнения [422].

Профили FAPI описывают, *что* должны делать стороны и *как* выглядит передаваемое сообщение. *Чем* оно подписывается — RSA, ECDSA, ГОСТ, — задаёт реализующий профиль через алгоритмы JWS из реестра IANA. Поэтому национальная адаптация FAPI включает замену криптографической части и локальную регуляторную надстройку — логика протокола сохраняется.

ФАПИ.СЕК: что наследуется, что меняется

СТО БР ФАПИ.СЕК-1.6-2024, введённый приказом от 07.10.2024 № ОД-1615 «О введении ФАПИ.СЕК», заменил редакцию 2020 года и стал актуальным профилем безопасности для открытых API. Стандарт разработан АФТ совместно с ИнфоТеКС при участии Банка России [415, 423].

Структура стандарта прямо наследует профили FAPI. ФАПИ.СЕК состоит из базового профиля безопасности OpenID API (соответствует FAPI 1.0 Part 1: Baseline) и расширенного профиля (соответствует FAPI 1.0 Part 2: Advanced). JARM, защищённый JWT-режим ответа авторизационного эндпоинта, описан в общих положениях (пункт 5.4.5) и применяется в расширенном профиле [415].[1] Расширенный профиль ФАПИ.СЕК требует тех же механизмов, что и FAPI Advanced: подписанный *request object*, переданный по значению в параметре `request` или по ссылке в `request_uri`, токены, ограниченные отправителем через mTLS, `private_key_jwt` либо `tls_client_auth`. PKCE, обязательный в базовом профиле, в расширенном профиле ФАПИ.СЕК не применяется (пункт 7.2.1).

Главное расхождение касается криптографии: для обмена внутри России ФАПИ.СЕК предписывает отечественные криптографические алгоритмы согласно методическим рекомендациям ТК 26 МР 26.2.002-2024 «Использование российских криптографических алгоритмов в протоколах OpenID Connect» [426]; при трансграничном обмене механизмы определяет соглашение сторон [415]. Подпись JWT и проверка подписи — по ГОСТ Р 34.10-2012 на эллиптических кривых вместо RSA или ECDSA. Хеш-функция в JWS, JWE и JWT — ГОСТ Р 34.11-2012 «Стрибог» вместо SHA-2. Симметричное шифрование в JWE — по ГОСТ Р 34.12-2015 («Кузнечик» или «Магма») вместо AES. Транспорт — TLS с российскими криптонаборами (ГОСТ TLS) вместо обычного TLS 1.2/1.3 с международными криптонаборами. Подпись запросов, хранение ключей и программные реализации криптографии ФАПИ.СЕК допускает только через сертифицированные СКЗИ (средства криптографической защиты информации).

[1] Международные спецификации, которые наследует ФАПИ.СЕК: [424], [418], [425].

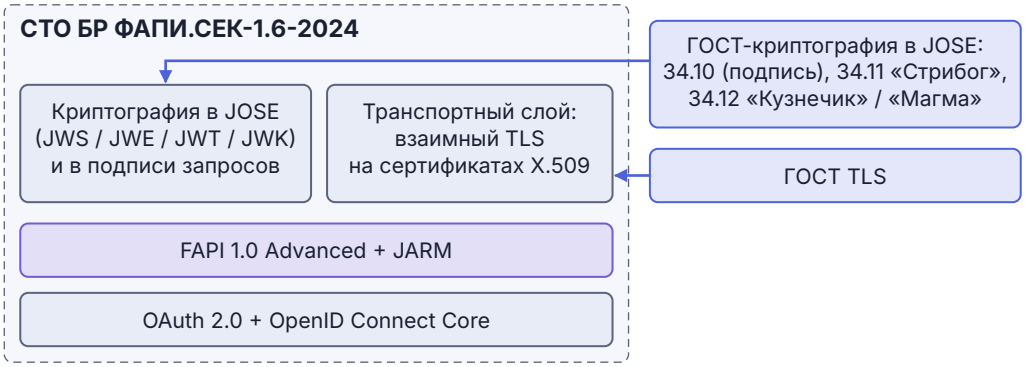


Рис. 52 — Стек ФАПИ.СЕК: процедурная часть FAPI и JARM поверх отечественной криптографии и ГОСТ TLS.

Отдельный стандарт СТО БР ФАПИ.ПАОК-1.0-2024, введённый приказом от 07.10.2024 № ОД-1616 «О введении ФАПИ.ПАОК», описывает профиль аутентификации по отдельному каналу, инициированной клиентом OpenID Connect, то есть приложением, запрашивающим доступ от имени пользователя (Client Initiated Backchannel Authentication, CIBA) [427]. Сценарий нужен там, где у устройства, инициирующего доступ, ограничены браузер или экран подтверждения: оплата с умной колонки, подтверждение через мобильное банковское приложение в ответ на инициацию из контактного центра, аутентификация на устройстве с отдельным клиентским входом. ПАОК относится к ФАПИ.СЕК так же, как *decoupled authentication* — к основному сценарию с редиректом у Open Banking UK [405]: разные каналы доставки шага аутентификации при общей модели доверия.

Согласие, аутентификация и подпись запроса

ФАПИ.СЕК наследует от FAPI раздельную модель объектов. Согласие хранится на стороне ASPSP (в российской терминологии — **ПУ**, *поставщик услуг*; роль TPP исполняет **СПУ** — *сторонний поставщик услуг*, обращающийся к API ПУ от имени клиента) с собственными статусами `AwaitingAuthorisation`, `Authorised`, `Rejected` и `Revoked`; срок действия задаёт поле `expirationDateTime`, отдельного статуса истечения нет [428]. Сама аутентификация клиента выполняется средствами банка согласно регуляторным требованиям. Подписанный запрос инициации операции — отдельный объект, в котором клиентское приложение доказывает, что согласие действительно и операция совпадает с тем, что подтвердил клиент.

В типовом сценарии инициации платежа (рис. 53) клиентское приложение формирует *request object* — JWT с описанием операции, подписанный закрытым ключом клиента средствами СКЗИ по ГОСТ Р 34.10-2012. Браузер клиента перенаправляется в банк с запросом аутентификации, который несёт этот объект по значению в параметре `request` или по ссылке в `request_uri` [415]; банк проверяет подпись запроса, выполняет многофакторную аутентификацию (*multi-factor*) по требованиям к средствам идентификации, показывает экран согласия с параметрами операции и возвращает `authorization_code` по обратному вызову. Клиентское приложение меняет `authorization_code` на `access_token`, привязанный к mTLS-сертификату, и использует токен для самого вызова API инициации платежа.

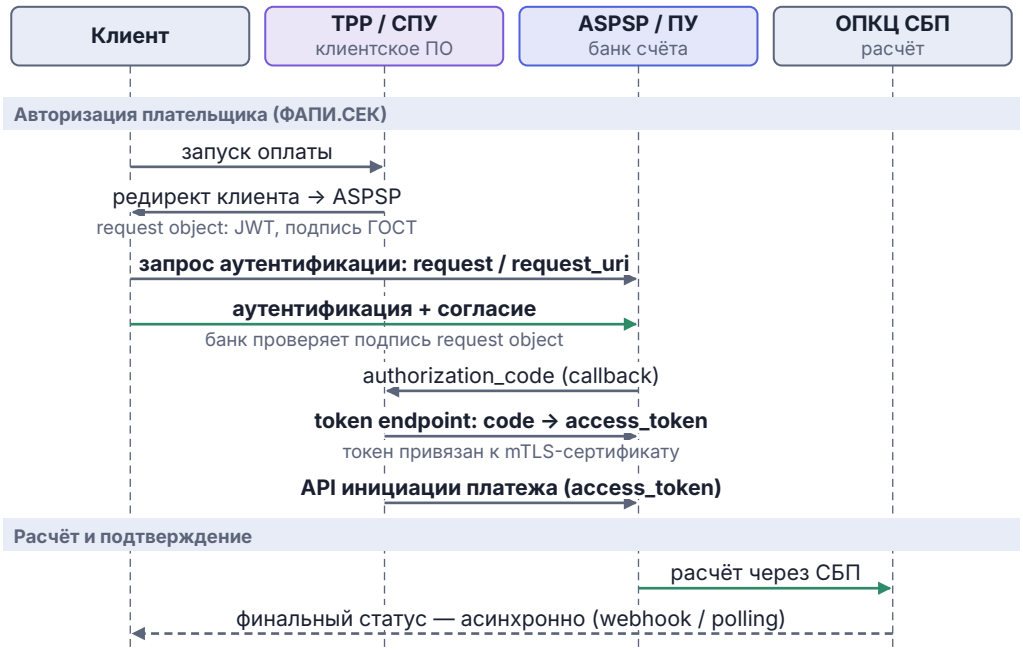


Рис. 53 — Поток инициации платежа через ФАПИ.СЕК с расчётом через ОПКЦ СБП.

Привязка `access_token` к mTLS-сертификату ограничивает токен контекстом ключа: для вызова API нужен сопутствующий криптоматериал, который хранится у легитимного клиента средствами СКЗИ. Если токен повторно используют с другого узла инфраструктуры СПУ, банк отказывает на этапе вызова API инициации платежа. Тот же принцип защищает от подмены подписи: запрос инициации с тем же `access_token` и подписью JWT, отличающейся от открытого ключа клиента из его документа Key Set (по разделу 5.7.3.4 ФАПИ.СЕК [415]), банк отклоняет до показа экрана согласия как ошибку конфигурации клиента.

Каждый шаг процедуры даёт отдельный код ответа. Ошибка проверки подписи *request object* отклоняет запрос до показа экрана согласия. Истекшее или отозванное согласие лишает силы выданный по нему `access_token`; банк возвращает статус, отличный от «недостаточно средств» или «лимит превышен». Сертификат клиента в mTLS, отличный от привязки токена, требует нового запроса аутентификации. Продукт, который объединяет все эти отказы в одну колонку «общий сбой платежа», ухудшает диагностику отказов так же, как описано в разделе 21.8 для Open Banking UK.

Жизненный цикл объекта согласия (рис. 54) зафиксирован в разделе 9.3.3 `ConsentStatus` стандарта, введённого приказом от 19.12.2025 № ОД-2895 «О введении стандарта согласия на доступ к счетам юрлиц» [429]. `DELETE`-операцию СПУ вызывает, когда пользователь отозвал согласие на стороне СПУ [429], как AISP удаляет `account-access-consent` в Open Banking UK; закрытый после `Authorised` переход `Revoke` относится там только к платёжному согласию.

ФАПИ.СЕК и 3-D Secure решают смежные задачи в разных системах. SCA в 3-D Secure аутентифицирует держателя карты по конкретной операции и работает внутри карточной сети. ФАПИ.СЕК аутентифицирует клиента банка по доступу к счёту и работает поверх инфраструктуры открытых API. У двух механизмов общий принцип сильной аутентификации из двух факторов разных категорий и разные

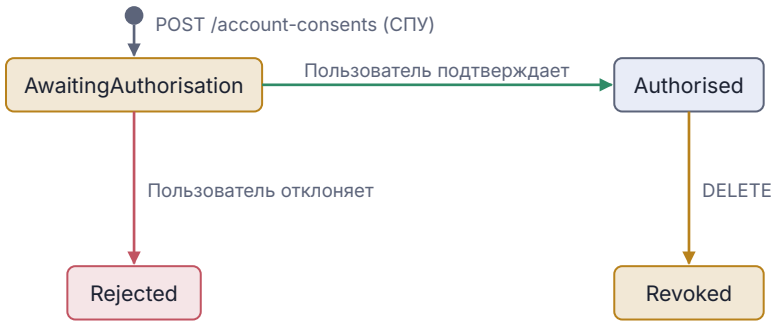


Рис. 54 — Жизненный цикл объекта согласия в ФАПИ.СЕК.

точки доверия в потоке операции. Для пользователя оба механизма выглядят как уведомление в приложении банка, а регулируются и сертифицируются раздельно.

Связка с СБП и график обязательности

ФАПИ.СЕК — технический протокол доступа к счёту и инициации операций по нему. Когда инициация платежа доходит до этапа исполнения, расчёт идёт через ту же инфраструктуру, что и любой другой A2A-платёж в России — через ОПКЦ СБП и платёжную систему Банка России (см. раздел 19.7). Полная A2A-модель состоит из регулируемого интерфейса доступа к счёту и мгновенной межбанковской расчётной системы.

Концепция Банка России от 9 ноября 2022 года задала исходный график [413], но после обратной связи от 166 организаций его пересмотрели. Документ Банка России от 2 сентября 2024 года «Основные принципы и этапы внедрения Открытых API на финансовом рынке» подтвердил гибридный подход и перенёс начало обязательного применения на 2026 год тремя этапами [430]. До начала обязательного применения в 2026 году использование Открытых API для всех участников финансового рынка остаётся рекомендательным.

Этап 1 (2026 год) распространяет обязательные требования только на крупнейших участников трёх секторов финансового рынка — банковского, страхового и инвестиционного, по критериям Банка России (все системно значимые банки, крупнейшие брокеры и страховые организации). Микрофинансовый сектор, фигурировавший в Концепции 2022 года, из первого этапа исключён [430]. Окончательный срок реализации этапа 1 зависит от готовности правовых и инфраструктурных условий; даты этапов 2 и 3 пересматриваются по результатам этапа 1.

24 декабря 2025 года Банк России опубликовал обновлённый комплекс стандартов Открытых API, утверждённых приказами от 19.12.2025. Стандарты сохраняют рекомендательный характер [431]; переход пилотных участников на новые версии спецификаций по счетам физических и юридических лиц запланирован на 1 октября 2026 года [414]. Окончательные сроки и состав обязательных API меняются; точные даты сверяются по сайту Банка России и публикациям АФТ [411, 412, 432].

Целевой комплекс на октябрь 2026

Состав целевого комплекса зафиксирован приказами Банка России от 19.12.2025. Приказ от 19.12.2025 № ОД-2887 «О введении общих положений и глоссария

СТО БР по открытым API» утвердил общие положения и глоссарий [433]. Приказ от 19.12.2025 № ОД-2894 «О введении стандарта доступа к информации о счетах физлиц» ввёл Accounts API ФЛ версии 2.0 [434]. Приказы от 19.12.2025 № ОД-2892 «О введении стандарта согласия на доступ к счетам физлиц» и от 19.12.2025 № ОД-2895 «О введении стандарта согласия на доступ к счетам юрлиц» ввели Account-Consents API [428, 429]. Кроме того, в комплекс входят правила взаимодействия (Accounts API Rules), технический стандарт расширенного профиля безопасности и рекомендательные материалы — *Best Practices* и *Methodological Recommendations*. Все целевые стандарты вступают в действие 1 октября 2026 года [432].

В российской модели европейские роли AISP и PISP заменены собственной парой ролей. **Поставщик услуг (ПУ)** — организация, ведущая счёт клиента и публикующая Открытые API; функциональный аналог ASPSP. **Сторонний поставщик услуг (СПУ)** — организация, обращающаяся к API ПУ от имени клиента; функциональный аналог TPP. И ПУ, и СПУ в российской модели работают через договор с банком и включение в реестр участников информационного обмена по Открытым API, ведение которого планирует Банк России. Вместо европейского лицензионного статуса действует договорная модель с реестром [430, 432].

Спецификация Account-Consents API задаёт эндпоинты: `POST /account-consents` для создания ресурса согласия, `GET /account-consents/{consentId}` для проверки статуса и `DELETE /account-consents/{consentId}` для отзыва. Авторизация всех трёх вызовов — по потоку *Client Credentials*; обязательный заголовок всех трёх — `x-fapi-interaction-id` (корреляция операций по UUID), `POST` дополнительно несёт `x-jws-signature` (отделяемая подпись JWS тела запроса по ГОСТ) [429]. `permissions` согласия наследуют модель Open Banking UK: `ReadAccountsBasic`, `ReadAccountsDetail`, `ReadBalances`, `ReadTransactionsBasic`, `ReadTransactionsCredits`, `ReadTransactionsDebits`, `ReadTransactionsDetail` [429].

Инициирование платежей через Открытые API описывает стандарт Банка России от 23.10.2020 «Инициирование перевода денежных средств клиента третьей стороной в валюте Российской Федерации» со спецификацией API версии 1.2.1 [435]. Новую спецификацию Payment Initiation для юридических лиц АФТ разрабатывает отдельно; она относится к следующим этапам и сохраняет рекомендательный статус [432]. До её введения единственный массовый канал A2A-инициации платежа со счёта в России — СБП.

Управление согласиями клиентов в среде Открытых API консолидируется в Платформе коммерческих согласий (ПКС), которую Банк России и Минцифры строят на базе Единого портала государственных и муниципальных услуг (Госуслуги). Хранение самих клиентских данных остаётся у участников рынка, на ПКС — только согласия. Пилот ПКС был запланирован на 2025 год с последующим переходом к централизованному управлению жизненным циклом согласий [411, 430].

Российский профиль рядом с европейскими

Табл. 34 сопоставляет ФАПИ.СЕК с Open Banking UK, Berlin Group NextGenPSD2 и базовым FAPI 2.0.

Главное отличие ФАПИ.СЕК от Open Banking UK и Berlin Group инфраструктурное: процедуры наследуются от FAPI, а под ними меняются криптография и TLS на отечественные алгоритмы, требуются сертифицированные СКЗИ у всех участников, лицензируемые роли TPP вытеснены договорной моделью с банком. Для команды, проектирующей продукт на ФАПИ.СЕК, FAPI 1.0 Advanced и JARM остаются

Таблица 34 — ФАПИ.СЕК рядом с европейскими профилями открытого банкинга.

Параметр	ФАПИ.СЕК (РФ)	Open Banking UK	Berlin Group (ЕС)	FAPI 2.0 (OIDF)
Базовый профиль	FAPI 1.0 Advanced + ГОСТ-надстройка	FAPI 1.0 Advanced	собственный профиль NextGenPSD2, OAuth 2.0 — один из вариантов SCA	FAPI 2.0
Криптография	ГОСТ Р 34.10/34.11/ 34.12 в JWS, JWE, JWK	RSA, ECDSA, SHA-2	RSA, ECDSA, SHA-2	задаётся реализующим профилем
Транспорт	ГОСТ TLS	TLS 1.2+	TLS 1.2+	TLS 1.2+
Подпись запроса	request object на ГОСТ, СКЗИ обязательно	signed JWT, mTLS	HTTP-подпись на QSeal по требованию ASPSP, TLS с QWAC	не требуется: целостность запроса даёт PAR, подпись — в профиле Message Signing
Лицензируемые роли	договор с банком + соответствие стандарту	AISP, PISP по PSD2	AISP, PISP, CBPII по PSD2	за пределами профиля
Расчётный канал	ОПКЦ СБП	Faster Payments	SEPA Instant либо локальная RTGS	за пределами профиля
Статус	рекомендательный, поэтапный переход к обязательному	обязательный для девяти крупнейших банков	обязательный по PSD2	добровольная адаптация

основным источником понимания процедурной части, а МР 26.2.002-2024 ТК 26, 821-П [205] и 851-П [206] (см. раздел 25.2) — источниками требований к криптографии и эксплуатации.

21.6 A2A-платежи

PISP инициирует перевод со счёта клиента, а расчётная система исполняет движение денег между банками. Открытый банкинг отвечает за согласие и безопасный доступ к счёту; A2A задаёт модель движения денег между банковскими счетами.

Сравнение национальных систем мгновенных платежей (СБП, Pix, UPI, FedNow, SEPA Instant) — в гл. 20. A2A здесь — класс расчётной модели; архитектура у каждой страны своя.

В Pix расчёт выполняет SPI — центральная инфраструктура расчёта мгновенных платежей Banco Central do Brasil, валовой расчёт в реальном времени через специальные счета участников в центральном банке, после расчёта перевод становится безотзывным [372]. Положительный статус A2A-перевода значит, что деньги уже зачислены получателю, а карточная авторизация подтверждает только разрешение на будущее списание; подробный разбор финальности, возвратов и споров — в разделе 19.9, расхождение жизненного цикла двух моделей сведено в табл. 35.

Таблица 35 — Жизненный цикл карточной операции и A2A-перевода.

Система	Что даёт первый положительный ответ	Когда деньги считаются окончательными	Как устроены возврат и спор
Карточный платёж	Разрешение на авторизацию и резервирование средств	После отдельного клиринга и расчёта по правилам сети	Возврат существует отдельно от авторизации/подтверждения; chargeback встроен в сетевые правила
A2A-платёж	Подтверждение инициирования перевода или его исполнения, в зависимости от системы	Когда межбанковский перевод исполнен и система считает его окончательным	Возврат — новый перевод по инициативе плательщика; спор решается правилами конкретной системы

В электронной коммерции мгновенная расчётная система сокращает для продавца интервал между подтверждением покупателя и зачислением денег. Промежуточный статус требует отдельного правила отгрузки, а возврат — отдельного денежного перевода или процедуры спора. A2A требует своей модели управления заказом, своей поддержки и собственной логики сверки.

21.7 ISO 20022 в A2A и переводах

ISO 20022 задаёт семантическую модель: у поля есть имя и место в общей структуре сообщения. Стандарт удобен там, где один и тот же платёж должен одновременно поддерживать маршрутизацию, санкционный контроль и ПОД/ФТ, сверку, выписку и отчётность [436].

Семейства сообщений соответствуют разным участкам платёжной последовательности. `pain` покрывает клиентскую инициацию (*customer initiation*) — запросы клиента на инициирование платежа; `pacs` используется в межбанковском клиринге и расчёте (*payments clearing and settlement*); `camt` относится к управлению денежными средствами (*cash management*) и отвечает за статусы, выписки, уведомления и связанные сообщения управления ликвидностью [437].

В типовом сценарии клиент или его система формирует `pain.001` как инструкцию на кредитовый перевод. На межбанковском уровне перевод идёт как `pacs.008`; ответ о состоянии на этом же уровне приходит через `pacs.002`. Когда деньги отражаются в учёте клиента, банк присылает `camt.054` или включает операцию в выписку вида `camt.053`. У каждого шага своя аудитория и своя доказательная сила. Если приложение получает только пользовательский API, а сверка строится по `camt`, между ними требуется явное внутреннее соответствие.

Структурированное сообщение окупается на сверке. Для сверки и расследования нужны сумма, валюта, поля уровня `EndToEndId`, идентификаторы дебитора и кредитора, структурированное назначение платежа и код причины в статусном сообщении. В карточном канале эти данные распределяются между внешним процессинговым диалектом (*processing*) и файлами клиринга. В ISO 20022 они закладываются в саму модель сообщения.

Миграция обходится дороже перехода с одной XML-схемы на другую. При переходе на новый профиль ISO 20022 меняются правила заполнения полей, правила применения (*usage guidelines*), допустимые статусы и обязательность отдельных атрибутов. Каноническая модель платежа внутри продукта локализует такой переход;

общая внутренняя запись заставляет одновременно переписывать API, оркестрацию и сверку.

В SWIFT период сосуществования двух форматов сообщений (*coexistence period*) для межбанковских платёжных инструкций — MT (*Message Type*, формат FIN MT в SWIFT) и ISO 20022 — завершился в выходные переключения (*cutover weekend*) 21–23 ноября 2025 года [10, 11]. После этой даты основным рабочим форматом для таких инструкций стал ISO 20022. С 1 января 2026 года резервная обработка для отправителей, остающихся на MT (*contingency processing*), и сквозная конверсия MT↔ISO внутри сети SWIFT (*in-flow translation*) тарифицируются отдельно. MT 199 и MT 299 для обработки исключений (*exception handling*) сохраняются после ноября 2025 года как переходный канал и подлежат окончательной отмене в ноябре 2027 года, когда их функцию полностью переймут сообщения camt.110 и camt.111 [11]. Помимо названия сообщения интегратору приходится учитывать профиль, правила переходного периода и процедуру обработки исключений.

В России Банк России ведёт отдельный раздел по стандарту ISO 20022, описывает его как основу собственных стандартов финансовых сообщений и отдельно поддерживает обмен сообщениями ISO 20022 в СПФС [438, 439]. Структурированные данные нужны для SWIFT, международных переводов и внутренних платёжных систем, которые используют счёт вместо PAN.

21.8 Открытый банкинг: отличия от A2A и карточной оплаты

В разговорах об A2A-платежах смешивают разные вещи: доступ к счёту и управление согласием; расчётный канал, по которому идут деньги; язык межсистемного сообщения. При таком разделении разговор об «оплате со счёта» становится точным.

Карточная страница оплаты работает с PAN, эмитентным каналом авторизации, клирингом и правилами споров карточной сети. A2A-модель работает с согласием на доступ к счёту, инициированием банковского перевода и финальностью расчётной системы. СБП — частный случай A2A-системы; настоящая глава вводит более

Таблица 36 — Составляющие A2A-платежа: доступ к счёту, расчёт, сообщение.

Компонент	На какой вопрос отвечает	Кто управляет	Ошибка при смешении
API доступа и согласия	Кто и на каких правах может обратиться к счёту	ASPSP, профиль API, профиль безопасности, управление согласиями	Команда принимает истечение токена или отказ согласия за сбой расчётной системы
Расчётная система	Как деньги переводятся между счетами и когда они окончательны	Платёжная система, расчётная инфраструктура, правила системы	Промежуточный статус принимается за расчёт; возврат проектируется как отмена уже исполненного перевода
Стандарт сообщения	Как операция описывается между системами и в отчётности	профиль ISO 20022, правила применения, локальные альбомы сообщений	Внешний API и внутренний реестр обязательств становятся зависимыми от одного конкретного формата сообщения

общий класс, в котором доступ к счёту и банковский перевод образуют самостоятельную архитектуру.

Последнее разделение — между отказом, статусом и спором. Отказ на этапе согласия или инициации — предусмотренная часть протокола: токен истёк, клиент отменил согласие, банк отклонил выбранный сценарий SCA, счёт недоступен. Статус платежа — отдельная задача: деньги остаются промежуточными даже при `Consumed` у согласия или `Accepted` у API. Спор после исполнения перевода — ещё одна задача со своей процедурой разрешения конфликта.

Три инженерных объекта — согласие, денежная операция, межсистемное сообщение — сохраняют собственные жизненные циклы и после того, как пользователь увидел экран «Оплачено». Если эти состояния объединены в одну запись во внутреннем учёте, истёкший токен, ожидание `pacs.002` и спор после расчёта попадают в одну колонку ошибок и требуют ручного разбора.

ПРАКТИКА

При проектировании A2A-платежей разделите внутренние объекты: объект согласия, объект денежной операции и объект межсистемного сообщения. Тогда миграция на новый банк, новую расчётную систему или новый профиль ISO 20022 меняет один объект; остальные части системы сохраняют свои контракты.

22 Платежи по QR и кошельки

QR-код и платёжное приложение не образуют отдельной платёжной системы. Фактический расчёт выполняет карточная сеть, A2A-перевод или закрытый кошелёк. Карточные системы остаются основой потребительских расчётов; альтернативы выигрывают там, где снижают комиссию, дают рассрочку или решают локальную задачу.

22.1 Таксономия методов оплаты

Метод оплаты задают признаки: кто инициирует списание, где наступает финальность и кто несёт риск спора. По этим признакам карта, банковский перевод, кошелёк, рассрочка и цифровые деньги расходятся сильнее, чем по виду кнопки или QR-кода на кассе.

Первый класс — карточные платежи: Visa, Mastercard, Мир, UnionPay и American Express. Продавец инициирует списание, отправляя запрос по карточным реквизитам клиента и получая либо авторизацию, либо отказ. Преимущества карт — глобальная инфраструктура, chargeback (сетевой возврат средств эмитентом по спорной операции, в отличие от коммерческого возврата продавца; см. гл. 32) и развитая практика PCI DSS (Payment Card Industry Data Security Standard — отраслевой стандарт защиты карточных данных; область применимости разбирается в гл. 12). Ограничение — стоимость приёма для продавца.

Второй класс — переводы со счёта на счёт (account-to-account, A2A), где клиент подтверждает перевод со своего счёта на счёт продавца — это *push*-модель, в отличие от *pull* карточных платежей, где списание по реквизитам клиента инициирует продавец. К A2A относятся СБП, SEPA Instant Credit Transfer, Pix и UPI [359, 370, 379, 440]. Преимущества A2A — финальность (после зачисления перевод нельзя односторонне отменить по правилам системы) и низкие комиссии; ограничение — более узкая защита покупателя.

Третий класс — кошельки: надстройка над базовой платёжной инфраструктурой. Закрытый кошелёк (*closed-loop wallet*) учитывает средства на собственном балансе и проводит расчёт внутри своего реестра, как Alipay и WeChat Pay. Открытый кошелёк (*open-loop wallet*) заменяет реквизиты карты платёжным токеном. По этой модели работают Apple Pay и Google Pay; о платёжной токенизации, на которой строится открытый кошелёк, подробно см. гл. 9. Для российских карт после марта 2022 года оба сервиса недоступны; их функции частично заменяют Mir Pay и SBPay (см. раздел 22.3).

Четвёртый класс — BNPL (Buy Now Pay Later): провайдер оплачивает продавцу всю сумму сразу, а клиент возвращает её частями по собственному графику. Для продавца BNPL похож на эквайринг с иной комиссией, но экономическая модель другая: ключевой элемент — кредитное решение провайдера, подробно разобранное в гл. 23.

Пятый класс — наличный сценарий (*cash-based*), в котором платёж начинается онлайн, но завершается офлайн через ваучер или платёжный идентификатор. Типичный пример — OXXO в Мексике, где покупатель получает код платежа и завершает операцию в физической точке [441]. Продавец получает подтверждение только после того, как покупатель внесёт деньги в кассе.

Шестой класс — цифровые деньги вне банковского депозита. Цифровая валюта центрального банка (central bank digital currency, CBDC) — цифровая форма обязательства центрального банка; цифровой рубль разобран в гл. 24. Криптовалюты и стейблкоины строятся на иной модели эмиссии и регулирования, а с CBDC их объединяет только учёт средств вне банковского счёта.

Таблица 37 — Сравнение методов оплаты по ключевым параметрам

Метод оплаты	Тип	Финальность	Chargeback	Область PCI	Международность	Скорость	Комиссия ТСП
Карты	pull	нет	есть	да	глобальный	мс	высокая
A2A (СБП/Pix)	push	да	нет	нет	региональный	сек	низкая
Закрытый кошелёк	push/pull	зависит	ограничен	нет	нишевый	мс	средняя
BNPL	pull	нет	есть	нет	региональный	сек	средняя
Наличный сценарий	push	да	нет	нет	нишевый	часы / дни	нет данных
CBDC (цифровой рубль)	push	да	нет	нет	региональный	сек / мин	нет данных
Криптоактивы	push	да	нет	нет	глобальный / нишевый	мин / часы	нет данных

Зелёный цвет показывает сравнительное преимущество, красный указывает на ограничение, серый — на нейтральную или зависящую от провайдера зону. Колонки: «Тип» — *push* (инициирует и подтверждает клиент) или *pull* (списание инициирует продавец); «Финальность» — безотзывность перевода после зачисления по правилам системы; «Chargeback» — наличие сетевого механизма *chargeback*, а не коммерческого возврата (см. гл. 32); «Область PCI» — попадание продавца в область применимости PCI DSS (см. гл. 12). Приведённые оценки меняются в зависимости от конкретного провайдера, маршрута и географии.

22.2 Модели платежей по QR

Фраза «мы принимаем QR» без указания инфраструктуры не сообщает, кто подтверждает платёж, где наступает финальность и кто разбирает спорные операции. QR-код только передаёт платёжные данные без оборудования NFC или ручного ввода реквизитов; расчёт выполняет A2A-перевод, закрытый кошелёк или карточная транзакция.

QR-код в платежах используется в двух сценариях, которые отличаются тем, кто инициирует сканирование. При *merchant-presented mode* (MPM) продавец показывает код, а клиент сканирует его камерой телефона. При *customer-presented mode* (CPM) клиент открывает динамический код в приложении, а продавец считывает его сканером на кассе. Термины MPM и CPM закреплены в спецификациях QR-кодов EMVCo [442, 443]. MPM дешевле в развёртывании, потому что достаточно напечатанной наклейки или экрана на кассе, тогда как CPM быстрее при большом потоке покупателей, но требует от продавца оборудования для считывания. Обе модели встречаются в каждой из трёх схем ниже, но преобладают по-разному.

СБП: QR поверх A2A-перевода

В СБП QR-код ведёт в мгновенный перевод со счёта клиента на счёт ТСП через инфраструктуру НСПК [359]. Перевод идёт по *push*-модели: клиент инициирует и подтверждает списание.

Статический QR — напечатанный бессрочный код с идентификатором ТСП и фиксированной суммой либо полем для её ввода [348]. Клиент сканирует код в приложении своего банка, при необходимости вводит сумму вручную и подтверждает перевод. Такой код подходит малому бизнесу: кассовое ПО не обязательно, достаточно наклейки. Динамический QR кассовая система генерирует под конкретную покупку; он содержит реквизиты получателя, сумму и назначение платежа. Клиент сканирует код, видит предзаполненные данные и подтверждает одним действием, а кассовая система получает вебхук об успешном переводе за несколько секунд [348].

Помимо QR, СБП поддерживает оплату по платёжной ссылке, по NFC и по привязке счёта в приложении SBPay [349, 359]. Все эти каналы ведут к одному и тому же A2A-переводу внутри инфраструктуры НСПК; различается только способ, которым клиент передаёт согласие на списание.

Тарифы C2B-переводов (consumer-to-business — от физического лица в пользу ТСП) в СБП устанавливает Совет директоров Банка России. Максимальная плата, которую банк взимает с ТСП, зависит от MCC (Merchant Category Code, код категории торговой точки) ТСП и составляет от 0 % до 0,7 % от суммы перевода. Для платежей в пользу государства она равна 0 %, для услуг ЖКХ ограничена 0,2 % (не более 10 руб.), для социально значимых категорий (продукты, лекарства, медицина и т. п.) — 0,4 % (не более 1500 руб.), для прочих категорий — 0,7 % (не более 1500 руб.). Межбанковское вознаграждение в пользу банка плательщика ниже: от 0 до 0,5 % [367]. Для сравнения, *interchange* (межбанковская комиссия в карточной сети, см. раздел 2.3) в карточном эквайринге составляет от 1 % до более чем 2 %.

Механизма chargeback в СБП нет, поскольку перевод финален с момента зачисления на счёт получателя. При возврате покупки продавец инициирует обратный перевод через свой банк [348]. Ошибочный перевод не тому получателю также требует согласия получателя на возврат, если иной порядок не установлен законом или решением суда [444]. Эта модель выгоднее продавцу, но перекладывает риск спора на покупателя.

Alipay и WeChat Pay: QR поверх закрытого кошелька

В Alipay и WeChat Pay QR-код ведёт в платёж внутри закрытой системы кошелька. Средства пользователя учитываются на балансе кошелька, который пополняется с банковского счёта или карты; оператор списывает сумму без выхода в межбанковский клиринг.

Здесь используются и MPM, и CPM; документация Alipay+ описывает MPM как основной сценарий для сторонних ТСП. Продавец показывает QR-код, клиент сканирует его в приложении кошелька, оператор списывает средства с баланса клиента и зачисляет их на счёт ТСП [445]. CPM распространён в офлайн-точках с высокой проходимостью: в сетевых магазинах, автоматах и общественном транспорте. Клиент показывает динамический штрихкод из приложения, кассир сканирует его, и оплата проходит без дополнительного подтверждения при сумме ниже порога беспарольного списания (для WeChat Pay — до 1000 юаней за операцию и не более 10 операций в сутки, оператор запрашивает пароль по оценке риска [446], для Alipay+ оператор задаёт порог с учётом валюты расчёта).

Оператор кошелька совмещает роли, которые в карточной сети разделены между эмитентом и эквайером. Он учитывает балансы клиентов и ТСП, проводит расчёт внутри своего реестра и сам определяет правила диспутов. Для клиента путь от пополнения до возврата остаётся внутри одного приложения; продавец интегрируется через API оператора кошелька, минуя эквайера.

Трансграничное расширение устроено как партнёрская сеть, в которой Alipay+ объединяет локальные кошельки (GCash, TrueMoney, KakaoPay и другие), а их пользователи платят в точках, принимающих Alipay, за пределами домашней страны [447]. Продавец подключается к одному контракту с локальным партнёром Alipay+ и получает доступ к пользователям нескольких кошельков [445]. Модель отличается от карточной модели Visa или Mastercard: вместо единого глобального протокола работает федерация кошельков, каждый из которых действует в собственной расчётной инфраструктуре.

Pix: QR, встроенный в национальную платёжную инфраструктуру

Pix как платёжная схема разобран в разделе 20.1. В отличие от FedNow и SCT Inst, где правила схемы заканчиваются на pacs.008, в Pix QR-код — штатный интерфейс системы: формат BR Code задаёт сам BCB [373].

BCB определяет два типа QR. Статический многоразовый код содержит идентификатор получателя и при необходимости сумму. Динамический одноразовый генерируется под конкретную транзакцию с полным набором данных; после исполнения кассовая система получает вебхук. Помимо сканирования, Pix поддерживает Pix Copia e Cola — текстовое представление тех же данных, которое копируется и вставляется в банковское приложение [374]. Этот вариант нужен, когда приложение плательщика и источник кода находятся на одном экране и камерой сканировать нечего.

Комиссия для физических лиц за переводы и платежи через Pix равна нулю по решению регулятора. Для юридических лиц тарифы определяются банком-участником, но ниже карточного эквайринга: в IV квартале 2022 года средняя стоимость приёма Pix для компаний составила 0,33 % против 1,13 % по дебетовым и 2,34 % по кредитным картам [448]. Chargeback как сетевой процедуры в Pix нет: *push*-перевод финален с момента зачисления на счёт получателя, а возврат при фроде выполняется через отдельный механизм схемы MED (см. раздел 20.1).

Сравнение моделей

Один и тот же носитель, QR-код, ведёт к разным расчётным моделям (табл. 38). СБП и Pix проводят платёж через межбанковскую инфраструктуру, управляемую центральным банком, тогда как Alipay или WeChat Pay замыкают расчёт внутри собственного реестра. A2A-модель даёт мгновенный *push*-перевод с ограниченной регулятором комиссией и без chargeback; модель закрытого кошелька даёт оператору контроль над правилами диспутов, ценообразованием и международным расширением.

22.3 Платёжные приложения и кошельки в России

После марта 2022 года в России сложилась собственная структура платёжных приложений и кошельков. Она заменяет часть функций ушедших Apple Pay и Google Pay и опирается на внутрироссийскую инфраструктуру: карты «Мир», СБП и цифровой рубль. Набор поддерживаемых функций и состав банков-партнёров у сервисов 2024–2026 годов меняется от релиза к релизу.

Mir Pay — кошелёк NFC на Android поверх токенизации НСПК (см. раздел 16.3). **SBPay** — мобильное приложение НСПК поверх СБП с оплатой по QR, табличке

Таблица 38 — Сравнение моделей платежей по QR

	СБП	Alipay / WeChat Pay	Pix
Инфраструктура	A2A-перевод (межбанковский)	Закрытый кошелёк	A2A-перевод (межбанковский)
Оператор	НСПК (Банк России)	Ant Group / Tencent	Banco Central do Brasil
Расчёт	Через НСПК, секунды	Внутри реестра оператора	SPI при BCB, секунды
Финальность	Мгновенная (push)	Мгновенная (внутри системы)	Мгновенная (push)
Chargeback	Нет	Правила оператора	Нет
Статический QR	Да	Да	Да
Динамический QR	Да	Да	Да
Основной сценарий QR	MPM	MPM + CPM	MPM
Комиссия C2B	0 %–0,7 % (регулятор)	Устанавливает оператор	0 % (физ. лица)
Трансграничность	Региональный	Федерация кошельков	Региональный

NFC, кнопке и ссылке за счёт привязанного счёта, доступно и на Android, и на iOS (см. раздел 19.3).

SberPay — кошелёк и платёжный сервис ПАО «Сбербанк», который поддерживает оплату на сайтах партнёров через кнопку SberPay и в подключённых офлайн-точках. Для держателей карт «Мир» Сбербанка также реализованы сценарии оплаты по QR-коду и NFC через мобильное приложение банка [449].

T-Pay, бывший «Tinkoff Pay», — платёжный сервис АО «ТБанк», бывшего Тинькофф Банка. Сервис работает на сайтах партнёров и в офлайн-точках, в том числе с использованием NFC на Android, а сценарии оплаты опираются на карты и счета клиентов банка [450].

AlfaPay — платёжный сервис АО «Альфа-Банк» для карт банка ПС Мир. На Android — NFC через HCE в приложении банка с пулом одноразовых ключей: банк заявляет до 10 транзакций между сессиями онлайн (LUK-пул разобран в разделе 8.3) [451]. На iPhone — BLE на терминалах Сбера с «Вжухом» через приложение «Альфото» [452]. Для iPhone и телефонов без NFC банк выпускает стикер — NFC-наклейку как отдельную дебетовую карту ПС Мир. Для ТСП AlfaPay — кнопка в интернет-эквайринге Альфа-Банка: REST-вызов на платёжный шлюз открывает приложение банка по *deep-link*, и покупатель подтверждает оплату в приложении банка, не вводя реквизиты карты на сайте ТСП [156].

Yandex Pay — платёжный сервис ООО «Яндекс.Пэй», встраиваемый в форму оплаты партнёрских сайтов и ориентированный на оплату ранее сохранёнными картами без повторного ввода реквизитов (*frictionless*). С 2024 года он интегрирован с сервисом рассрочки «Сплит» (раздел 23.4) [453, 454].

ЮKassa — платёжный сервис ООО НКО «ЮМани», дочерней структуры Сбербанка. Работает как PSP для бизнеса с приёмом карт, платежей СБП и BNPL-сценариев. Часть инфраструктуры общая с клиентским кошельком **ЮMoney**, который остаётся электронным средством платежа для розничных пользователей и наследует Яндекс.Деньги [455, 456].

Биоэквайринг и оплата по лицу — сценарий, который НСПК и Банк России развивают на основе Единой биометрической системы (ЕБС). Покупатель оплачивает

покупку, подтверждая личность биометрией на терминале, без карты и телефона [457, 458]. К 2025 году платформа НСПК объединяет несколько биоэквайеров и эмитентов, оплата работает в кассах самообслуживания X5 («Перекрёсток», «Пятёрочка»); в метро Казани в 2024 году стартовал пилот оплаты проезда по биометрии через СБП [459]. Московский Face Pay — отдельный сервис метрополитена с привязкой карты в приложении «Метро Москвы» [460]. Оборот канала на порядки ниже, чем у карт и СБП.

Для ТСП в России в 2024–2026 годах базовый набор — приём карт «Мир» через эквайринг, СБП по QR или кнопке, один или несколько кошельков (SberPay, T-Pay, Yandex Pay) и BNPL для подходящих категорий; на отдельных типах ТСП добавляется биоэквайринг.

22.4 Структура способов оплаты в России и СНГ

Россия сочетает массовую карточную инфраструктуру и растущие альтернативы. Банк России указывает, что карты остаются самым популярным средством безналичной оплаты, а платежи по QR-коду в 2024 году достигли 4,1 трлн рублей при порядка 22 млрд рублей оплат по биометрии [459]. В Казахстане национальная статистика отдельно выделяет крупный поток безналичных платежей по QR наряду с карточными операциями [461]. Узбекистан опирается на две национальные карточные системы — HUMO и UzCard [328, 462]. Армения сохраняет собственную карточную инфраструктуру ArCa [327].

При локализации продукта в регионе структуру способов оплаты нужно оценивать отдельно по каждой стране: российский набор нельзя переносить на Казахстан, а армянскую модель на Узбекистан без проверки локальной инфраструктуры, роли QR и регуляторных требований.

ПРАКТИКА

При локализации в новой стране СНГ проверьте распределение трафика по BIN, наличие массового локального A2A-метода и требования к обязательному приёму локальных карт. Они определяют экономику приёма и конверсию сильнее остальных.

Правовой статус локальной карточной системы задают требования: обязательной маршрутизации всех внутренних карточных операций через национальный коммутатор (как в России — через НСПК), обязательного приёма национальных карт всеми ТСП определённого размера и отдельных тарифов на C2B-переводы по QR, утверждаемых регулятором. В Казахстане локальный коммутатор — ISPC АО «Национальная платёжная корпорация Национального банка Республики Казахстан»; он работает с 30 июня 2022 года и обрабатывает внутриказахстанские карточные операции [463]. Операторы узбекских систем — Национальный межбанковский процессинговый центр (HUMO) и Единый общереспубликанский процессинговый центр (UzCard) [328, 462]. Правила локальной маршрутизации каждый регулятор задаёт для своей страны: Национальный банк Казахстана и Центральный банк Узбекистана. В Армении ArCa — единый процессинг для собственного бренда и для Visa, Mastercard, American Express и JCB; банки-участники эмитируют ArCa параллельно с международными системами [327]. Карты «Мир» банки-участники ArCa не обслуживают с 30.03.2024 [464]. Доля карт ArCa в эмиссии (около 16 % на 01.10.2025) ниже доли карт «Мир» в России (на 01.10.2024 около 62 % эмиссии и около 64 % стоимости внутрироссийских операций по картам по данным Банка России [465]).

22.5 Почему карты остаются основным инструментом

Карты сохраняют центральное место в потребительских платежах благодаря сетевым эффектам, международности, защите покупателя и инфраструктурной инерции.

Сетевые эффекты: глобальные карточные сети уже выстроили массовую эмиссию, приём и привычный пользовательский сценарий. Продавец, который принимает карты, доступен большинству покупателей, а новый метод должен одновременно получить поддержку и у эквайеров, и у эмитентов.

Международность: карта, выпущенная в одной стране, работает во множестве других по единому протоколу, тогда как локальные A2A-системы вроде СБП, Pix и UPI не взаимозаменяемы.

Защита покупателя через chargeback: механизм, который A2A-системы не воспроизводят без изменения самой идеи финальности. Покупатель, оплативший картой незнакомому продавцу, имеет формальный механизм возврата. Покупатель, оплативший через A2A, может требовать возврат по договору или специальным правилам схемы, но chargeback уровня карточной системы здесь нет.

Инфраструктурная инерция: мировая сеть POS-терминалов (Point of Sale, кассовый терминал в физической точке обслуживания) уже выстроена под карточные сети. Переоснащение или добавление нового метода окупается при массовом спросе, а массовый спрос не возникает, пока продавцы не видят достаточного потока покупателей. Этот круг разрывает регулирование или встраивание в уже массовый кошелёк.

Альтернативные методы выигрывают в нишах: A2A снижает комиссию, наличные сценарии обслуживают клиентов без банковского счёта, CBDC добавляет условные платежи, BNPL даёт рассрочку, а криптоактивы поддерживают программируемые международные сценарии. Глобального охвата карт они не достигают и работают рядом с картами там, где их преимущество перевешивает универсальность карточного приёма.

Выбор метода привязан к рынку и чеку. Внутри России при среднем чеке ниже 100 000 руб. СБП даёт комиссию от 0 до 0,7 % в зависимости от категории ТСП и мгновенное зачисление, а карты остаются резервным методом для клиентов без мобильного банка. На международных рынках основной метод — карты, а A2A-системы других стран, например Pix или UPI в Индии, требуют отдельной интеграции на каждый рынок. При среднем чеке 10 000–150 000 руб. и важной для продавца конверсии BNPL повышает конверсию за счёт рассрочки, но добавляет кредитный риск на стороне провайдера и задержку в расчёте. Для покупателей без банковского счёта, например в части стран Азии и Африки, нужны наличные через агентскую сеть или мобильные деньги. Карты остаются базовым методом, а остальные добавляются там, где комиссия, рассрочка, доступ без счёта или финальность дают измеримый выигрыш.

23 BNPL

Со стороны клиента BNPL (Buy Now Pay Later) выглядит как рассрочка: клиент выбрал товар, разбил оплату на части и сразу забрал покупку. В момент оплаты провайдер BNPL в реальном времени оценивает клиента и принимает кредитное решение — одобряет рассрочку с фиксированным графиком платежей или отказывает. При одобрении провайдер сразу перечисляет ТСП полную сумму покупки. Клиент затем возвращает деньги провайдеру равными частями по графику.

ТСП получает выручку так же быстро, как при обычном эквайринге, но платит за это комиссию провайдеру BNPL. В этой модели кредитный риск несёт провайдер: если клиент не выплатит оставшиеся части, ТСП денег не потеряет. В альтернативной модели «BNPL на карте» (см. раздел 23.2) риск несёт эмитент или участвующий кредитор. Провайдер зарабатывает на комиссии ТСП и иногда на пенях за просрочку, а ТСП получает рост конверсии и увеличение среднего чека за счёт меньшего разового платежа для покупателя.

23.1 BNPL в роли PSP

Провайдер BNPL работает как отдельный PSP (Payment Service Provider, платёжный провайдер). ТСП заключает с ним *merchant agreement* — договор о приёме платежей конкретным методом, фиксирующий комиссии, обязательства по отгрузке и порядок возвратов, — встраивает SDK или редирект на форму оплаты провайдера и обрабатывает обратные вызовы с результатом кредитного решения.

Клиент на странице оплаты выбирает провайдера BNPL, и провайдер показывает условия: количество платежей, даты, сумму каждого платежа. Кредитное решение опирается на скоринг — алгоритмическую оценку кредитоспособности заявителя по внутренней модели провайдера. Провайдер рассчитывается с ТСП банковским переводом или внутренним зачислением за вычетом комиссии; карточной авторизации между провайдером и ТСП нет. ТСП видит одну транзакцию на полную сумму и отгружает товар. Когда провайдер собирает взносы с карты клиента, первый платёж маркируется как CIT, последующие — как MIT по рассрочке (*installment* MIT); цепочку связывает NTID (Visa) или Trace ID (Mastercard). Альтернатива — списания не с карты, а напрямую с банковского счёта клиента: например, Affirm в США по умолчанию собирает взносы через ACH (Automated Clearing House, межбанковская сеть пакетных переводов).

Интеграция повторяет подключение обычного PSP: API для создания заказа, серверные уведомления (вебхуки) об изменении статуса, API для возвратов. Споры регулирует договор с провайдером: карточная сеть в оплате не участвует, и карточного chargeback между ТСП и клиентом нет.

По этой модели работают Klarna, Affirm, Tabby, а также все основные сервисы BNPL в России.

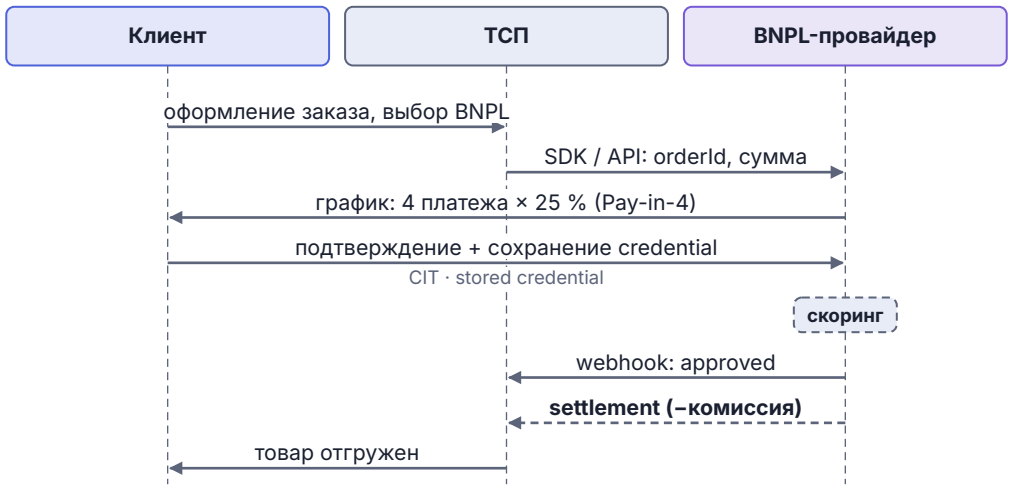


Рис. 55 — Покупка: ТСП интегрирует BNPL как обычный платёжный метод [466, 467].

Рис. 56 — Сбор взносов с клиента: отдельная цепочка, MoR — BNPL [468].

23.2 BNPL на карте

Второй вариант встраивает рассрочку в карточную инфраструктуру: клиент расплачивается картой, а разбиение на части происходит на стороне эмитента или отдельного кредитора внутри карточной сети, так что ТСП может вообще не знать, что покупка оплачена в рассрочку.

Visa Installments (Visa Installment Solutions, VIS) строится на API Visa. ТСП или эквайрер через API запрашивает планы рассрочки, доступные по карте, и подтверждает план, выбранный клиентом; авторизация проходит на полную сумму. Эмитент через свои API конвертирует исходную транзакцию в план рассрочки и сам выставляет платежи по графику. Кредитный риск несёт эмитент; он решает, для каких карт и каких покупок доступна рассрочка. ТСП должно поддерживать Installments API у своего процессора, а эмитент — активировать программу для своих карт. Рассрочка появляется у клиента только при обоих условиях [469].

В Mastercard Installments участвующий кредитор — банк или финтех, выступающий провайдером BNPL, заключивший договор с Mastercard, — выпускает одноразовый виртуальный номер карты (*single-use virtual card number*, действительный на одну конкретную покупку) на отдельном BIN (Bank Identification Number, банковский идентификационный префикс карты; см. гл. 3). Клиент расплачивается этим номером у ТСП, ТСП получает полную сумму сразу как обычную карточную транзакцию,

а кредитор самостоятельно собирает взносы с клиента [470]. ТСП не подключает отдельный API и не активирует программу, а распознать такую транзакцию может по выделенному BIN.

BNPL в роли PSP требует отдельного *merchant agreement* с провайдером: только после его заключения ТСП добавит провайдера как метод оплаты. BNPL на карте требует поддержки Installments API у процессора для Visa или участвующего кредитора в сети для Mastercard, но не требует от ТСП отдельной интеграции с провайдером BNPL.

Visa Core Rules обязывают эквайреров поддерживать VIS в Канаде, Великобритании, Азербайджане, Иордании и ряде стран Персидского залива, а с 2026–2027 годов — на Филиппинах, во Вьетнаме, в Гонконге и Сингапуре [13]. Такой же сдвиг происходит у эмитентов: вместо запуска отдельного BNPL-продукта банки активируют рассрочку как дополнительную возможность существующих карт, выбирая категории ТСП и диапазоны сумм. Сетевая рассрочка ослабляет позицию независимых провайдеров: ТСП проще включить её на существующем процессоре, чем подключать новую PSP-интеграцию.

23.3 Глобальный рынок BNPL

Эпоха независимых BNPL-провайдеров без банковской лицензии заканчивается. Apple Pay Later запустился в марте 2023 года при участии Goldman Sachs; в июне 2024 года Apple закрыл сервис после 15 месяцев работы [471]. В iOS 18 Apple заменил собственный BNPL интеграцией сторонних провайдеров (Klarna, Affirm, банковские программы) в экран оплаты Apple Pay [472]. Даже игрок с миллиардной пользовательской базой и контролем над устройством на уровне ОС не удержал BNPL как самостоятельный продукт: модель работает только в связке с банковской или кредитной инфраструктурой партнёра.

Klarna прошла противоположный путь. Запущенная в 2005 году в Стокгольме, к 2021 году компания достигла оценки $45,6 млрд, упала до $6,7 млрд в июле 2022 года [473] на коррекции BNPL-сектора и 10 сентября 2025 года провела IPO на NYSE (тикер KLAR) по цене $40 за акцию; в первый день торгов акция закрылась на $45,82 ($+15\,\%$) [474]. Метрики из проспекта: 111 млн активных потребителей, 790 тыс. ТСП в 26 странах, GMV $112 млрд за 12 месяцев на 30 июня 2025 года. Глобальный рынок BNPL по прогнозам — около $23 млрд выручки (не оборота) в 2025 году с ожидаемым ростом до $90 млрд к 2035 году [475]. По оценке отчёта CFPB за декабрь 2025 года, шесть крупных провайдеров США (Affirm, Afterpay, Klarna, PayPal, Sezzle, Zip) в 2023 году занимали около 40 % рынка кредитования в точке продажи [476].

Игроки, сохранившие масштаб, имеют либо банковскую лицензию (Klarna — банк с 2017 года в Швеции, Affirm работает через банков-партнёров, а в Канаде вышел на рынок приобретением BNPL-провайдера PayBright [477]), либо входят в платёжную группу с собственным банком (PayPal с банковской лицензией в Люксембурге [478], Afterpay внутри Block с промышленным банком Square Financial Services в США [479]). Финтех без собственного кредитного бизнеса и поддержки банковской группы платит больше за капитал и комплаенс.

Региональные рынки развиваются отдельно от глобальных лидеров. На Ближнем Востоке и в Северной Африке доминирует Tabby (основана в 2019 году в Дубае, штаб-квартира перенесена в Эр-Рияд в 2023 году при подготовке к листингу на Tadawul; BNPL-лицензия Saudi Central Bank, SVF-лицензия Central Bank of the UAE; основные

рынки — Саудовская Аравия и ОАЭ) [480, 481]. В Юго-Восточной Азии конкурируют Atome (Сингапур, дочерняя компания финансовой группы Advance Intelligence) и Akulaku в Индонезии. В Латинской Америке выделяются Kueski в Мексике и Nubank через Nu Pay в Бразилии, где BNPL встраивается в существующую банковскую инфраструктуру Pix. У всех трёх регионов свой путь регулирования, и глобальные лидеры в них почти не работают: банковская лицензия и локальная кредитная инфраструктура остаются конкурентным барьером.

23.4 BNPL в России

Российский рынок BNPL сформировался по модели «BNPL в роли PSP». В отличие от западных аналогов, все крупные сервисы принадлежат банкам или финансовым группам с банковской лицензией и кредитной инфраструктурой. Сервисы принимают карты любых банков, включая чужие; доступ конкретного плательщика ограничивает собственный скоринг сервиса.

Первый сервис BNPL в России — «Долями» от Т-Банка, запущен в апреле 2021 года [482]. ТСП интегрирует его как внешний PSP: отдельный договор, API или плагин для CMS, отдельный поток уведомлений [483]. «Подели» устроен аналогично; оператор сервиса — ООО «А-Четыре Технологии», 100 %-дочернее общество АО «Альфа-Банк»; интеграция идёт через API, плагины для CMS или платёжных партнёров [484, 485]. Сбер запустил «Плати частями» как отдельный сервис BNPL; оператор — ООО «Центр новых финансовых сервисов», ЦНФС, 100 %-дочернее общество Сбербанка. ТСП подключает его как самостоятельный платёжный способ у процессора; с интеграцией SberPay он не связан [486].

Исключение из этой схемы — «Сплит» от Яндекса: сервис работает внутри Yandex Pay SDK, и ТСП подключает его через единую интеграцию с Yandex Pay, без отдельного договора BNPL [454].

К 2026 году в реестр ОСР Банка России вошли операторы всех перечисленных сервисов плюс операторы рассрочек, встроенных в маркетплейс Wildberries, и отдельные микрокредитные компании [487].

Скоринг в реальном времени

Кредитное решение по BNPL принимается за сотни миллисекунд на этапе подтверждения покупки. У российских сервисов скоринговая модель опирается на собственные данные банковской группы — историю карточных операций, остатки на счетах, ранее выданные кредиты — плюс реквизиты заказа (категория ТСП, сумма, доставка).

Главное ограничение задаёт внешний API бюро кредитных историй: запрос в Объединённое кредитное бюро или НБКИ превышает SLA страницы оплаты. Поэтому сверка с БКИ идёт асинхронно: первое одобрение строится на данных группы, синхронизация с бюро выполняется позже. Независимый провайдер без собственной банковской группы либо принимает риск без полного кредитного отчёта, либо увеличивает время подтверждения до неприемлемых для конверсии значений.

23.5 Регулирование

До 2024 года BNPL в большинстве юрисдикций попадал в пробел регулирования. Формально кредитом BNPL не считается — процентов для клиента нет; экономически это кредитный продукт.

В России этот пробел закрыт Федеральным законом от 31.07.2025 № 283-ФЗ «О деятельности по предоставлению сервиса рассрочки»[1] [488]. Закон вводит понятие «оператор сервиса рассрочки», ОСР, и устанавливает для него регистрацию в реестре Банка России [489], требования к капиталу, обязательное изложение цены договора и графика платежей в табличной форме до заключения договора, ограничение максимального срока и запрет на взимание вознаграждения с клиента. Если задолженность клиента перед оператором и аффилированными с ним лицами вместе с новой покупкой превышает 50 тыс. рублей, договор заключается только при передаче данных в бюро кредитных историй (часть 5 статьи 13). Для работы после вступления в силу основных положений закона провайдеру нужен статус ОСР.

На 1 апреля 2026 года Банк России включил в реестр 14 юридических лиц [487]. Из них только один банк — ПАО «Совкомбанк»; остальные 13 позиций — микрофинансовые организации и технологические компании, включая операторов, связанных с маркетплейсами и финансовыми группами (Wildberries, Яндекс, Альфа-Банк, Т-Банк, Сбер). Подзаконные акты, определяющие ведение реестра, состав сведений и перечень документов, утверждены Указаниями Банка России от 12.01.2026 № 7274-У «О ведении реестра ОСР» и № 7276-У «О порядке внесения сведений в реестр ОСР»[2] [490, 491].

Регулирование BNPL за пределами РФ

С 2024 по 2026 год регуляторы синхронно закрывают пробел в нескольких крупных юрисдикциях. Это меняет экономику провайдера BNPL, работающего в нескольких странах.

В ЕС BNPL включён в обновлённую Consumer Credit Directive [492]; страны-члены обязаны были принять национальные акты до 20 ноября 2025 года и применяют их с 20 ноября 2026 года. Директива требует обязательной оценки кредитоспособности, единого стандарта раскрытия условий — Standard European Consumer Credit Information — и права клиента на отказ в течение 14 дней без причины. До директивы BNPL в большинстве стран ЕС подпадал под исключение для рассрочки без процентов из прежней CCD 2008 года.

В США попытка закрыть пробел административным путём провалилась. CFPB интерпретирующим правилом от 22 мая 2024 года признал BNPL-продукты с разбиением на четыре части кредитными картами по Regulation Z и распространил на провайдеров требования о раскрытии условий, разрешении споров и возврате [493]. Правило продержалось меньше года: 12 мая 2025 года CFPB отозвал его вместе с другими разъяснениями, выпущенными с 2011 года [494]. Пробел снова открыт. Отчёт CFPB за декабрь 2025 года описывает рынок, а не применение Regulation Z: рост объёмов и доля списаний (*charge-off*) у шести крупнейших провайдеров *pay-in-4* [476].

Великобритания пошла третьим путём. HM Treasury опубликовал правительственный ответ и план передачи BNPL под FCA в 2025 году; FCA получит надзорные

[1] В силе с 01.04.2026, кроме статьи 11 об отчётности ОСР перед Банком России, которая вступает в силу с 01.01.2027.

[2] Оба в силе с 01.05.2026.

полномочия: обязательная оценка платёжеспособности, информационные требования, порядок обработки споров через FCA и Financial Ombudsman Service [495]. FCA регулирует BNPL с 15 июля 2026 года; провайдеры, работавшие до этой даты, продолжают деятельность по временным разрешениям (*Temporary Permissions Regime*) [496].

Австралия завершила процесс первой: Treasury Laws Amendment Act от декабря 2024 года расширил National Consumer Credit Protection Act 2009 на BNPL, признав продукты Low Cost Credit Contracts; с 10 июня 2025 года провайдеры обязаны иметь Australian Credit Licence и соблюдать стандарт ответственного кредитования [497].

Регуляторный пробел, в котором BNPL вырос до глобального рынка, за два года закрылся в ЕС, Великобритании и Австралии, но в США открылся снова. Стоимость комплаенса — отчётность, надзор, порядок споров, лицензирование — растёт быстрее, чем удельный платёж клиента; это даёт преимущество крупным провайдерам с действующими лицензиями. Российский реестр ОСР, где крупнейшие сервисы принадлежат маркетплейсам и банковским группам, показывает ту же закономерность.

Stacking и прозрачность задолженности

Stacking — одновременное открытие нескольких рассрочек у разных провайдеров на одного клиента, при котором ни один провайдер не видит совокупную задолженность. До передачи данных в бюро кредитных историй каждый провайдер принимает решение по собственной скоринговой модели; суммарная задолженность клиента превышает уровень, допустимый для любой отдельной модели.

Российский ответ — 283-ФЗ (часть 5 статьи 13): если задолженность клиента перед оператором и его аффилированными лицами превышает 50 тыс. руб., оператор передаёт данные в БКИ, и их видят остальные провайдеры. Отчёт CFPB за декабрь 2025 года признаёт, что провайдер не всегда знает о займах клиента у других провайдеров [476]. Без общей отчётности рынок повторяет траекторию субпрайм-ипотеки в миниатюре: каждый игрок видит свою долю риска, никто не видит совокупную.

Возврат и спор

В BNPL-модели PSP спор между клиентом и ТСП не проходит через карточную сеть: правил *chargeback* нет, арбитра в лице платёжной системы — тоже. Споры разрешаются по договору между провайдером, ТСП и клиентом. Если клиент возвращает товар, провайдер останавливает оставшиеся транши и возвращает уже уплаченные; жалоба на качество рассматривается по договорной процедуре провайдера, а не по правилам Visa/Mastercard для диспутов (см. гл. 32).

Для ТСП это меняет повседневную работу поддержки: команда сопровождает спор параллельно в интерфейсе провайдера BNPL и в интерфейсе карточных диспутов; данные не синхронизированы. Сближение регулирования в 2024–2026 годах вводит формальный порядок спора: право на отказ в течение 14 дней в ЕС, надзор FCA в Великобритании, ответственное кредитование в Австралии; в США правило CFPB о применении Regulation Z отозвано. У ТСП появляется обязанность поддерживать два процесса одновременно, и стоимость интеграции с BNPL-провайдером растёт.

ПРАКТИКА

При выборе провайдера BNPL проверяйте долю одобрений на своей аудитории и регуляторный статус: для России — наличие в реестре ОСР Банка России.

24 Цифровой рубль

Цифровой рубль — третья форма денег наряду с наличными и безналичными (см. раздел 1.1): Банк России эмитирует его напрямую как цифровую форму национальной валюты [4, 369] и ведёт отдельный реестр обязательств на своей платформе. Это розничная CBDC (*central bank digital currency*, цифровая валюта центрального банка): платформа обслуживает переводы между гражданами, ТСП и бюджетными распорядителями, а не расчёты между финансовыми организациями, как оптовая (*wholesale*) CBDC [498]. Сравнение с СБП — в разделе 19.11.

24.1 Двухуровневая архитектура

Банк России эмитирует цифровой рубль и управляет платформой; участники платформы (банки и Федеральное казначейство) открывают клиентам кошельки и исполняют поручения. Граждане и ТСП получают доступ к кошельку через мобильное приложение банка; главные распорядители бюджетных средств (ГРБС; ст. 158 Бюджетного кодекса РФ [499]) используют интерфейсы Казначейства [369]. Требования к защите информации для участников платформы установлены Положением Банка России от 07.12.2023 № 833-П «О защите информации для участников платформы цифрового рубля» [500].

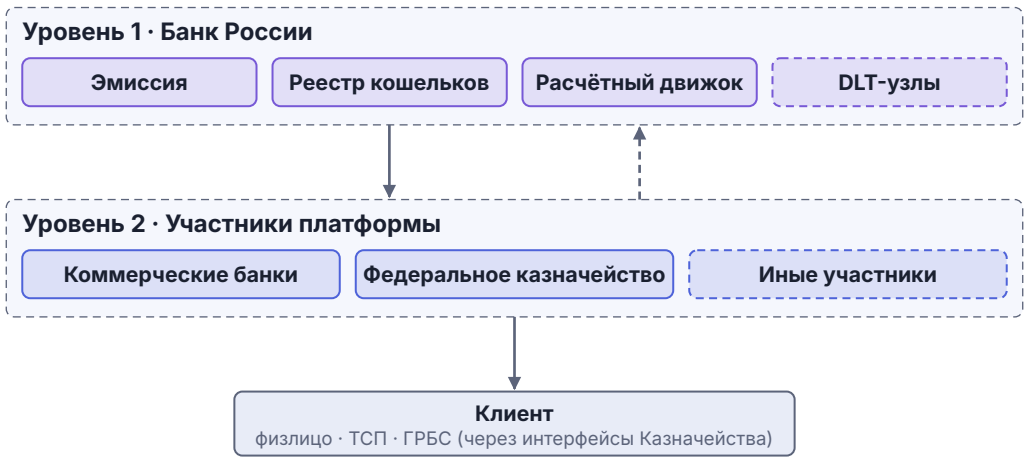


Рис. 57 — Двухуровневая архитектура платформы цифрового рубля.

Платформа Банка России включает (рис. 57) эмиссию цифрового рубля, единый реестр кошельков и операций, централизованный расчётный движок и узлы DLT (*distributed ledger technology*, технология распределённого реестра; формальное определение — в разделе 24.3), реплицирующие реестр обязательств между узлами Банка России. На втором уровне участники платформы обслуживают клиентов: банки — розничных и корпоративных, Федеральное казначейство ведёт бюджетные кошельки и целевые выплаты с казначейским сопровождением; круг может расширяться по решению Банка России. До передачи распоряжения на платформу участник как лицензированная организация идентифицирует клиента, проводит проверки по ПОД/ФТ (противодействие отмыванию доходов и финансированию терроризма),

оценивает риск фрода, проверяет лимиты и реквизиты. На платформу поступает подписанное и проверенное распоряжение, готовое к расчёту.

От безналичного рубля цифровой отличается природой обязательства. Безналичный рубль — обязательство коммерческого банка перед клиентом; цифровой рубль — прямое обязательство Банка России. Для клиента исчезает кредитный риск банка; для банков появляется риск оттока депозитной базы [369].

24.2 Роль банка-посредника

Платформа Банка России хранит кошелёк и ведёт расчёт; клиентскую сторону регулятор оставил банкам. Банк ведёт клиентскую часть: открывает человеку доступ к кошельку, авторизует перевод, связывает кошелёк с расчётным счётом и обеспечивает приём на кассе (рис. 58).

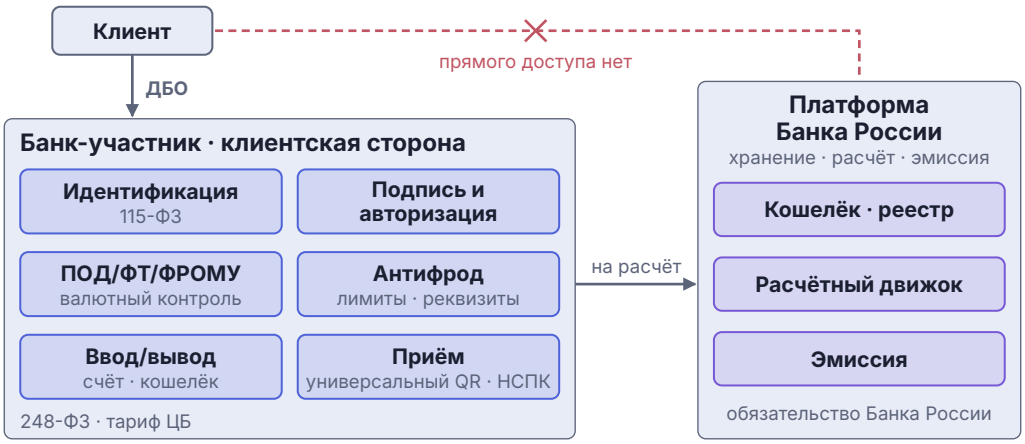


Рис. 58 — Разделение функций в цифровом рубле: платформа Банка России хранит кошелёк и ведёт расчёт, банк обслуживает клиента.

Хранение и доступ разнесены: кошелёк учитывается на платформе, а доступ к нему клиент получает только через дистанционное банковское обслуживание (ДБО) своего банка. Банк России называет «привычные для них каналы взаимодействия — мобильные приложения и системы дистанционного банковского обслуживания» [501]; собственного розничного интерфейса у регулятора нет.

До отправки распоряжения на платформу банк выполняет клиентские проверки: идентифицирует клиента по 115-ФЗ, проводит проверки ПОД/ФТ/ФРОМУ и валютного контроля, оценивает риск фрода, сверяет лимиты и реквизиты. Подпись и авторизация перевода тоже происходят в ДБО; на платформу приходит уже проверенное распоряжение (см. раздел 24.1).

Обмен между безналичным счётом и кошельком проводит банк: клиент пополняет кошелёк с расчётного счёта и выводит средства обратно через банк, где открыт счёт. Безналичный и цифровой рубль — разные формы денег, поэтому переход между ними остаётся банковской операцией.

Оплата на кассе проходит через универсальный QR-код НСПК (см. раздел 19.5): один код на кассе предлагает покупателю и СБП, и карту, и цифровой рубль. Обеспечить работу с ним обязаны все банки, а НСПК предоставляет банкам сам код бесплатно [362].

Расчёты цифровым рублём банк обязан обеспечить поэтапно. Федеральный закон от 23.07.2025 № 248-ФЗ «О поэтапном внедрении цифрового рубля»[1] [361] задаёт сроки по категориям: системно значимые банки и банки, включённые в реестр кредитных организаций, признанных Банком России значимыми на рынке платёжных услуг, — с 1 сентября 2026 года, банки с универсальной лицензией — с 1 сентября 2027 года, остальные — с 1 сентября 2028 года [362, 502]. За информационное и технологическое взаимодействие клиента с платформой оператор платформы платит участникам вознаграждение [503]; депозитный отток (см. раздел 24.1) остаётся риском банка, и вознаграждение его не компенсирует.

24.3 Выбор между приватным и публичным блокчейном

Распределённый реестр (*distributed ledger*, DLT) — база данных, копии которой одновременно хранятся у нескольких независимых участников. При записи новой операции участники подтверждают её корректность и обновляют свои копии. *Блокчейн* — частный вид распределённого реестра, где записи объединены в цепочку блоков, а каждый блок ссылается на предыдущий через криптографический хеш; изменение старой записи задним числом требует переподписания всей цепочки. *Валидатор* — участник с правом подтверждать новые записи; механизм, которым валидаторы приходят к согласию, называется *консенсусом*.

Proof-of-work (PoW, доказательство выполненной работы) заставляет валидаторов соревноваться в подборе хеша, удовлетворяющего условию; победитель тратит реальное электричество и машинное время, и именно эти затраты делают подделку невыгодной. Так работает Bitcoin. *Proof-of-stake* (PoS, доказательство доли владения) отдаёт право подписать блок участнику, заблокировавшему в залог крупную сумму криптовалюты; за некорректное поведение залог конфискуется (механизм *slashing*), и по такой схеме с 2022 года работает Ethereum. *Proof-of-authority* (PoA, доказательство полномочия) допускает к подписи блоков только тех участников, которым оператор сети заранее выдал такие полномочия; ни работы, ни залога не требуется, доверие основано на репутации и договоре. PoA часто выбирают для приватных корпоративных и банковских сетей, включая платформы CBDC.

Публичный (*permissionless*) реестр допускает валидатором любого участника, набравшего ресурс по правилам PoW или PoS. В *приватном* (*permissioned*) реестре список валидаторов утверждён заранее (PoA или его варианты), а вход возможен только по разрешению оператора сети. В публичной сети любой пользователь видит все транзакции; в приватной видимость определяется правилами оператора.

В консультативной фазе Банк России сравнивал варианты: централизованную базу данных под полным контролем регулятора, децентрализованную сеть на базе распределённого реестра и гибридную архитектуру [504]. В выбранной гибридной модели валидирующие узлы распределённого реестра размещены на инфраструктуре Банка России, банки подключаются к платформе через API, а окончательный расчёт по операциям выполняют централизованные компоненты Банка России [504]. Действующие стандарты платформы 2026 года описывают подключение банков через узлы доступа транспортного шлюза Банка России и распределённый реестр не упоминают [505, 506]. Полностью централизованный вариант проигрывал в устойчивости (одна точка отказа), полностью децентрализованный — в производительности: DLT медленнее обычной СУБД.

[1] В силе с 01.09.2026.

Ни один центральный банк, экспериментирующий с CBDC, не выбрал публичный вариант: BIS (*Bank for International Settlements*, Банк международных расчётов в Базеле), проанализировав все доступные на 2020 год отчёты регуляторов, не нашёл ни одного [498].

Юридическая финальность платежа. В PoW транзакция считается «достаточно надёжной» только после добавления нескольких последующих блоков; до этого сохраняется риск отмены через перестроение цепочки. PoS снижает этот риск, но не устраняет его: при разделении сети возможны откаты. Платёжное право требует, чтобы в момент списания деньги были переведены *окончательно*, без вероятностных оговорок. PoA с доверенным списком валидаторов даёт такую финальность по построению: подпись утверждённого узла сразу фиксирует запись.

Пропускная способность. Bitcoin (PoW) обрабатывает порядка семи операций в секунду на всю сеть, Ethereum после перехода на PoS на уровне основной цепи (*mainnet*) — несколько десятков: суточный рекорд апреля 2026 года — около 3,6 млн транзакций, в среднем около 40 в секунду [507]; розничная платёжная инфраструктура страны должна выдерживать тысячи в секунду круглосуточно. В открытом консенсусе чем больше валидаторов и чем меньше у оператора инструментов отбора, тем дороже согласование каждой записи. PoA с небольшим утверждённым кругом участников устраняет это ограничение, потому что согласование сводится к подписям заранее известных сторон.

Эмиссия. Цифровой рубль — обязательство Банка России, поэтому выпускать его вправе только Банк России. На публичной сети любой валидатор, собравший достаточный ресурс по правилам PoW или PoS, может влиять на правила выпуска, что для национальной валюты неприемлемо.

Поэтому в архитектуре цифрового рубля DLT остаётся способом надёжно реплицировать реестр между утверждёнными узлами и зафиксировать историю операций криптографически. Слово «блокчейн» в этом контексте означает закрытую сеть с подписями участников из заранее известного списка. Та же модель применяется в китайском e-CNY (*Digital Currency Electronic Payment*, DC/EP — розничная CBDC Народного банка Китая с двухуровневой архитектурой и гибридной платформой из централизованных и распределённых компонентов под централизованным управлением) [508]. Технологически разница между таким реестром и хорошо защищённой банковской базой данных невелика: отличаются только репликация и формат подписи, а участие закрыто в обоих случаях.

Производительность цифрового рубля задаёт процессинг: окончательный расчёт по операциям выполняют централизованные компоненты Банка России, а валидирующие узлы DLT ведут проверяемый журнал событий [504]. Открытого согласования, которое ограничивает Bitcoin семью операциями в секунду, здесь нет: запись подтверждает утверждённый узел, а расчёт выполняется по логике обычной СУБД с горизонтальным масштабированием. Целевые TPS (*transactions per second*, операций в секунду) Банк России не публикует.

Клиентские проверки участник платформы выполняет до передачи распоряжения (раздел 24.2), и в ядро поступает подписанное распоряжение — типовая операция «списать с одного кошелька, зачислить на другой» в транзакции с гарантиями ACID (*atomicity, consistency, isolation, durability* — атомарность, согласованность, изолированность, устойчивость; классический набор свойств транзакций реляционной СУБД). Такую нагрузку уже обрабатывают ядро НСПК и инфраструктура СБП: тысячи операций в секунду на всю платёжную систему страны.

В пилоте с 15 августа 2023 года по 1 декабря 2024 года выполнено более 38 тыс. переводов между физическими лицами [465]. В сентябре 2025 года Федеральное

казначейство провело первые платежи из федерального бюджета в цифровых рублях [509], а в Татарстане, Чувашии и Ростовской области в 2025 году завершено тестирование бюджетных выплат со смарт-контрактами [510] (рис. 57). Тот же 248-ФЗ устанавливает встречную обязанность ТСП принимать цифровой рубль в три волны (банковская сторона — в разделе 24.2): с 1 сентября 2026 — продавцы с выручкой свыше 120 млн руб./год, с 1 сентября 2027 — свыше 30 млн руб./год (в обеих волнах — клиенты банков соответствующей волны на 1 января 2026 года), с 1 сентября 2028 — остальные продавцы с выручкой свыше 20 млн руб./год, кроме торговых объектов с выручкой менее 5 млн руб./год и мест без мобильной связи и интернета [361]. Розничный безналичный поток в III квартале 2025 года составил около 2,8 тыс. операций в секунду на всю страну [511]; до этого уровня платформе цифрового рубля остаются три года на нагрузочное тестирование и рост инфраструктуры.

24.4 Смарт-контракты

Смарт-контракт в контексте цифрового рубля — программный сценарий, опубликованный на платформе Банка России и автоматически исполняющий перевод цифровых рублей при наступлении заданных условий (дата, событие, подтверждение от стороны сделки) без вмешательства оператора [369]. Возможность встроить условия исполнения непосредственно в единицу денег называют *программируемыми деньгами* (*programmable money*); у безналичного рубля такого свойства нет [498].

Простые смарт-контракты уже работают в пилоте и автоматически переводят цифровые рубли в заданные дату и время. К 1 июня 2026 года исполнено 37,4 тыс. таких контрактов [510]; типовые сценарии — автоплатёж за жилищно-коммунальные услуги, автопополнение кошелька, поэтапная оплата подрядчику [512].

Концепцию коммерческой платформы смарт-контрактов, на которой участники рынка смогут публиковать собственные сценарии, Банк России вынес на публичное обсуждение в 2026 году: замечания принимаются до 30.09.2026, оператором на первом этапе предполагается сам Банк России [510]. Целевые выплаты, страховые сценарии и B2B-расчёты с условиями пока остаются на стадии концепции.

24.5 Цифровой рубль и СБП

Цифровой рубль и СБП часто сравнивают из-за государственного участия и низких тарифов. Архитектурно это разные системы: СБП переводит безналичные рубли между банковскими счетами, а цифровой рубль хранится в отдельном кошельке как самостоятельная форма денег [369].

Для клиента и ТСП оба сценария похожи: быстрый перевод по номеру телефона или QR-коду. Различие — в распределении расчётного и кредитного риска. В СБП клиент несёт кредитный риск банка-участника, в цифровом рубле этот риск исчезает по построению. Для банка-участника СБП сохраняет комиссию и контакт с клиентом, а цифровой рубль создаёт риск оттока депозитной базы, который банку нужно компенсировать другими доходами.

24.6 Цифровой рубль в международном контексте

Россия в 2026 году — единственная страна, перешедшая от пилота к законодательно обязательному приёму CBDC в розничном сегменте [513].

Таблица 39 — СБП и цифровой рубль по ключевым параметрам.

	СБП	Цифровой рубль
Природа обязательства	Коммерческого банка	Банка России
Учёт остатков клиента	Банк-участник (счёт клиента)	Банк России
Расчётный цикл	Круглосуточно, в реальном времени	Круглосуточно, в реальном времени
Тариф для ТСП (C2B)	до 0,7 % (по категориям)	0 % до 31.12.2026 (льготный период); с 2027 года — 0,3 %, не более 1500 руб. за перевод [503]
Офлайн-платёж	Нет	Предусмотрен архитектурой, в пилоте не запущен
Смарт-контракты	Нет	Простые — в пилоте; коммерческая платформа в стадии разработки

e-CNY (КНР)

К концу ноября 2025 года в Китае проведено 3,48 млрд транзакций в e-CNY на общую сумму 16,7 трлн юаней (около $2,37 трлн), более чем в восемь раз больше, чем в 2023 году [514]. Пилот охватывает 26 населённых пунктов в 17 регионах. С 1 января 2026 года Народный банк Китая ввёл обновлённую модель управления, в которой e-CNY переходит от аналога наличных к цифровым депозитным деньгам (*digital deposit money*) с депозитными функциями; модель сближается с банковской инфраструктурой. e-CNY остаётся розничной CBDC под централизованным управлением, без публичного блокчейна.

Digital euro (ЕС)

Подготовительная фаза ЕЦБ шла с ноября 2023 по октябрь 2025 года; 30 октября 2025 года Управляющий совет принял решение о переходе в следующую фазу [515]. Целевой запуск — 2029 год при условии принятия законодателями ЕС Регламента о цифровом евро в 2026 году; промежуточный пилот ожидается в середине 2027 года. *Rulebook* — свод единых правил для эмиссии, держателей, ТСП и поставщиков инфраструктуры — четыре месяца обсуждался с участниками рынка и вошёл в итоговый отчёт подготовительной фазы [516].

Digital pound (Великобритания)

Банк Англии провёл публичные консультации в 2023 году и до 2026 года работает в фазе проектирования. В августе 2025 года открыт Digital Pound Lab — экспериментальная отраслевая платформа для проверки сценариев и бизнес-моделей [517]. Решение запускать проект или отказаться от него Банк Англии вместе с HM Treasury планирует представить в 2026 году; запуск требует отдельного парламентского решения. Великобритания, в отличие от ЕС, откладывает законодательство до решения по итогам фазы проектирования [518].

США

Указ Президента США «Strengthening American Leadership in Digital Financial Technology» от 23 января 2025 года запретил федеральным агентствам создавать, выпускать и продвигать CBDC и прекратил их текущие проекты [519]. Это разворот политики предыдущей администрации, при которой инновационный центр ФРБ Нью-Йорка проводил исследовательский Project Cedar [520]. В июле 2025 года Палата представителей приняла Anti-CBDC Surveillance State Act (H.R. 1919) Тома Эммера; законопроект запрещает выпуск CBDC Федеральной резервной системе на уровне федерального закона [521]. Параллельно политический акцент смещается к долларовым стейблкоинам как частной альтернативе CBDC.

Китай форсирует развёртывание с прицелом на глобальную инфраструктуру; ЕС сначала оформляет нормативную базу; Великобритания сохраняет за собой право не запускать проект; США отказались от CBDC через прямой правовой запрет. Россия выбрала другую траекторию: 248-ФЗ [361] превращает приём в обязанность ТСП, а расчёты — в обязанность банков, тремя волнами с 1 сентября 2026 по 1 сентября 2028 года, и такой обязательности нет ни у одного из перечисленных проектов. Международная совместимость цифрового рубля с e-CNY, евро или фунтом не следует из текущих проектов: платформы строятся под разные правила, и синхронизация требует отдельного двустороннего соглашения.

24.7 Project mBridge и Project Agorá

Инфраструктура трансграничных CBDC делится на две непересекающиеся группы центральных банков. Project mBridge — мультивалютная оптовая платформа на базе DLT для прямых расчётов между центральными банками — запущена в 2021 году как совместный проект PBoC, HKMA, Bank of Thailand, Central Bank of the UAE и BIS Innovation Hub. В 2024 году к проекту присоединился Saudi Central Bank, и mBridge перешёл от проверки концепции к минимально жизнеспособному продукту.

31 октября 2024 года генеральный директор BIS Агустин Карстенс объявил о выходе BIS из проекта с формулировкой «graduation» — проект достиг зрелости, при которой партнёрам участие BIS более не требуется [522]. Это произошло через неделю после саммита БРИКС в Казани, где mBridge упоминался как инструмент дедолларизации. BIS подчеркнул, что mBridge «не является BRICS-bridge» и что переход к независимой работе не связан с политическим давлением. Партнёры — PBoC, HKMA, центробанки Таиланда и ОАЭ — продолжают работу самостоятельно; Saudi Central Bank вышел из проекта после завершения своей проверки концепции в мае 2025 года, что стало известно в сентябре 2026 года [523].

Параллельно BIS развивает Project Agorá. В составе — Bank of France, Bank of Japan, Bank of Korea, Bank of Mexico, Swiss National Bank, Bank of England, Federal Reserve Bank of New York и присоединившийся в мае 2026 года Bank of Canada [524, 525]. Цель — единый реестр для токенизированных обязательств коммерческих банков (*tokenised commercial bank money*) и оптовых денег центрального банка (*wholesale central bank money*) с сохранением механизмов контроля корреспондентского банкинга (*correspondent banking*). В Agorá нет участников из БРИКС.

Российские трансграничные инструменты — СПФС, БРИКС Pay, потенциально mBridge через партнёров в Азии — не получают подключения к Agorá. Двусторонние интеграции цифрового рубля с e-CNY или другими CBDC участников mBridge

технически возможны; интеграция с CBDC участников Agorá упирается в санкции и требования корреспондентского банкинга, заложенные в Agorá.

24.8 DCash в Восточно-Карибском валютном союзе

12 января 2024 года Центральный банк Восточно-Карибского валютного союза (ECCB) закрыл пилот DCash после 34 месяцев работы — редкий публичный случай сворачивания розничной CBDC [526]. Ещё в декабре 2023 года ECCB объявил запрос информации у поставщиков (RFVI) для DCash 2.0 с расширенным набором сценариев: P2P, P2B, B2B, G2P, P2G [527, 528]. Монетарный совет ECCB на 112-м заседании 13 февраля 2026 года приостановил разработку DCash 2.0 в пользу межбанковской Fast Payment System и участия в региональном пилоте CARICOM Payments and Settlement System [529].

Пилот работал без обязательного приёма; держателю DCash было удобнее использовать привычные карточные и электронные кошельки. Без массового сценария использования платформа не накапливала транзакции: за 34 месяца совокупный объём остался пилотным и несопоставимым со штатной розничной нагрузкой региона. У российского пилота цифрового рубля похожая статистика на той же стадии: 38 тыс. переводов P2P за 15 месяцев [465]. Разница в том, что у российского цифрового рубля есть обязательный приём по 248-ФЗ [361]; у DCash такого механизма не было.

Розничная CBDC без обязательного приёма не получает регулярного спроса. e-CNY масштабируется через государственные сценарии (зарплаты госслужащим в пилотных провинциях, целевые выплаты, госуслуги) и интеграцию с Alipay и WeChat Pay; цифровой рубль — через законодательное обязательство приёма. Пилоты без регулярных поступлений на кошелёк повторяют траекторию DCash.

Розничной CBDC нужен регулярный источник пополнения кошелька и причина держать остаток между транзакциями. Без этого она проигрывает картам и быстрым переводам по зрелости тарифа и приёмной сети: тариф для ТСП в СБП не превышает 0,7 % (см. табл. 39), карточный эквайринг работает по всей розничной сети, а цифровой рубль на старте обязательного приёма получает только льготный тариф без готовой инфраструктуры. Технологическое преимущество CBDC — прямое обязательство центрального банка и программируемость — ощутимо только тогда, когда пользователь обязан принимать платёж именно в этой форме или заинтересован в этом.

Отдельный механизм регулярного спроса — оптовый wCBDC как расчётный актив для токенизированных обязательств коммерческих банков (*tokenised commercial bank money*). Его рассматривает Великобритания и параллельно пилотирует ЕС: у Банка Англии — токенизация центральных денег на обособленном распределённом реестре [517], у ЕЦБ — расчёт DLT-транзакций в центральных деньгах через Pontes с запуском в III квартале 2026 года и долгосрочная стратегия Appia до 2028 года [530]. Оптовый wCBDC ведётся параллельно с розничной CBDC, не сливаясь с ней в единый проект. DCash не получил ни одного механизма регулярного спроса: розничный пилот без обязательного приёма, без массовых бюджетных каналов и без оптового wCBDC прошёл 34 месяца как демонстрация и закрылся, а DCash 2.0 приостановлен до промышленной эксплуатации.

Часть IV

Жизнь после запуска

Реальный платёжный продукт сопротивляется после запуска: корректно спроектированный поток приносит убыток, теряет деньги на сверке, упирается в комплаенс, провоцирует ложные отказы, накапливает спорные списания и ломается там, где на уровне протокола всё выглядело безупречно.

Часть IV переходит от вопроса «как должен работать платёж» к вопросу «что с ним происходит в эксплуатации»: как авторизация, токен и перенос ответственности ведут себя под давлением атак, операционных ошибок, требований регулятора и поведения пользователя.

Сначала — регуляторика: 161-ФЗ, положения Банка России и лицензионные модели; на них опирается разговор о фроде, спорах и сверке. Затем — дисциплины комплаенса: идентификация клиентов и ТСП (в международной терминологии — KYC, *Know Your Customer*, и KYB, *Know Your Business*), ПОД/ФТ (противодействие легализации/отмыванию доходов и финансированию терроризма; в банке эти обязательства исполняет финмониторинг, в англоязычной практике — AML, *anti-money laundering*) и санкционная проверка. Они разнесены по отдельным главам: пороги, перечни и маршруты эскалации у каждой дисциплины свои, а их смешение быстро оборачивается ошибками на стыке.

Фрод — набор конкретных атак, вынуждающих балансировать между конверсией и защитой. Подписки и *card-on-file* продлевают жизнь платёжного инструмента далеко за пределы одной успешной транзакции: даже при исходном согласии клиента каждое следующее списание требует дисциплины.

Дальше — последствия уже совершившихся операций. Сверка отвечает на вопрос, где теряются деньги или состояния, когда внешние события перестают совпадать с внутренним учётом. Диспуты и chargeback показывают, что успешный платёж не равен защищённой выручке. Управление отказами разбирает точку, где сталкиваются сеть, эмитент, эквайер, антифрод и пользовательская логика.

Часть собирает вместе темы, которые в компаниях разнесены по разным командам. Регуляторикой и ПОД/ФТ занимается комплаенс, фродом — команда риска, регулярными списаниями — биллинг, сверкой — финансовая служба, chargeback — команда диспутов, управлением отказами — команда роста или платёжной эффективности. Для платёжного продукта это одно целое: пользователь видит только, что оплата прошла, не прошла, была оспорена, повторилась неожиданно или исчезла где-то между авторизацией и выпиской.

Продукт взрослеет, когда команда связывает конверсию с потерями от фрода, рост — с требованиями ПОД/ФТ, доход от подписок — с дисциплиной согласия, а финансовый результат — со сверкой, диспутами и отказами.

Дальше в части V книга переходит к внутренней топологии платёжной системы: какой компонент за что отвечает и как они связаны.

25 Нормы регулятора

В платёжном продукте право задаёт архитектуру, когда продукт принимает деньги, открывает кошелёк, маршрутизирует транзакции или гарантирует продавцу срок зачисления. Оно определяет роли участников, разделение ответственности, состояния перевода и обязательные требования к безопасности; код либо реализует эти требования, либо нарушает их.

Глава разбирает российское регулирование; сравнение национальных сетей и стран СНГ — в гл. 18. Точные пороги и даты сверяйте по действующим нормативным актам, правилам платёжных систем и актуальным материалам участников рынка.

25.1 161-ФЗ: субъекты перевода

Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платёжной системе» (далее — 161-ФЗ) отвечает на вопрос: *кто имеет право менять записи* в реестрах банков [1]. Сеть, процессинг, банк и платёжный продукт — юридически разные сущности с разной ответственностью; 161-ФЗ закрепляет это разделение.

Оператор по переводу денежных средств

Перевод денежных средств выполняет оператор по переводу денежных средств (ОПДС) — банк или небанковская кредитная организация (НКО), которые вправе принять распоряжение к исполнению, списать деньги у плательщика и обеспечить их зачисление получателю [1]. У этих участников — эмитента, эквайера, банка получателя, кошелька с клиентским остатком (роли в карточной экосистеме разбираются в гл. 2 и гл. 3) — возникают денежные обязательства и право изменять денежное состояние.

Пока система только передаёт сообщения и остаётся интерфейсом к чужой денежной функции, статус ОПДС остаётся у партнёра. Как только продукт ведёт клиентские остатки, инициирует списание от своего имени или обещает пользователю хранение средств, вопрос о собственном статусе ОПДС нужно решать ещё до запуска.

Платёжная система и её оператор

Закон отдельно выделяет платёжную систему и оператора платёжной системы. Оператор задаёт правила участия, порядок обмена сообщениями, модель расчётов, требования к бесперебойности и управлению рисками [1]. Жизненный цикл сообщения, обязательные поля, сроки сверки и правила работы с инцидентами — следствия правил конкретной системы; в карточном мире — Visa, Mastercard или Мир.

Среди обязательных правил участия 161-ФЗ называет и порядок приостановления и прекращения участия [1]. После выхода участник сохраняет уже возникшие обязательства: незавершённые расчёты и споры по операциям до прекращения закрываются в сроки, установленные правилами системы. Это сетевой аналог ответственности эквайера перед уходящим ТСП (гл. 3).

Провайдер платёжных услуг (*payment service provider*, PSP), платёжный шлюз или платёжный оркестратор (маршрутизатор трафика между несколькими PSP и эквайерами) упрощают интеграцию, но не меняют применимый свод правил. Если сеть требует возможности отмены, фиксированного набора полей или обязательной связки с клиринговой записью, продукт исполняет этот свод правил; собственные соглашения его не подменяют.

Функции платёжной инфраструктуры

161-ФЗ разделяет услуги платёжной инфраструктуры на операционный центр (маршрутизирует и передаёт сообщения между участниками), платёжный клиринговый центр (принимает и сводит распоряжения, рассчитывает нетто-позиции) и расчётный центр (исполняет окончательное движение денег по счетам участников) [1]. Даже если эти роли совмещены у одного участника, маршрутизация авторизации, обработка клиринговых записей и окончательное движение денег остаются разными функциями. Сообщение проходит операционный центр, а расчёт происходит позже и через другой механизм.

Система, которая маршрутизирует сообщения, не обязана отвечать за расчёт; она работает на уровне сообщения. Продукт, обещающий окончательное зачисление в определённый момент, опирается на передачу сообщений и на регламент расчёта — со всеми его сроками и ограничениями. Национальная система платёжных карт (НСПК) обеспечивает маршрутизацию и клиринг внутрироссийского карточного трафика, но банки остаются эмитентами, эквайерами и участниками расчётов.

161-ФЗ закрепляет роли и ответственность участников, а технологическую реализацию оставляет положениям Банка России и правилам платёжных систем, которые обновляются быстрее закона. Протокол авторизации меняется, обязательство банка перед клиентом — нет; закон, фиксирующий технологический стек, требовал бы поправки на каждый новый стандарт.

Сопоставление с PSD2

В ЕС ту же задачу разделения ролей решает директива (EU) 2015/2366, вторая платёжная директива (*Revised Payment Services Directive*, PSD2) [225]. Она делит участников рынка на провайдера платёжных услуг (PSP), платёжную организацию (*payment institution*), организацию электронных денег (*e-money institution*) и банк, ведущий счёт клиента (*account servicing payment service provider*, ASPSP). Российский ОПДС соответствует ASPSP плюс части функций платёжной организации. Статуса оператора платёжной системы PSD2 не вводит: директива определяет только саму платёжную систему (*payment system*) как систему перевода средств с общими правилами обработки, клиринга и расчёта [225].

PSD2 добавляет требования, которых нет в 161-ФЗ. Во-первых, она лицензирует роли третьих лиц с обязательным доступом к счёту клиента: провайдер инициации платежа (*payment initiation service provider*, PISP) инициирует платёж от имени плательщика через счёт в банке-владельце, провайдер информации о счетах (*account information service provider*, AISP) агрегирует сведения о счетах клиента. У 161-ФЗ прямого аналога для PISP/AISP нет; доступ финтеха к счёту клиента в российской модели строится по договору с банком, а не по регуляторному обязательству банка предоставить API. Во-вторых, PSD2 устанавливает обязательную усиленную аутентификацию клиента (*strong customer authentication*, SCA) по двум из трёх факторов

(знание, владение, неотъемлемая характеристика); в российской регуляторике сопоставимые требования к аутентификации распределены по 161-ФЗ (статья 9 об уведомлении клиента о каждой операции) и положениям Банка России. Подробный разбор PSD2 и российской модели открытого банкинга — в гл. 21.

25.2 Положения Банка России

Положения Банка России переводят требования закона в правила работы системы: какие реквизиты обязаны быть в распоряжении, как защищается платёжная инфраструктура, какие требования действуют для банковской информационной безопасности (ИБ), какие документы получает клиент по карточной операции.

По состоянию на март 2026 года инженерные требования по ИБ задают Положения: № 821-П — защита информации при переводах, № 850-П — операционная надёжность, № 851-П — противодействие переводам без согласия клиента [205, 206, 531]. 821-П и 851-П отсылают к ГОСТ Р 57580.1 в части состава мер защиты и к 57580.2 в части оценки соответствия (разбор стандарта — в разделе 25.2). 850-П ссылок на ГОСТ не содержит; операционной надёжности посвящены парные стандарты ГОСТ Р 57580.3 и 57580.4.

762-П: жизненный цикл распоряжения

Положение Банка России от 29.06.2021 № 762-П «О правилах осуществления перевода денежных средств» (далее — 762-П) задаёт реквизиты распоряжения, порядок приёма и исполнения, условия отзыва, прохождение через банки-посредники [532]. У любого перевода есть машина состояний: распоряжение получено, принято к исполнению, исполнено, отклонено, возвращено или отозвано.

762-П делит путь распоряжения на процедуры приёма к исполнению (удостоверение права распоряжения, контроль целостности, структурный контроль, контроль значений реквизитов, контроль достаточности денежных средств) и процедуры исполнения (списание и зачисление, подтверждение исполнения) [532]. Термина «авторизация» в 762-П нет: в карточном цикле ему соответствует контроль достаточности средств. На примере карточной покупки за 3 000 руб. (полный жизненный цикл карточной транзакции с авторизацией, клирингом и расчётом — в гл. 5):

- **T+0, 12:00:00**, приём — банк-эмитент получает авторизационный запрос от сети. Момент фиксируется в журнале; с этой секунды распоряжение считается поступившим.
- **T+0, 12:00:01**, удостоверение права — хост эмитента проверяет PIN или криптограмму, сверяет статус карты.
- **T+0, 12:00:02**, авторизация — проверка достаточности средств, скоринг антифрода, решение (одобрение или отказ).
- **T+1…T+2**, клиринг и исполнение — эквайер передаёт клиринговую запись, сеть рассчитывает нетто-позиции, расчётный центр списывает и зачисляет.
- **T+2**, уведомление — банк-эмитент формирует выписку; продавец получает подтверждение зачисления.

Срок перевода задаёт не 762-П, а часть 5 статьи 5 161-ФЗ: не более трёх рабочих дней со дня списания денежных средств со счёта плательщика; переводы ЭДС, операции с цифровыми рублями и случаи части 5.1 из этого правила исключены [1].

Отзыв распоряжения возможен до наступления безотзывности перевода [532]; для перевода, кроме перевода ЭДС, она наступает в момент списания денежных

средств со счёта плательщика (часть 7 статьи 5 161-ФЗ) [1]. Безотзывность — юридическая точка, после которой логика «отмены» меняется на логику «возврата»: другие сроки, другие документы, обязательное согласование сторон.

Платёжный API, бэк-офис и внутренняя учётная модель обязаны хранить полную машину состояний перевода с временны́ми метками каждой стадии. Поля обязательных реквизитов, времени приёма и времени исполнения подтверждают правовой статус перевода и упрощают сопровождение системы в эксплуатации.

821-П: защита информации при переводе

Положение Банка России от 17.08.2023 № 821-П «О защите информации при переводах денежных средств»[1] задаёт действующие требования к защите переводов [205]. Платёжная инфраструктура становится контролируемой средой с требованиями к защищённым каналам связи, разграничению доступа, журналированию, управлению инцидентами, оценке соответствия и средствам криптографической защиты.

Процессинговый коммутатор и платёжный шлюз нельзя проектировать по схеме «сначала обычный веб-сервис, потом межсетевой экран уровня приложений (*Web Application Firewall*, WAF) сверху». Сегментацию, ключи, администрирование и логи планируют на этапе проектирования.

Переделка после запуска обходится дороже проектирования: сегментация сети постфактум — переработка топологии под рабочей нагрузкой; замена алгоритмов криптозащиты — миграция данных и ротация ключей; разграничение привилегий после выдачи десятков ролей — пересмотр модели доступа.

Надзорная проверка по 821-П опирается на артефакты, которые Банк России запрашивает по графику и в ходе проверок:

- **Журнал инцидентов** фиксирует события защиты информации с точностью до конкретного действия и принятого решения; о значимых инцидентах оператор оперативно информирует ФинЦЕРТ через АСОИ ФинЦЕРТ, а обобщённые сведения о событиях нарушения защиты информации сдаёт по форме 0403203[2] [533].
- **Оценка соответствия** требованиям защиты информации оформляется по форме 0409071 Указания Банка России от 10.04.2023 № 6406-У «О формах отчётности кредитных организаций» и направляется в Банк России по её итогам; периодичность задана Указанием 6406-У и зависит от организации — от одного раза в год до одного раза в три года [534].
- **Отчётность по операционной надёжности** — сведения о показателях технологических процессов и применяемых ИТ — сдаётся по форме 0409072 (того же 6406-У) на основании Положения Банка России от 13.01.2025 № 850-П «Об операционной надёжности»[3] [531].
- **Предписания** Банк России выдаёт по результатам проверок; типовые формулировки — расхождение декларации и реализации по средствам криптозащиты, отсутствие журналирования критических действий, отсутствующая модель угроз для конкретного объекта инфраструктуры, неполная сегментация сети передачи карточных данных. На каждое предписание организация отвечает планом устранения с привязкой к конкретному артефакту, и план остаётся под контролем до закрытия предписания.

[1] В силе с 01.04.2024.

[2] Предусмотрена Указанием Банка России от 27.06.2023 № 6470-У «О формах и сроках отчётности операторов платёжной системы и перевода денежных средств»; заменило 6060-У.

[3] В силе с 03.05.2025; заменило 787-П.

851-П: противодействие переводам без согласия клиента

Положение Банка России от 30.01.2025 № 851-П «О противодействии переводам без согласия клиента»[1] разделяет требования на две группы [206]. *Целевое назначение* первой группы — противодействие фроду на стороне банка-эмитента (см. гл. 29): мониторинг операций по признакам, установленным Банком России, информирование клиента, ограничения на дистанционные операции по заявлению клиента, противодействие выдаче кредитных средств под влиянием обмана. *Исполнительные меры* охватывают систему ИБ кредитной организации, требования к прикладному ПО банковских операций, оценку соответствия по 57580.2, использование сертифицированных СКЗИ.

Прикладное ПО. Пункт 4.1 851-П распространяется на всё ПО, используемое для осуществления банковских операций: оно должно либо пройти сертификацию ФСТЭК (по Постановлению Правительства Российской Федерации от 26.06.1995 № 608 «О сертификации средств защиты информации» [535]), либо иметь оценку соответствия по оценочному уровню доверия не ниже ОУД4 (п. 7.6 раздела 7 ГОСТ Р ИСО/МЭК 15408-3-2013 [536]). Так требование к прикладному банковскому ПО становится самостоятельным объектом контроля, прямого аналога которому в PCI DSS нет — разбор пересечения с PCI DSS см. в разделе 12.7.

Уровень соответствия по 57580.2. Пункт 13 851-П задаёт конкретные пороги: для кредитной организации — уровень соответствия не ниже четвёртого (подп. «д» п. 6.9 раздела 6 57580.2); для филиала иностранного банка — не ниже третьего (подп. «г») до 31.12.2026 и не ниже четвёртого с 01.01.2027. Внешний независимый аудит проводит проверяющая организация с лицензией ФСТЭК, отчёт хранится не менее пяти лет, периодичность — не реже одного раза в два года.

Новое относительно 683-П. 851-П добавляет регистрацию аутентификации с геолокацией и IP-адресами, контроль изменения SIM-карт клиента, уведомление законных представителей при выдаче электронных средств платежа (ЭСП) несовершеннолетним 14–18 лет, модель СУИБ, описанную через цикл PDCA. С 01.10.2025 банк, применяющий усиленную неквалифицированную электронную подпись для целостности электронных сообщений или подтверждения их составления, обязан создавать её средствами электронной подписи и удостоверяющего центра, имеющими подтверждение соответствия требованиям ФСБ России (подп. 5.1 и 5.3 п. 5, п. 15 851-П) [206].

Соответствие PCI DSS и соответствие 821-П, 851-П, 850-П — параллельные обязательства, не альтернативы. Карточная среда, соответствующая PCI DSS, остаётся под российскими регуляторными требованиями: действуют требования 821-П к переводам, 851-П к прикладному ПО и антифроду, 850-П к операционной надёжности. Формулировка «Мы соответствуем PCI DSS» подтверждает выполнение одного свода требований и не подтверждает выполнение остальных.

ГОСТ Р 57580.1 и 57580.2: исполнительный стандарт защиты информации

За конкретными мерами защиты 821-П и 851-П отсылают к национальному стандарту ГОСТ Р 57580.1-2017, где зафиксирован базовый состав мер. Стандарт разработан Банком России совместно с НПФ «КРИСТАЛЛ» [181]. Парный ГОСТ Р 57580.2-2018 «Методика оценки соответствия» задаёт способ внешнего аудита по 57580.1 [249].

[1] В силе с 29.03.2025; заменило 683-П.

ГОСТ становится требованием только в той части, на которую ссылается нормативный акт регулятора — через нормативную ссылку по статье 27 Федерального закона от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации» [537]. 821-П делает такие ссылки для конкретных категорий объектов информатизации; 851-П распространяет требования на систему ИБ кредитной организации в целом, задавая через 57580.2 конкретный минимальный уровень соответствия (см. выше). За пределами охвата обоих Положений 57580 остаётся рекомендательным.

Структура 57580.1. Базовый состав мер разделён на процессы: управление доступом, защита вычислительных сетей, контроль целостности и защищённости информационной инфраструктуры, защита от вредоносного кода, предотвращение утечек, управление инцидентами, защита виртуализации, защита при удалённом и мобильном доступе. К процессам добавлены четыре направления управления (планирование, реализация, контроль, совершенствование) и отдельный раздел требований к защите на этапах жизненного цикла автоматизированных систем (АС).

Уровни защиты. Стандарт определяет уровни защиты информации УЗ-1 (усиленный), УЗ-2 (стандартный) и УЗ-3 (минимальный). Уровень для конкретной АС задаёт нормативный акт Банка России: он зависит от категории организации и типа объекта информатизации.

Оценка соответствия по 57580.2. Оценку соответствия проводит сторонняя организация с лицензией ФСТЭК России на техническую защиту конфиденциальной информации (минимум один из видов работ: контроль защищённости от НСД, проектирование в защищённом исполнении, установка, монтаж и испытания средств защиты) [249]; внутренняя самооценка того же результата не даёт. Каждая мера получает числовую оценку 0 или 1 (выбор), для процессов управления и жизненного цикла АС — 0, 0,5 или 1 (полнота реализации). Среднеарифметическое по процессу даёт итоговый показатель, который сопоставляется с шестибалльной качественной шкалой: нулевой уровень (меры не реализуются), первый (бессистемно, эпизодически), второй (значительный объём без контроля), третий (значительный объём с эпизодическим контролем), четвёртый (полный объём со стабильным контролем), пятый (полный объём с непрерывным совершенствованием). Минимальный уровень задаёт 851-П (см. выше).

266-П: карточная операция как документ

Эмиссию платёжных карт и операции с их использованием регулирует Положение Банка России от 24.12.2004 № 266-П «Об эмиссии платёжных карт» [538]; обязанность информировать клиента о каждой операции с использованием ЭСП дополнительно установлена статьёй 9 161-ФЗ [1]. На момент подготовки главы Банк России готовит акт на смену 266-П: в 2024 году опубликован проект Положения «О порядке предоставления электронных средств платежа и осуществления операций с их использованием».[1] До его вступления в силу 266-П сохраняет прямое действие. Помимо авторизационного жизненного цикла, у карточного платежа есть документальный след: чек или иной документ по операции, электронное подтверждение, запись в мобильном банке, уведомление клиенту, механизм оспаривания.

266-П задаёт обязательные реквизиты документа по операции: идентификатор банкомата или терминала, вид операции, дату, сумму и валюту операции, сумму комиссии, код авторизации, реквизиты карты; бумажный документ в пункте

[1] По состоянию на май 2026 года заменяющий акт не вступил в силу; реквизиты вступления в силу проверяйте по первоисточнику на сайте Банка России.

выдачи наличных дополнительно подписывают держатель и кассир [538]. Каждая операция должна однозначно идентифицироваться по документу, выданному или направленному клиенту.

Минимальный набор реквизитов по каждой транзакции — исходный материал для ответа клиенту, аудитору и регулятору. Терминальное ПО и страница оплаты формируют и выдают документ с правильным составом полей. Мобильный банк и личный кабинет показывают детали операции в формате, пригодном для оспаривания.

Цифровой рубль: обязанность банка

Цифровой рубль добавляет банку отдельные обязанности. 340-ФЗ [4] закрепил его как форму национальной валюты, а 248-ФЗ обязал банки поэтапно обеспечить клиентам операции с цифровыми рублями: системно значимые банки и банки, включённые в реестр кредитных организаций, признанных Банком России значимыми на рынке платёжных услуг [502], — с 1 сентября 2026 года, банки с универсальной лицензией — с 1 сентября 2027 года, остальные — с 1 сентября 2028 года. Тот же закон ввёл универсальный платёжный код, оператором которого назначен оператор НСПК; сроки подключения к нему банков определяет Банк России [361]. Защиту информации для участников платформы задаёт 833-П [500], а архитектуру и роль банка как посредника доступа разбирает гл. 24 (раздел 24.2).

25.3 Лицензирование

Интерфейс с банком-партнёром

Продукт, который предоставляет пользователю или продавцу интерфейс, но не берёт обязательства хранить или переводить деньги, строится в партнёрстве с банком, эквайером или PSP. На стороне партнёра остаётся денежный статус, расчёты, регуляторная отчётность и формальное исполнение распоряжения. На сам продукт всё равно распространяются платёжные требования и требования по защите информации через договоры и интеграции, но самостоятельным носителем банковской функции он не становится.

До запуска архитектура должна ответить на вопросы: где хранятся деньги, чьё имя стоит в договоре с клиентом, кто выпускает чек, кто отвечает за спорную операцию, кто меняет баланс. Пока ответы не зафиксированы, формула «мы только интерфейс» не отвечает ни на один из них.

Агрегатор, агент и PayFac: пограничные модели

Между чистым интерфейсом и полноценным хранением денег есть промежуточные модели:

- **Платёжный агент** действует от имени банка по агентскому договору по Федеральному закону от 03.06.2009 № 103-ФЗ «О деятельности по приёму платежей физических лиц, осуществляемой платёжными агентами» [539].
- **Агрегатор** принимает платежи в пользу нескольких ТСП через расчётный счёт банка-партнёра.
- **Платёжный фасилитатор** (*payment facilitator*, PayFac) — модель платёжных систем, при которой фасилитатор самостоятельно подключает субмерчантов по собственному контракту с эквайером.

- Иной продукт, который подключает ТСП и управляет клиентским сценарием, хотя денежная функция и расчётная обязанность остаются у банка или другого партнёра.

Модели различаются тем, у кого находятся деньги, кто выпускает расчётный документ и кто входит в договорные отношения с клиентом и продавцом.

Подключение ТСП, идентификация клиентов и ТСП, чек, возврат, спорная операция и расчётные сроки распределяются между участниками экосистемы из раздела 2.2: кто заключает договор с ТСП, кто несёт риск, кто меняет баланс, кто отвечает за расчёт после операции. Чем больше продукт определяет ценообразование, маршрутизацию, поддержку клиентов и операции ТСП, тем раньше нужно зафиксировать, где заканчивается сервис и начинается регулируемая денежная функция. Слова «агрегатор», «платформа» или «сервис для приёма платежей» не определяют статус — его определяет фактический набор функций.

Процессинг и маршрутизация без хранения денег

Платформа, которая маршрутизирует сообщения и обрабатывает авторизации, но не становится должником клиента по его деньгам, ближе всего к роли операционного центра. Если она начинает подтверждать и сводить распоряжения, она получает функции платёжного клирингового центра. В обоих случаях это услуги платёжной инфраструктуры; деньги остаются у партнёра [1].

Такая система не превращается автоматически в банк, но получает требования к бесперебойности, защите информации, аудиту и управлению инцидентами. Формула «мы только передаём сообщения» снижает лицензионные требования по сравнению с хранением денег, но перечисленные требования инфраструктуры остаются в силе.

Кошелёк или баланс клиента

Продукт, который начинает хранить клиентские средства, вести баланс, открывать кошелёк или иным образом становиться должником пользователя по деньгам, требует статуса кредитной организации (по Федеральному закону от 02.12.1990 № 395-1 «О банках и банковской деятельности») с правом на соответствующие операции, включая перевод электронных денежных средств (ЭДС) [1, 540]. С этого момента меняются ключевые требования: капитал, отчётность, комплаенс, антифрод, противодействие отмыванию доходов и финансированию терроризма (ПОД/ФТ), безопасность и отношения с регулятором.

Денежная функция возникает там, где у продукта появляется обязательство вернуть клиенту его деньги по требованию. Балансы в личном кабинете, бонусные кошельки с возможностью оплаты у произвольного продавца, предоплаченные счета маркетплейса с остатком, конвертируемым в деньги к выводу, — во всех этих случаях продукт хранит остаток клиента и обязан вернуть его по запросу. Если продукт даёт пользователю обещание «ваши деньги хранятся у нас и доступны по запросу», название продукта в личном кабинете не меняет правовой природы операции. Архитектурно остаются два варианта — становиться кредитной организацией самому или встраиваться в банковскую инфраструктуру через ОЭДС-партнёра, который остаётся обязанным по ЭДС (часть 2 статьи 12 161-ФЗ [1]; лимиты остатка и операций по ЭДС см. гл. 26). Получение лицензии банка или НКО — годы; работа через ОЭДС-партнёра по статусу платёжного агрегатора (статья 14.1 161-ФЗ) — кварталы, но партнёр определяет тарифную сетку и учётную модель кошелька,

а продукт работает в его операционном дне. Федеральный закон от 20.02.2026 № 44-ФЗ «Об ограничении идентификации физических лиц банковскими платёжными агентами»[1] [53] исключил схему, в которой банковский платёжный агент (БПА) самостоятельно идентифицировал физлицо и открывал ему электронный кошелёк: эта функция централизована у кредитных организаций, и агентская модель остаётся для приёма платежей и переводов без открытия счёта в пределах установленных лимитов.

Собственная платёжная система

Организация, которая сама задаёт правила взаимодействия участников, обязана зарегистрироваться оператором платёжной системы по 161-ФЗ [1]. Вместе с регистрацией приходят обязанности по своду правил, управлению рисками, непрерывности работы, допуску участников и модели расчётов.

Пока платформа помогает передавать сообщения, она — поставщик технологии. Как только она задаёт обязательные правила обработки этих сообщений для нескольких участников, к ней применяются обязанности оператора платёжной системы.

ПРАКТИКА

Главный архитектурный вопрос — возникает ли у нас собственное обязательство по чужим деньгам. Если нет, схему можно строить через партнёра; если да, схема переходит к банку, НКО и полному набору регуляторных требований.

25.4 Вопросы к платёжной архитектуре

Приведённые ниже вопросы, заданные новой платёжной схеме или партнёрской интеграции, выявляют правовой, операционный и продуктовый риск до запуска; каждый в российской практике 2022–2026 годов уже проявлялся в публичных случаях.

Где возникает денежное обязательство?

Юридический должник перед пользователем или продавцом не всегда совпадает с брендом, который видит клиент. Когда Банк России приказом от 21.02.2024 № ОД-266 «Об отзыве лицензии КИВИ Банка» отозвал лицензию у КИВИ Банка (финмониторинг и разбор причин — в разделе 27.3), держатели вкладов получили выплаты АСВ до 1,4 миллиона рублей, а держатели кошельков QIWI — нет: остатки на кошельках учитывались как электронные денежные средства по 161-ФЗ и под систему страхования вкладов не подпадают [1, 541]. Та же схема воспроизводится в маркетплейсах: остаток продавца на внутреннем счёте маркетплейса — требование к маркетплейсу, а не вклад в банке-партнёре, и при банкротстве маркетплейса страхование вкладов АСВ не применяется.

Кто вправе принять распоряжение и поменять баланс?

Интерфейс, процессинг и маршрутизация юридически отделяются от стороны с денежной функцией; перепутать эти роли — значит работать без требуемой лицензии. С 1 октября 2024 года платёжные агенты обязаны быть включены в реестр

[1] В силе с 03.03.2026; договоры ОПДС с БПА приводятся в соответствие в течение 180 дней.

операторов по приёму платежей Банка России [539, 542]; сервисы, маршрутизировавшие платежи между ролью «агент» и ролью «оператор ЭДС», включились в реестр или прекратили работу в прежней модели. Тот же критерий определяет, нужна ли стартапу банковская лицензия: если продукт сам меняет балансы пользователей, лицензия нужна.

По какому своду правил исполняется операция?

Закон, правила платёжной системы, договор с партнёром и внутренняя модель состояний не должны противоречить друг другу. После 6 марта 2022 года карты Visa и Mastercard, выпущенные российскими банками, продолжили приниматься внутри страны через операционный и платёжный клиринговый центр (ОПКЦ) НСПК; для эквайеров и ТСП переход не потребовал замены интеграций — внутрироссийские операции по этим картам ОПКЦ НСПК процессировал с 2015 года (гл. 16). Администрирование правил для внутрироссийского трафика перешло к НСПК: тарифы межбанковской комиссии (*interchange*) теперь устанавливает НСПК [1, 543], а интеграция эквайера и договоры с ТСП сохранили прежнюю основу.

Какие статусы, документы и уведомления система обязана выдавать?

Если ответа на этот вопрос нет, сбой проявится на споре, возврате и аудите. СБП — это сервис прямых переводов между счетами (*account-to-account*, a2a) клиентов в разных банках, и любой межбанковский спор по такому переводу с 30 июня 2023 года идёт через систему урегулирования «Диспут+» НСПК [544] (механика клиентских споров и отличие от карточного цикла — в разделе 32.8). Регламент задаёт сроки (180 дней на инициирование, до 30 дней на рассмотрение), роли инициатора и ответчика, состав подтверждающих документов; двусторонние договорённости между банками его не подменяют. Спор рассматривает банк получателя; если решение положительное, НСПК проводит автоматические расчёты между сторонами диспута — возмещение приходит отдельной проводкой, не отзывом исходного перевода.

В какой момент операция становится окончательной и кто разбирает спор?

Безотзывность платежа — инженерное свойство, ограниченное правом. Поправки в 161-ФЗ Федеральным законом от 24.07.2023 № 369-ФЗ «О защите клиентов от переводов без согласия» [350] обязали банк плательщика выявлять операции с признаками перевода без согласия клиента, в том числе по сведениям базы данных Банка России о случаях и попытках таких переводов. Карточную операцию, перевод ЭДС и перевод через СБП с такими признаками банк отклоняет, а клиент вправе повторить операцию с теми же реквизитами и суммой; распоряжение по остальным переводам банк приостанавливает на два дня, и клиент может подтвердить его не позднее следующего дня [1]. Признаки задаёт приказ Банка России от 05.11.2025 № ОД-2506 «О признаках перевода без согласия клиента»[1] [545]. Если банк получил сведения из базы и всё же исполнил такую операцию в нарушение этих требований, он обязан возместить клиенту-физлицу сумму в течение 30 дней после его заявления. Для СБП это означает, что между приёмом распоряжения и межбанковской проводкой появляется стадия проверки, в которой банк пропускает

[1] В силе с 01.01.2026; заменил ОД-1027 от 27.06.2024.

или отклоняет перевод, а клиент подтверждает намерение повторной операцией; финальность по-прежнему наступает в момент проводки (детальная механика антифрода и финальности в СБП — в разделе 19.8).

Ответы на «кто меняет баланс», «кто владеет сводом правил» и «кто разбирает ошибочный платёж» нужны на этапе раннего проектирования: от них зависит, выполнит ли архитектура обязательства перед регулятором и клиентом. На этапе интеграции, когда API, договор, сценарий поддержки и внутренняя модель статусов дают разные ответы на один и тот же вопрос, расхождение проявится на возврате, диспуте, аудите или инциденте.

25.5 Мир: нормативное требование как инженерная задача

Закон и нормативные акты требуют поддержки Мир; для инженерии это означает корректное распознавание карт Мир, маршрутизацию внутрироссийского трафика через инфраструктуру НСПК, сценарии приёма в терминалах и электронной коммерции, отражение Мир в процедуре подключения ТСП и в клиентской поддержке [5, 294].

Инженерная работа PSP или эквайера по обязательной поддержке Мир состоит из терминальной, хостовой и договорной частей.

На терминалах — обновление конфигурации системы управления терминалами (*Terminal Management System*, TMS), развёртывание ядра бесконтактного приёма Мир, проверка, что терминал распознаёт диапазоны банковских идентификационных номеров (*Bank Identification Number*, BIN) карт Мир и корректно обрабатывает контактный и бесконтактный сценарии.

На хостовой стороне — подключение маршрутизации через ОПКЦ, согласование профиля полей формата сообщений финансовых транзакций ISO 8583 (см. гл. 6) по спецификации НСПК, прохождение хостовой сертификации.

В договорах — включение Мир в стандартный контракт ТСП, настройка сопоставления кодов категории торгового предприятия (*Merchant Category Code*, MCC), корректное отображение в расчётных отчётах и на панели управления.

Подробный разбор НСПК, ОПКЦ, Mir Pay и обязательности Мир — в гл. 16. Точные пороги обязательного приёма, даты развёртывания и актуальные исключения нужно сверять по действующим документам НСПК, Банка России и правилам сетей.

26 Идентификация клиентов и ТСП

Идентификация физлица (KYC, *Know Your Customer*) и идентификация юрлица или ТСП (торгово-сервисное предприятие; KYB, *Know Your Business*) формируют профиль клиента — совокупность собранных и оценённых сведений, по которой принимается решение по каждой последующей операции. Комплаенс в платёжном бизнесе отвечает на вопросы: кого можно подключить, какие сведения о клиенте или ТСП уже проверены и когда операцию нужно остановить.

26.1 Идентификация при подключении физлиц

Идентификация физлица задаёт уровень доверия к клиенту. На каждом уровне оператор решает, можно ли считать человека тем, за кого он себя выдаёт, и какой риск принимает, открывая ему следующий набор операций.

Проверка начинается с минимального набора сведений и доходит до документальной сверки и дополнительных процедур там, где этого требует закон или профиль риска — набор признаков клиента, по которым оператор относит его к уровню риска, заданному Положением Банка России от 15.10.2015 № 499-П «Об идентификации клиентов в целях ПОД/ФТ» [546]. Чем меньше сведений собрано при подключении, тем меньше доступных операций и ниже лимиты; Банк России разъясняет это на примере переводов и электронных кошельков по упрощённой идентификации [547]. Автоматизация ускоряет подключение, но качество данных проверяют до допуска клиента или продавца: ошибка при подключении редко ограничивается одним клиентом.

Стандартный набор проверок — сверка документов по государственным источникам, проверка по перечням Росфинмониторинга и иным санкционным спискам (см. гл. 28), а также выявление политически значимого лица (PEP, *politically exposed person*) — человека, наделённого или ранее наделённого значимой публичной функцией; процедуры противодействия легализации (отмыванию) доходов и финансированию терроризма (ПОД/ФТ) распространяют этот статус на членов его семьи и ближайшее окружение и применяют ко всей категории усиленную проверку из-за повышенного коррупционного риска [546, 548]. Методология PEP восходит к рекомендациям FATF; о приостановке членства РФ в FATF и текущей роли ЕАГ как региональной *FATF-style body* для СНГ — см. раздел 27.4.

Для неидентифицированного пользователя электронных денежных средств (ЭДС) 161-ФЗ (статья 10) ограничивает остаток ЭДС суммой 15 000 руб. в любой момент и месячный оборот — суммой 40 000 руб., и эти ограничения действуют до прохождения упрощённой идентификации (без подтверждения личности по документу с фотографией). После упрощённой идентификации лимит остатка ЭДС увеличивается до 100 000 руб., а месячный оборот — до 200 000 руб. [1]. Для полной (персонифицированной, то есть с очной или эквивалентной сверкой документа, удостоверяющего личность) идентификации физлица-резидента РФ лимит остатка установлен законом на уровне 600 000 руб.; дополнительные параметры могут определяться договором с оператором. Система должна хранить текущий статус идентификации клиента и применять соответствующие лимиты перед каждой операцией.

ЕСИА: упрощённая идентификация через инфраструктуру электронного правительства

Основной канал упрощённой идентификации в РФ — Единая система идентификации и аутентификации (ЕСИА), федеральная информационная система, созданная Постановлением Правительства РФ от 28.11.2011 № 977 «О ЕСИА» как часть инфраструктуры электронного правительства [549]. 115-ФЗ допускает её использование кредитными организациями для упрощённой идентификации физических лиц, ссылаясь на инфраструктуру электронного правительства как на источник проверенных сведений [351].

У учётной записи ЕСИА три уровня. **Упрощённая** (уровень 1) подтверждена телефоном или электронной почтой и не идентифицирует пользователя для целей 115-ФЗ. **Стандартная** (уровень 2) дополнительно требует СНИЛС и паспортные данные, прошедшие сверку с реестрами Социального фонда России и МВД. Для упрощённой идентификации через ЕСИА 115-ФЗ требует квалифицированную подпись или простую подпись, ключ которой выдан при личном приёме, то есть подтверждённую учётную запись [351]. **Подтверждённая** (уровень 3) требует личного визита в центр обслуживания или подтверждения кодом из заказного письма Почты России и открывает полный объём государственных услуг.

PSP или банк получает результат проверки через систему межведомственного электронного взаимодействия (СМЭВ): запрос возвращает набор подтверждённых атрибутов клиента из ЕСИА вместо очного предъявления документов. Делегированная идентификация (T-ID Т-Банка, Сбер ID и подобные) устроена иначе: банк, уже идентифицировавший клиента по собственной процедуре, передаёт подтверждённые атрибуты партнёру с согласия пользователя [550].

ЕБС: дистанционная полная идентификация по биометрии

Полную (персонифицированную) идентификацию без визита в отделение банка с 2018 года обеспечивает Единая биометрическая система (ЕБС). Нормативная основа — Федеральный закон от 29.12.2022 № 572-ФЗ «Об идентификации и аутентификации по биометрическим персональным данным» [551]; удалённую идентификацию по биометрии в 115-ФЗ ввёл Федеральный закон от 31.12.2017 № 482-ФЗ «Об удалённой идентификации по биометрии» [351, 552]. Биометрия (голос и изображение лица) хранится в государственной системе, уровень регистрации определяет доступные сервисы [553, 554]:

- упрощённый — самостоятельно в приложении «Госуслуги Биометрия» по подтверждённой учётной записи Госуслуг и селфи; проезд в транспорте, проход в офис и другие базовые сервисы;
- стандартный — в том же приложении по загранпаспорту нового образца, прочитанному через NFC, с записью голоса; дополнительно SIM-карты, дистанционное обучение, покупки до 5 000 руб.;
- подтверждённый — очно по паспорту и СНИЛС; все сервисы ЕБС, включая дистанционное открытие счёта и выпуск электронной подписи.

Подтверждённый уровень всегда требует очной сверки личности с паспортом: в отделении банка или при выезде сотрудника банка к клиенту [555]. Самостоятельная регистрация в приложении банковской идентификации не даёт: дистанционное открытие счёта доступно только на подтверждённом уровне [556]. При последующем удалённом обращении клиент подтверждает личность по биометрии.

Оператор ЕБС с 16 декабря 2022 года — АО «Центр биометрических технологий», созданное Указом Президента РФ от 30.09.2022 № 693 «Об определении организации, обеспечивающей развитие цифровых технологий идентификации и аутентификации» [557]; ранее функции оператора исполнял ПАО «Ростелеком» [458]. К 30 сентября 2023 года банки передали в ЕБС накопленные массивы биометрических данных; с 1 марта 2026 года микрофинансовые компании (микрокредитные — с 1 марта 2027 года) при дистанционном обслуживании обязаны идентифицировать физических лиц через ЕСИА и ЕБС [558].

Через ЕБС банк может предоставлять клиенту услуги, требующие полной идентификации, без очного визита: повышать лимит остатка ЭДС до 600 000 руб., открывать счёт, выдавать карту. С индийским Aadhaar ЕБС роднит централизованная государственная база биометрии [559]; эстонская ID-карта подтверждает личность ключом на чипе, без биометрического сличения [560].

Атаки на биометрию: *presentation* и *injection*

Требование первого очного визита в отделение — контрмера против атаки вбросом (*injection*). *Presentation attack* — предъявление устройству захвата фальшивого артефакта: распечатки лица, экрана с фотографией, маски, видео на стороннем дисплее. *Injection attack* — обход устройства захвата: атакующий вбрасывает синтетическое видео (дипфейк) или подменённый поток прямо в API верификации, минуя камеру.

Стандарты охватывают эти классы по-разному. ISO/IEC 30107-3 описывает методологию тестирования *presentation attack detection* (PAD); iBeta Level 1 и Level 2 — стандартная отраслевая сертификация для PAD по ISO 30107-3 [561]. *Injection attacks* этот стандарт не покрывает. Европейская техническая спецификация CEN/TS 18099 от 2024 года и готовящийся ISO 25456 посвящены этому классу атак [562]; в США NIST в четвёртой редакции *Digital Identity Guidelines* (SP 800-63-4), окончательная редакция которой вышла в августе 2025 года, выделяет *injection attack* в отдельный класс [563].

Число атак выросло с распространением AI-генерации лиц. Один из крупных финансовых институтов зафиксировал за январь — август 2025 года 8065 попыток обхода *liveness* через дипфейки — десятки попыток в день на один канал [564]. Открытые платформы *deepfake-as-a-service* снизили требования к навыкам атакующего; статичная проверка живости (пассивный *liveness* — по артефактам видеопотока) и даже проверка отклика на запрос (активный *liveness* — моргнуть, повернуть голову) обходятся синтетическими моделями реального времени.

Защита строится как многофакторная (*multi-factor*) верификация на стороне канала идентификации. ЕБС реализует её через первое очное предъявление: атакующий должен скомпрометировать и биометрическую проверку, и очную сверку с паспортом. Полностью удалённое подключение открыто для атаки вбросом, которую PAD-сертификация по iBeta Level 2 не покрывает. При проектировании реестра клиентских профилей устойчивость биометрического канала оценивают по CEN/TS 18099 или NIST SP 800-63-4, не только по ISO 30107-3, которая атаки вбросом не охватывает.

26.2 EUDI Wallet и eIDAS 2.0

К концу 2026 года все страны ЕС обязаны выдавать гражданам и резидентам European Digital Identity Wallet (EUDI Wallet) [565]. Это часть Регламента 2024/1183, известного как eIDAS 2.0 и изменившего регламент 910/2014. Не позднее 24 декабря 2027 года частные проверяющие стороны, обязанные применять строгую аутентификацию пользователя, — банки, телеком, энергетика — должны принимать кошелёк как канал аутентификации.

EUDI Wallet работает по модели избирательного раскрытия (*selective disclosure*): пользователь выбирает, какие атрибуты раскрыть проверяющей стороне (*relying party*). Можно подтвердить факт совершеннолетия без раскрытия даты рождения, факт резидентства без раскрытия адреса, факт юридической дееспособности без раскрытия профессии. Для этого служат подтверждаемые удостоверения (*verifiable credentials*) в форматах SD-JWT VC и ISO/IEC 18013-5 (mdoc): эмитент подписывает хеши отдельных атрибутов, кошелёк раскрывает только выбранные; доказательства с нулевым разглашением (ZKP) ARF рассматривает как надстройку над этими форматами. Архитектурная и эталонная модель (ARF) — техническая спецификация, в июле 2026 года вышла версия 3.0 — описывает протоколы и форматы для эмитентов, кошельков и проверяющих сторон [566].

ЕБС — централизованная государственная система с единым реестром биометрических шаблонов; EUDI Wallet — децентрализованная модель, где кошелёк находится на устройстве пользователя, а эмитент атрибута (государство, банк, университет) подписывает удостоверение (*credential*), не получая информации о местах его использования. ЕБС опирается на единый канал верификации; EUDI Wallet — на интероперабельность между независимыми сервисами и странами.

Для российского PSP с европейскими клиентами или корреспондентскими отношениями EUDI Wallet с 2027 года становится ещё одним стандартом удалённой идентификации параллельно с ЕБС. Реестр клиентских профилей должен поддерживать оба формата: атрибуты из ЕБС по существующему формату и подтверждаемые удостоверения из EUDI Wallet по ARF-схеме.

26.3 Идентификация при подключении ТСП

У юридического лица проверяют регистрационные данные и деловую конструкцию: структуру собственности, фактический вид деятельности, возвраты, спорные операции и риск использования бизнеса как транзитной оболочки. Идентификация юрлица связывает регистрационные данные, владельцев и платёжное поведение в профиль риска.

Базовый пакет документов включает выписку из реестра, данные директора и учредителей, сведения о бенефициарном владельце (*ultimate beneficial owner*, UBO), банковские реквизиты и описание бизнеса. Нестыковки в структуре владения или сайт, не соответствующий заявленному виду деятельности, — повод для дополнительных вопросов. Формально корректные документы не устраняют риск: после подключения профиль сверяют с наблюдаемым поведением по операциям. Проверку владельцев требуют 115-ФЗ [351] и 499-П: кредитная организация должна установить данные самого клиента и сведения о бенефициарном владельце [546].

Код категории торгового предприятия (*Merchant Category Code*, MCC) сам по себе нейтрален; правила сетей требуют корректно классифицировать ТСП и передавать правильный код категории. Для категорий повышенного риска (*high-integrity risk*

merchants в терминологии Visa) действуют отдельные ограничения и требования мониторинга [13]. Подмена MCC — попытка скрыть фактический профиль бизнеса под менее рискованной категорией. Если заявленная категория не сходится с фактической деятельностью, платёжный поток останавливают до выяснения.

Модель платёжного фасилитатора (*payment facilitator*, PayFac) переносит ответственность за идентификацию субмерчантов (*sponsored merchants* — продавцов, подключённых через PayFac), их KYB, текущий мониторинг и разбор споров на саму платформу; содержание проверки остаётся прежним. Visa возлагает на эквайера ответственность за PayFac и его субмерчантов: до начала обработки нужно подтвердить регистрацию PayFac у Visa, присвоить уникальные идентификаторы самому PayFac и его субмерчантам, получать отчётность по их операциям и следить за корректным MCC [13]. Платформа подключает субмерчантов быстрее, но берёт на себя собственные процедуры идентификации и частый мониторинг. Без них быстрое подключение превращается в быстрое накопление риска.

Глубина должной проверки (*due diligence*) — комплекса процедур по сбору и оценке сведений о клиенте — растёт вместе с профилем риска ТСП: расширяется пакет документов, учащается мониторинг, к высокорисковым категориям применяют плавающий резерв (*rolling reserve*) — удержание части оборота ТСП на отдельном счёте до истечения срока оспаривания. Андеррайтинг сверяет заявителя с реестрами расторгнутых ТСП карточных сетей (MATCH у Mastercard, VMSS у Visa; см. гл. 3): прежнее отключение за chargeback или фрод повышает уровень риска либо останавливает подключение.

ПРАКТИКА

При проверке ТСП основной признак риска — несоответствие заявленного MCC фактической деятельности.

Проверка ТСП идёт по шагам: сбор данных (документы, UBO, банковские реквизиты в профиль), решение (риск-ориентированный подход, RBA — подробнее см. гл. 27 — присваивает уровень риска и определяет глубину должной проверки) и мониторинг после подключения (сравнение заявленного с наблюдаемым). Все три шага используют запись ТСП в реестре клиентских профилей, где регистрационные сведения, бенефициары, MCC, лимиты и резерв связаны общим идентификатором. Несоответствие MCC заявленной деятельности система выявляет автоматически только при наличии второго независимого источника данных о фактической специализации продавца: анкеты эквайера, страницы оплаты, состава чеков. Без такого источника MCC остаётся самозаявленным, а ручной разбор начинается после первой жалобы. Модель PayFac добавляет к записи уровень субмерчантов: их атрибуты хранятся в реестре клиентских профилей платформы на той же глубине, что и атрибуты прямых ТСП эквайера, иначе общий идентификатор не связывает проверки.

Таблица 40 — Критерии идентификации ТСП по категориям риска.

Критерий	Низкий риск	Средний риск	Высокий риск
Примеры MCC	розница, SaaS (*Software as a Service*)	путешествия	криптобиржа, азартные игры, контент 18+
Документы	стандартный пакет	расширенный пакет + лицензии	расширенный пакет + финансовая отчётность
Мониторинг после подключения	квартальный	ежемесячный	еженедельный
Плавающий резерв	нет	5–10%	10–20%

26.4 Мониторинг ТСП после подключения

Риск меняется после подключения, поэтому мониторинг сравнивает текущие объёмы, географию и долю возвратов с профилем ТСП. Схемы типа *bust-out* (когда клиент или ТСП длительное время ведёт себя добросовестно, чтобы нарастить лимиты, а затем резко выводит средства; подробнее — в гл. 29) и попытки использовать ТСП для отмывания проявляются после подключения. Если правила опираются только на статический профиль, сигнал появляется поздно.

Сигналы для расследования — резкий рост оборота, нетипичная география клиентов, высокий процент возвратов и несоответствие MCC фактической деятельности.

В промышленных системах это надстройка над авторизационной базой: агрегаты по ТСП, скользящие периоды, поиск выбросов и очередь расследований. При резком росте объёма у ТСП аналитик получает сигнал сразу, а не в конце месяца. Для платёжных фасилитаторов и ТСП категории *high-integrity risk* Visa требует от эквайера сохранять ежедневные данные по обороту, среднему чеку, количеству операций и количеству диспутов и сравнивать их с обычным профилем операций не реже раза в день [13].

Цикл обновления данных по уровню риска

115-ФЗ задаёт периодичность обновления сведений о клиенте по уровню риска: для клиентов высокого и среднего риска — не реже раза в год, для клиентов низкого риска — не реже раза в три года (пп. 3 п. 1 ст. 7) [351]. Внеочередное обновление обязательно при изменении сведений о клиенте и при возникновении подозрений в отношении его операций. К ТСП применяют ту же схему: плановый пересмотр KYB-профиля по уровню риска и внеочередной — по событию.

В процедурах ПОД/ФТ цикл обновления — частая точка отказа. Идентификация при подключении проходит через шлюз с интеграциями: ЕСИА, ЕБС, проверка по реестрам, формирование профиля. Обновление по графику ведётся в отдельной очереди задач, куда запись клиента поступает по таймеру перед контрольной датой. Очередь распределяется по аналитикам KYC/KYB-команды и при высокой нагрузке откладывается. В сегменте среднего риска годовой интервал переносит работу на конец периода, и декабрьское обновление становится массовой кампанией с низким качеством разбора.

В реестре клиентских профилей у каждого клиентского профиля хранятся дата последнего обновления и контрольный срок следующего. Триггер создаёт задачу за две-четыре недели до контрольной даты. Без таймера в записи клиента обновление превращается в годовой отчёт, а годовой отчёт — в предписание регулятора.

26.5 Платформа «Знай своего клиента»

Банк России с июля 2022 года ведёт собственную платформу оценки риска юридических лиц и ИП — «Знай своего клиента», ЗСК. Каждый клиент получает зону риска: зелёная — без ограничений, жёлтая — усиленное наблюдение, красная — строгие ограничения вплоть до отказа в обслуживании и расторжения договора банковского счёта [567]. Оценка строится на совокупности признаков: профиль операций, контрагенты, отраслевая принадлежность, история регулятивных обращений, связи с уже маркированными лицами.

С 1 октября 2024 года Банк России открыл бесплатный публичный доступ к сервису проверки контрагентов, прежде доступному только кредитным организациям [568]. Любая компания может запросить категорию ЗСК потенциального контрагента, и часть KYB-проверки переходит к самим ТСП. Контрагент в красной зоне — маркер высокого риска для продавца независимо от внутреннего KYB; контрагент в жёлтой зоне требует расширенной проверки документов и внеочередного обновления профиля.

Для банка ЗСК работает как внешний источник данных для внутреннего RBA: категория поступает от Банка России асинхронно, и оператор сравнивает её с собственной KYB-оценкой клиента. Расхождения разбирают вручную: если банк присвоил клиенту низкий риск, а ЗСК отнесла его к красной зоне, оператор обязан пересмотреть профиль и провести дополнительные процедуры по 115-ФЗ. Обратный сценарий (клиент в зелёной зоне ЗСК, но банк нашёл признаки высокого риска) не даёт оснований снизить уровень риска: окончательный уровень присваивает банк по правилам внутреннего контроля [567]. Пока банк держит клиента в группе низкого риска, 115-ФЗ запрещает отказывать ему в переводах низкорисковым юрлицам и ИП; при подозрении в отмывании доходов или финансировании терроризма отказ допустим, но не позднее следующего рабочего дня банк обязан изменить клиенту уровень риска (ст. 7.7) [351].

В сентябре 2025 года Банк России анонсировал аналог ЗСК для физических лиц, направленный на снижение числа ошибочных блокировок счетов добросовестных клиентов. Для реестра клиентских профилей это та же модель: платформа с централизованным реестром оценок риска, доступом для кредитных организаций и асинхронным потоком обновления категорий. ЗСК для физлиц использует ту же интеграционную точку реестра клиентских профилей, что и текущая ЗСК для юрлиц, но с отдельной таблицей и собственной классификацией.

26.6 KYC/KYB как готовый сервис

Большинство команд покупает KYC как готовый сервис: сегмент *compliance-as-a-service* предоставляет идентификацию физлиц и юрлиц через единый API: верификация документа с селфи-фотофиксацией, биометрическое сравнение, проверка по санкционным спискам и спискам PEP, сверка по реестрам юридических лиц. Одна интеграция даёт доступ к десяткам источников данных, которые иначе пришлось бы подключать поочерёдно.

Среди крупных провайдеров — Sumsub [569], зарегистрированный в Лондоне в 2015 году выходцами из Санкт-Петербурга под маркой Sum & Substance: первые клиенты приходили из СНГ, сейчас платформа обслуживает банки и финтехи в десятках юрисдикций. ComplyAdvantage [570] — лондонская платформа финмониторинга: санкционная проверка (*sanctions screening*), мониторинг транзакций (*transaction monitoring*) и поиск негативных упоминаний (*adverse media*) в одном API. На западных рынках в том же классе работают Jumio, Onfido, Persona — с акцентом на верификацию документов и биометрию.

Выбор «разработать или купить» зависит от объёма потока, профиля риска клиентского сегмента и цены ошибки. Готовый сервис покрывает 80–90 % типовых сценариев и ускоряет прохождение регуляторных проверок; собственный конвейер оправдан там, где стандартные правила провайдера не покрывают специфику клиентского потока и рисков — у крупных банков с собственным аппетитом к риску и у финтехов, чей основной продукт — собственно идентификация.

26.7 Travel Rule для VASP

Recommendation 16 FATF (Travel Rule) переносит требование KYC из банковского периметра в криптообмены. VASP (*Virtual Asset Service Provider* — криптобиржа, кастодиальный кошелёк, OTC-деск) обязан при переводе криптоактивов между двумя VASP передавать получающей стороне набор атрибутов отправителя и получателя: имя, адрес, идентификатор кошелька, иногда дата рождения. Данные передаются вне блокчейна (*off-chain*) параллельно с ончейн-транзакцией, например через TRP или Sumsub Travel Rule; получающий VASP использует их для санкционной проверки и ведения журнала аудита.

К 2025 году Recommendation 16 внедрили 85 юрисдикций, ещё 14 готовят внедрение [571]. Порог применения различается: в ЕС — 0 евро (применяется к любой сумме), в Великобритании требование действует с любой суммы, но ниже 800 фунтов стерлингов трансграничный перевод сопровождают только имя и номер счёта [572], в США — $3000, в большинстве других юрисдикций — эквивалент $1000. В ЕС действует с 30 декабря 2024 года EU *Transfer of Funds Regulation* (TFR, регламент 2023/1113) вместе с финальными руководящими указаниями (*guidelines*) EBA от июля 2024 года [573].

Для российского PSP, работающего с криптоэквайрингом через зарубежных VASP-партнёров, это означает дополнительное KYC-требование на стороне партнёра. VASP-партнёр запрашивает у PSP атрибуты плательщика по Travel Rule до зачисления криптоактива; если данные неполны или не прошли санкционную проверку получающей стороны, перевод останавливается. Российское законодательство Recommendation 16 не закрепило, поэтому трансграничную операцию определяют требования партнёра в зарубежной юрисдикции.

27 ПОД/ФТ

ПОД/ФТ — противодействие легализации (отмыванию) доходов и финансированию терроризма; 115-ФЗ объединяет эти два направления контроля. Банковская функция, исполняющая эти обязательства — мониторинг операций, формирование ФЭС, разбор сигналов, — называется финмониторингом (*anti-money laundering*, AML в англоязычной практике). Платёжный комплаенс по ПОД/ФТ опирается на 115-ФЗ, подзаконные акты Банка России и Росфинмониторинга.

Международные стандарты заданы FATF (*Financial Action Task Force*, Группа разработки финансовых мер борьбы с отмыванием денег) [574], а для СНГ (Содружество Независимых Государств) ту же методологическую функцию выполняет ЕАГ — Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма [575]; подробнее см. раздел 27.4.

27.1 115-ФЗ и платёжный бизнес

Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» — основа контроля ПОД/ФТ в России [351]. Закон требует от оператора знать клиента, контролировать операции и при формальных основаниях блокировать средства.

Закон различает полную и упрощённую процедуру идентификации (УПРИД), а подзаконные акты Банка России задают состав сведений и документов по клиенту, представителю, выгодоприобретателю и бенефициарному владельцу [546]. В одних случаях хватает регистрационных данных, в других нужны документы, внешние реестры и дополнительные вопросы. Объём проверки зависит от типа клиента, операции и уровня риска; пороги и частные исключения регулятор пересматривает быстрее, чем выходит редакция книги, поэтому здесь они не фиксируются. Идентификация физлиц и ТСП подробно разобрана в гл. 26.

При мониторинге финансовых операций система выявляет операции, подпадающие под критерии обязательного контроля, и отправляет сведения в Росфинмониторинг. Кроме того, оператор выявляет операции, которые закон прямо не описывает, но которые выбиваются из нормального профиля клиента по поведению или контексту. Для этого нужны регламент, поток данных, порядок проверки и понятное решение по результату; контроль по одним формальным критериям даёт слепые зоны или перегружает очередь ложными срабатываниями.

Обязательный контроль по статье 6 115-ФЗ применяется к закрытому перечню операций [351]. По сумме базовый порог 1 000 000 руб. работает для операций с наличными у юрлиц (внесение и снятие со счёта), для покупки наличной валюты физлицом и для ряда смежных категорий; для зачислений на отдельные счета по гособоронзаказу порог — 600 000 руб., для почтовых переводов — 100 000 руб. Для сделок с недвижимостью закон задаёт только нижний предел 5 000 000 руб.; действующие пороги устанавливает Приказ Росфинмониторинга от 26.01.2026 № 13 «О порогах обязательного контроля сделок с недвижимостью» [576]: для кредитных организаций — 75 000 000 руб., для посредников по сделкам купли-продажи — 5 000 000 руб.[2] По виду операция попадает в обязательный контроль независимо

[2] В силе с 10.03.2026; ранее в самом законе действовал единый порог 5 000 000 руб.

от суммы, когда сторона находится в перечне лиц, причастных к экстремизму или терроризму, либо в смежных перечнях Росфинмониторинга. Контроль подозрительных операций по статье 7 обязывает оператора выявлять необычные и подозрительные операции по собственным правилам внутреннего контроля; именно эту работу выполняет программа выявления операций в ПВК.

Сведения направляются в Росфинмониторинг через личный кабинет — формализованным электронным сообщением (ФЭС). Сроки задают 115-ФЗ и нормативные акты Банка России и Росфинмониторинга [351, 577, 578].

Порядок представления ФЭС кредитной организацией задаёт Указание Банка России от 17.06.2025 № 7081-У «О представлении кредитными организациями сведений в Росфинмониторинг» [578]; для некредитных организаций тот же порядок задаёт Приказ Росфинмониторинга от 08.02.2022 № 18 «О представлении в Росфинмониторинг информации по 115-ФЗ» в действующей редакции [579]. Требования к ПВК, на которые опирается логика выявления, устанавливает 860-П [577]. В инфраструктуре сборка ФЭС идёт последовательно: программа выявления формирует запись с кодом сработавшего критерия; программа документального фиксирования дополняет её реквизитами клиента и контрагента из программы идентификации; сборщик ФЭС преобразует результат в формализованное сообщение к моменту отправки. Если поле клиента в платёжном журнале не заполнено или не нормализовано, ФЭС не будет сформировано. Поэтому качество этих полей проверяют заранее, до срабатывания критерия.

В международной практике той же цели служат сообщения SAR (*Suspicious Activity Report*) и STR (*Suspicious Transaction Report*), направляемые в национальный финансово-разведывательный орган — например, FinCEN в США. По функции они эквивалентны российскому ФЭС; по составу полей и регламенту подачи прямого соответствия форм нет.

Если клиент или бенефициар попадает в перечни лиц, связанных с терроризмом или экстремизмом, организация обязана применить меры по замораживанию и исполнить предусмотренный законом порядок информирования [351]. Технология сопоставления имён и передачи на проверку разобрана в гл. 28.

Правила внутреннего контроля по 860-П

Идентификацию, мониторинг и блокировку банк оформляет в единый рабочий регламент — правила внутреннего контроля (ПВК). Положение Банка России от 18.06.2025 № 860-П «О требованиях к ПВК по ПОД/ФТ»[1] задаёт действующий состав ПВК [577].

ПВК по 860-П состоит из нескольких связанных программ. Программа **идентификации** клиента, представителя, выгодоприобретателя и бенефициарного владельца отвечает на вопрос, с кем банк работает и какие сведения о нём фиксирует. Программа **управления риском** задаёт классификатор клиентов и операций по уровням риска и пересмотр этих уровней по событиям. Критерии срабатывания, на которые опирается мониторинг, описывает программа **выявления операций** — обязательного контроля по ст. 6, подозрительных по ст. 7 и подозрительной деятельности. Состав сведений, формат и сроки хранения каждого решения закрепляет программа **аудита**. Учебный цикл сотрудников по ПОД/ФТ задаёт программа **обучения**; регламент самопроверки и регулярный отчёт ответственного сотрудника — программа **проверки внутреннего контроля**.

[1] В силе с 13.08.2025; заменило 375-П. К 12.11.2025 кредитные организации обязаны были привести ПВК к новому составу.

В коде это разделение сохраняется. Программа выявления операций реализуется в модуле классификатора, где объединяются пороги статьи 6, признаки подозрительных операций статьи 7 и набор перечней лиц, к которым применяется обязательный контроль независимо от суммы. Журнал аудита фиксирует решение и стабильный код причины, по которому это решение принято — иначе разбор возражения клиента, запрос регулятора или ретроспективная оценка правил превращается в ручной поиск по журналам.

В примере классификатора `classify` работает с минимальной доменной моделью: на вход подаётся `Operation` с суммой, категорией, клиентом и контрагентом, причём клиент — собственный тип `Client` с id и уровнем риска (рисковый профиль — динамическое свойство клиента, а не отдельной транзакции). На выходе возвращается `Verdict` с решением и кодом причины. Для иллюстрации перечень категорий ст. 6 приводится условно, а RBA-ветка сведена к булевой проверке уровня риска клиента с коэффициентом 1/2 от порога; в рабочей системе оба значения берёт программа управления риском:

```
def classify(op: Operation, sanctioned: frozenset[str]) → Verdict:
  # Сторона из перечня экстремистов/террористов: обязательный контроль
  # независимо от суммы (статья 6 пункт 1.1, абзац о перечне).
  party_in_list = op.client.id in sanctioned or (
    op.counterparty_id is not None and op.counterparty_id in sanctioned
  )
  if party_in_list:
    return Verdict(Decision.MANDATORY, "party_in_list")

  threshold = _threshold(op.kind)

  # Сумма + категория операции: обязательный контроль по статье 6.
  if op.kind in _KINDS_WITH_MANDATORY and op.amount_kopecks >= threshold:
    return Verdict(Decision.MANDATORY, f"threshold:{op.kind.value}")

  # Risk-based approach: для высокорискового клиента нижняя граница
  # подозрительности сдвинута к половине формального порога. Конкретный
  # коэффициент задаёт программа управления риском в ПВК.
  if op.client.risk == "high" and op.amount_kopecks >= threshold // 2:
    return Verdict(Decision.SUSPICIOUS, "rba:high_risk_client")

  return Verdict(Decision.NORMAL, "below_threshold")
```

Разделение статьи 6 и статьи 7 в коде представлено ветками: обязательный контроль по сумме и категории операции (ст. 6), участник из перечня (тоже ст. 6) и подозрительная операция по правилу из ПВК (ст. 7). Каждая ветка сохраняет стабильный код причины (`threshold:cash_deposit`, `party_in_list`, `rba:high_risk_client`) в Verdict. В программе документального фиксирования по 860-П коды другие, эти условны.

ПВК — внутренний документ организации, но Банк России и Росфинмониторинг проверяют в нём наличие всех программ в действующей редакции и соответствие правил тому, как работает система. Неполнота правил или расхождение между документом и работающей системой — типовые основания предписаний по ПОД/ФТ.

Риск-ориентированный подход

Программа управления риском в 860-П требует от банка применять риск-ориентированный подход (в англоязычных документах – *risk-based approach*, RBA) во всех процедурах ПОД/ФТ. Принцип RBA изначально сформулирован в Рекомендации 1 FATF и развёрнут в отраслевом руководстве FATF для банковского сектора (октябрь 2014 года) [574, 580]. В российской нормативной базе принципы,

аналогичные RBA, закреплены в 499-П (идентификация и оценка риска клиента) [546] и 860-П (применение оценки к мониторингу и выявлению подозрительных операций) [577].

При RBA от уровня риска клиента зависят глубина сбора сведений на входе, чувствительность мониторинга и цикл пересмотра данных. Для низкого риска оператор обходится минимальным набором сведений, для высокого запрашивает расширенный пакет, привлекает внешние источники и оценивает структуру владения. По мере роста риска порог выявления подозрительных операций сдвигается к меньшим суммам, а правила срабатывают на большем числе ситуаций. Цикл обновления данных и пересмотра уровня для высокого риска короче, чем для низкого (см. раздел 26.4).

В примере выше RBA проявляется веткой `rba:high_risk_client`: операция, формально не дотягивающая до порога обязательного контроля, для высокорискового клиента попадает в очередь подозрительных. Коэффициент (половину, треть, четверть формального порога) закон не устанавливает, его задаёт программа управления риском. ПВК документирует коэффициент и обоснование, журнал аудита фиксирует, что решение принято именно по этой ветке. На запрос регулятора банк предъявляет конкретный коэффициент и конкретную запись журнала, а не формулу «мы внимательно смотрим за высокорисковыми клиентами».

Алгоритмы детекции дробления

Программа выявления операций совмещает формальные критерии статьи 6 и поведенческие схемы. Самая частая из них — дробление (*structuring*): клиент разбивает крупную сумму на несколько операций ниже порога, чтобы избежать формального обязательного контроля.

Методические рекомендации Банка России от 21.07.2017 № 19-МР «О снятии наличных по корпоративным картам юрлиц и ИП» рекомендуют кредитным организациям проводить «не реже одного раза в неделю мониторинг операций»; среди признаков названы поступления на счёт «суммами, как правило, не превышающими 600 тыс. рублей» и снятие наличных в сумме ниже того же порога [581]. Парные Методические рекомендации от 21.07.2017 № 18-МР «О подходах к управлению риском ПОД/ФТ» задают общий подход к RBA в этой работе [582]; Методические рекомендации Банка России от 29.02.2024 № 4-МР «Об усилении контроля за операциями физических лиц» расширяют его на переводы физлиц [583]. Конкретные коды необычных операций, по которым формируется ФЭС кредитной организации, перечислены в приложении к 860-П [577].

19-МР задаёт частоту мониторинга (не реже раза в неделю) и оставляет выбор алгоритма банку. Типовые формы дробления выявляют правила со скользящими окнами: накопление мелких переводов по одному счёту; веер от одного отправителя многим получателям; зеркальный веер от многих отправителей одному получателю.

У этих правил общий интерфейс. Метод `observe` принимает `Event` (поля `ts`, `source`, `destination`, `amount_kopecks`) и возвращает `None` либо `StructuringHit` с типом срабатывания (`sub_threshold`, `fan_out`, `fan_in`) и счётом, по которому зафиксировано срабатывание. Источник времени правило не задаёт: рабочий код передаёт в `ev.ts` результат `time.monotonic()`, тест — любую монотонно возрастающую последовательность секунд.

```
from collections import defaultdict, deque
from dataclasses import dataclass, field
```

(продолжение)

```
from typing import Literal

HARD_THRESHOLD_KOPECKS = 1_000_000_00  # статья 6 115-ФЗ
HALF_THRESHOLD_KOPECKS = 500_000_00


@dataclass(frozen=True)
class Event:
  ts: float  # секунды от эпохи; источник времени -- параметр вызывающей системы
  source: str  # счёт отправителя
  destination: str  # счёт получателя
  amount_kopecks: int


Kind = Literal["sub_threshold", "fan_out", "fan_in"]


@dataclass(frozen=True)
class StructuringHit:
  kind: Kind
  key: str  # счёт, по которому сработал паттерн (source или destination)
  count: int
  total_amount_kopecks: int
  window_sec: float
```

Sub-threshold velocity — индекс по одному счёту-источнику с подсчётом числа операций и общей суммы в окне. Срабатывает, когда за окно (обычно неделя, как у недельной доли наличных в 19-MP, иногда сутки или час у активных каналов) накапливается N операций общей суммой выше параметра ПВК (обычно равного порогу обязательного контроля по ст. 6) при том, что каждая отдельная операция меньше порога ст. 6. Англоязычная литература называет это «микроструктурированием» (*microstructuring*) — дроблением до уровня, на котором отдельный платёж не пересекает порог отчётности. Схема возникла как ответ на порог отчётности $10 000 по Bank Secrecy Act США 1970 года [584]; уголовным деянием дробление в США сделал Money Laundering Control Act 1986 года (31 U.S.C. 5324) [585].

```
@dataclass
class SubThresholdVelocity:
  window_sec: float
  sum_threshold_kopecks: int
  count_threshold: int
  hard_threshold_kopecks: int = HARD_THRESHOLD_KOPECKS
  _by_source: defaultdict[str, deque[Event]] = field(
    default_factory=lambda: defaultdict(deque)
  )

  def observe(self, ev: Event) -> StructuringHit | None:
    # Операция >= порога обязательного контроля идёт по ст. 6
    # отдельным потоком, не накапливается в детекторе дробления.
    if ev.amount_kopecks >= self.hard_threshold_kopecks:
      return None
    timeline = self._by_source[ev.source]
    cutoff = ev.ts - self.window_sec
    while timeline and timeline[0].ts < cutoff:
      timeline.popleft()
    timeline.append(ev)
    total = sum(e.amount_kopecks for e in timeline)
    if len(timeline) >= self.count_threshold and total >= self.sum_threshold_kopecks:
      return StructuringHit(
        kind="sub_threshold",
        key=ev.source,
        count=len(timeline),
        total_amount_kopecks=total,
        window_sec=self.window_sec,
      )
    return None
```

Fan-out — один счёт-источник за короткий срок переводит небольшие суммы на много разных счетов. Это смурфинг (*smurfing*) через подставные счета: реальный

плательщик проводит поток через смурфов — людей, на чьё имя преступники открывают счета на короткий срок, чтобы разорвать видимую связь между источником средств и их назначением [584].

В ранних правилах пары отправитель–получатель учитывались порознь: переводы A → B и A → C попадали в разные счётчики. Fan-out агрегирует поток по одному отправителю независимо от получателя; суммы выше половины порога ст. 6 правило игнорирует — такие операции заметны и поодиночке.

```
@dataclass
class FanOut:
  window_sec: float
  distinct_destinations_threshold: int
  amount_threshold_kopecks: int = HALF_THRESHOLD_KOPECKS
  _by_source: defaultdict[str, deque[Event]] = field(
    default_factory=lambda: defaultdict(deque)
  )

  def observe(self, ev: Event) → StructuringHit | None:
    if ev.amount_kopecks >= self.amount_threshold_kopecks:
      return None
    timeline = self._by_source[ev.source]
    cutoff = ev.ts - self.window_sec
    while timeline and timeline[0].ts < cutoff:
      timeline.popleft()
    timeline.append(ev)
    distinct = {e.destination for e in timeline}
    if len(distinct) >= self.distinct_destinations_threshold:
      return StructuringHit(
        kind="fan_out",
        key=ev.source,
        count=len(distinct),
        total_amount_kopecks=sum(e.amount_kopecks for e in timeline),
        window_sec=self.window_sec,
      )
    return None
```

Fan-in — зеркальная схема: много разных счетов-источников переводят небольшие суммы на один счёт-получатель. Та же логика смурфинга с противоположной стороны: смурфы получают мелкие суммы из разных источников и сводят их на один контролируемый счёт получателя. Индекс строится по получателю; отсечка по сумме та же, что в fan-out.

```
@dataclass
class FanIn:
  window_sec: float
  distinct_sources_threshold: int
  amount_threshold_kopecks: int = HALF_THRESHOLD_KOPECKS
  _by_destination: defaultdict[str, deque[Event]] = field(
    default_factory=lambda: defaultdict(deque)
  )

  def observe(self, ev: Event) → StructuringHit | None:
    if ev.amount_kopecks >= self.amount_threshold_kopecks:
      return None
    timeline = self._by_destination[ev.destination]
    cutoff = ev.ts - self.window_sec
    while timeline and timeline[0].ts < cutoff:
      timeline.popleft()
    timeline.append(ev)
    distinct = {e.source for e in timeline}
    if len(distinct) >= self.distinct_sources_threshold:
      return StructuringHit(
        kind="fan_in",
        key=ev.destination,
        count=len(distinct),
        total_amount_kopecks=sum(e.amount_kopecks for e in timeline),
        window_sec=self.window_sec,
      )
    return None
```

Каждое правило поддерживает индекс по своему ключу: `SubThresholdVelocity` и `FanOut` индексируют по `source`, `FanIn` — по `destination`. Окна не зависят друг от друга, и срабатывание одного правила не мешает другому: один и тот же поток может одновременно сформировать `sub_threshold` (по сумме за неделю) и `fan_out` (по числу получателей за тот же интервал).

ВАЖНО

Часто путают «смурфов» и «дропперов», потому что все они временно предоставляют свои счета для незаконных финансовых потоков. Но за смурфом стоят нелегальные доходы (наркотики, коррупция, теневой оборот), которые отмываются — этим занимается финмониторинг по 115-ФЗ. Дроппер же принимает деньги, украденные у жертв через фишинг и социальную инженерию, и переводит их дальше; его разбирает антифрод по 161-ФЗ и 851-П, а законодательный ответ закреплён в 44-ФЗ (см. раздел 27.3). Детектор fan-out/fan-in/sub-threshold выявляет обе схемы одинаково; различается дальнейший разбор — смурфинг передаётся финмониторингу, дропперство — антифроду.

Графовые модели расширяют анализ. Метод GARG-AML (*Graph-Aided Risk Grading for Anti-Money Laundering*, 2025) строит матрицу смежности окружения счёта второго порядка, измеряет плотность (*density-based*) её блоков и оценивает, насколько структура похожа на эталонные схемы смурфинга scatter-gather и gather-scatter [584]. Правила выше выявляют дробление на одном переходе (источник раздаёт получателям или собирает от них), GARG-AML распознаёт цепочки от A через посредников к B, где каждый отдельный шаг подпороговый, но связность графа выдаёт намерение. Цена такого подхода — поддержание обновляемого графа платежей и снижение интерпретируемости вывода. В сложных системах графовая (*graph-based*) надстройка дополняет правила (*rule-based*).

Каждая сработавшая схема попадает в ту же очередь ручного разбора, что и операции обязательного контроля по ст. 6 (раздел 27.2): алгоритм создаёт запись с кодом причины (`sub_threshold`, `fan_out`, `fan_in`), её разбирает аналитик первого уровня, а дело передаётся на второй. Без калибровки RBA доля ложноположительных результатов при поиске дроблений особенно высока: интенсивность, которая для одного клиента — нормальный поток, для другого — явная схема обхода порога.

Банк России при надзоре за кредитной организацией проверяет рабочую систему ПОД/ФТ целиком: формальные правила, подготовку сотрудников и порядок обработки выявленных случаев.

27.2 Ложные срабатывания финмониторинга

Программа выявления операций неизбежно даёт ложные сигналы. Доля ложных срабатываний (*false positives*, FP) в финмониторинге у банков по оценке вендоров доходит до 95 % от общего числа сигналов [586], а для систем на одних правилах исследователи приводят 95–98 % [587]; конкретные цифры оператор не раскрывает, порядок виден по отчётам вендоров и консультантов (Nice Actimize, FICO TONBELLER, SAS, Oracle FCCM). Низкая базовая частота настоящего отмывания делает поток FP ожидаемым результатом любой достаточно чувствительной программы выявления.

Сработавший сигнал задерживает операцию до решения аналитика, пока средства не списаны со счёта плательщика: с момента списания перевод безотзывен (ст. 5 ч. 7 161-ФЗ) [1]. Приостановление на пять рабочих дней по ст. 7 п. 10 115-ФЗ связано только с мерами замораживания и перечнями и не распространяется на зачисление на счёт; по собственному подозрению банк вправе отказать в операции (ст. 7 п. 11), причём до наступления безотзывности перевода по 161-ФЗ

(ст. 7 п. 11.1) [351]. Аналитик первого уровня разбирает запись журнала: собирает базовый контекст (профиль клиента, история операций, связанные стороны, внешние источники) и либо закрывает разбор как FP с кодом причины в журнале (тогда операция исполняется), либо передаёт его на второй уровень (операция остаётся задержанной).

Второй уровень ведёт углублённую проверку (*enhanced due diligence*, EDD): запрашивает у клиента документы по операции, проверяет связанные счета, сверяется с накопленными ранее данными. По итогам аналитик второго уровня готовит ФЭС в Росфинмониторинг или меру по 115-ФЗ (отказ в проведении операции, замораживание средств) и передаёт на подпись ответственному сотруднику по ПОД/ФТ; либо закрывает дело как FP.

Скорость обработки зависит от характера операции. Подозрение на финансирование терроризма требует немедленного разбора. Разбор операции по правилу мониторинга в стандартном случае закрывается за 1–3 рабочих дня; столько ждёт только распоряжение, по которому средства ещё не списаны, а уровень риска клиента периодически пересматривают по графику программы управления риском. Сроки задаёт операционный риск: каждый день задержки увеличивает вероятность клиентской жалобы. После наступления безотзывности перевода отказ в проведении операции уже невозможен; после этого остаются только направление ФЭС в Росфинмониторинг и решение о прекращении обслуживания клиента. Замораживание — отдельная мера по ст. 7 п. 1 подп. 6: применяется только при попадании клиента или контрагента в перечень лиц, причастных к экстремизму или терроризму.

Скрытое снижение чувствительности быстро разгружает очередь, но за квартал может довести систему до регуляторного нарушения. Сдвиг порога вверх без обновления оценки риска сокращает FP, но одновременно сокращает число выявленных настоящих случаев. Регулятор оценивает эффективность программы выявления: долю ФЭС, приведших к делам, и меры замораживания по результатам собственного мониторинга. Программа, в которой за квартал не направлено ни одного ФЭС, требует такого же объяснения, как и программа, направившая сто тысяч.

Устойчивый способ снизить FP — добавлять признаки в оценку риска и адаптировать правила под новые источники: признаки необычных операций из приложения к 860-П [577], информационные письма и типологии Росфинмониторинга, типологические исследования ЕАГ. Чем точнее калибровка RBA, тем меньше шума и тем больше выявленных реальных случаев. Пороги калибруются в программе управления риском, а оба уровня применяют уже настроенные правила: первый закрывает разбор или передаёт его на второй, второй ведёт EDD и готовит ФЭС.

ПРАКТИКА

Очередь финмониторинга лучше измерять в часах обработки: эта мера прямо показывает запас до регуляторных сроков. Если очередь растёт быстрее найма аналитиков, начнутся просрочки и рост отказов по необработанным операциям.

27.3 Отзыв лицензии у КИВИ Банка

Банк России отозвал лицензию у КИВИ Банка приказом от 21.02.2024 № ОД-266 [541]. В официальном пресс-релизе регулятор указал на систематические нарушения требований законодательства по ПОД/ФТ, вовлечённость банка в высокорисковые операции, включая переводы в пользу криптообменников и нелегальных

онлайн-казино, а также на случаи открытия кошельков QIWI с использованием персональных данных граждан без их ведома.

115-ФЗ требует от банков идентифицировать клиентов и проводить контроль операций; открытие кошельков без ведома граждан означает, что процедура идентификации либо не выполнялась, либо не проверялась системой контроля. Переводы в пользу криптообменников и казино становятся проблемой тогда, когда мониторинг транзакций (автоматическая проверка операций по наборам правил и скоринговым моделям) не маркирует их как высокорисковые или маркирует, но сигнал не передаётся на ручной разбор. В системе оба сбоя видны как отсутствие автоматического правила усиленной проверки клиента или неполный журнал аудита по спорным транзакциям.

ВАЖНО

Законодательный ответ на ту же практику — Федеральный закон от 20.02.2026 № 44-ФЗ «Об ограничении идентификации физических лиц банковскими платёжными агентами» [53]: с 03.03.2026 БПА не вправе проводить идентификацию и упрощённую идентификацию физлиц, в том числе для переводов электронных денежных средств и предоставления ЭСП. Пояснительная записка опирается на выявленные Банком России случаи незаконного использования персональных данных для открытия кошельков без ведома граждан и на борьбу с дропперством. Идентификация физлица возвращена в банк; БПА-агрегатор по ст. 14.1 161-ФЗ сохраняет идентификацию ЮЛ/ИП-субмерчантов.

Операционный риск ПОД/ФТ для платёжного бизнеса шире штрафов: отзыв лицензии у ключевого расчётного банка сразу останавливает каналы приёма и выплат у всех его клиентов. Бизнесу с зависимостью от одного платёжного провайдера нужен заранее проверенный план непрерывности — альтернативный провайдер, резервные счета и порядок переключения.

27.4 FATF и ЕАГ для СНГ

FATF задаёт международные стандарты через рекомендации, взаимные оценки и публичные списки юрисдикций под усиленным наблюдением [574, 588]. С 24 февраля 2023 года членство Российской Федерации в FATF приостановлено [589]: это означает, что Россия не участвует в выработке решений FATF, не направляет своих представителей в её рабочие группы и не подвергается очередным взаимным оценкам в стандартном порядке. В СНГ функции региональной *FATF-style body* (организации, действующей по методологии FATF) выполняет ЕАГ. Она проводит взаимные оценки государств региона и публикует методологические документы, на которые опираются национальные регуляторы стран СНГ [575, 590].

После приостановки членства стандарты FATF продолжают влиять на платёжный бизнес в России косвенно. Банки-корреспонденты и платёжные посредники в третьих юрисдикциях оценивают риск через рекомендации FATF и публичные списки. Крупные банки практикуют «*de-risking*»: сокращают или полностью прекращают отношения с целыми классами клиентов и юрисдикций вместо точечного управления риском по каждому отношению [591]. Для российского оператора это означает усложнение открытия и поддержания корреспондентских счетов в валютах недружественных стран — дополнительные проверки на стороне контрагента и снижение доступности канала.

ПРАКТИКА

Перед выходом в новую юрисдикцию проверяют оценку ЕАГ для стран СНГ либо FATF для остальных, последнюю публичную взаимную оценку страны и местную практику ПОД/ФТ. Если оценка или практика вызывает сомнение, заранее закладывается запас по времени и каналам расчёта.

27.5 Блокчейн-аналитика для AML за рубежом

Блокчейн-аналитика отвечает на вопрос, на который у банка нет источника в банковской платёжной телеметрии: связан ли криптокошелёк, с которого пришли средства, с миксером (*mixer* — сервис анонимизации криптоактивов), даркнет-площадкой, оплатой вымогателям (*ransomware*) или санкционным адресом.

Рынок ведут **Chainalysis**, **Elliptic** и **TRM Labs**. Chainalysis — крупнейший по охвату, основной поставщик аналитики для IRS-CI и FBI; в 2022 году выделил подразделение Chainalysis Government Solutions для работы с американскими ведомствами [592]. Elliptic (Лондон, основана в 2013 году) декларирует мониторинг около 98 % криптоактивов по рыночной капитализации; основные клиенты — банки и финразведки Великобритании и ЕС. TRM Labs (Сан-Франциско, 2018 год) в феврале 2026 года оценён в $1 млрд по раунду Series C под Blockchain Capital [593]; развивает ИИ-скоринг и трассировку между блокчейнами (*cross-chain*) в реальном времени.

Инструменты ведут таблицу связей адресов по собственной кластеризации (объединение адресов, контролируемых одним кошельком) и открытым типологиям (известные миксеры, биржи, адреса криминальных сервисов). Клиент передаёт вендору адрес контрагента и получает оценку риска и метки источника, не раскрывая отдельные операции. Результат добавляется в авторизационный или послеавторизационный мониторинг наравне с профилем клиента и атрибутами контрагента.

Спрос поддерживают регуляторные требования. В ЕС с 30.12.2024 применяется Регламент (ЕС) 2023/1113 о переводах криптоактивов [594] — адаптация *travel rule* FATF (Рекомендация 16) к европейскому рынку. Порог FATF $1 000 регламент не перенял: поставщики услуг с криптоактивами (CASP в европейской терминологии — эквивалент VASP, *virtual asset service provider*, в терминах FATF) передают данные отправителя и получателя при переводе любой суммы [573], а инструменты DLT-аналитики и оценка KYT (*know your transaction*) названы в регламенте среди предметов его пересмотра. Параллельно действует MiCA — Регламент (ЕС) 2023/1114 о рынке криптоактивов [595].

OFAC включил Tornado Cash в санкционный список SDN 8 августа 2022 года [596]; американские банки и биржи обязаны были блокировать любые взаимодействия с адресами миксера, а выявить такие переводы можно только через блокчейн-аналитику. В ноябре 2024 года Апелляционный суд пятого округа (*Fifth Circuit*) постановил, что неизменяемые смарт-контракты Tornado Cash не являются «собственностью» в смысле санкционного закона и санкции против них недействительны; OFAC исключил Tornado Cash из SDN 21 марта 2025 года. Метки риска в блокчейн-аналитике после исключения не изменились: средства, прошедшие через миксер, по-прежнему помечаются как высокорисковые: прохождение через миксер от санкционного статуса не зависит.

28 Санкционная проверка

У санкционной проверки (*sanctions screening*) собственные перечни, алгоритмы сравнения, пороги ложных срабатываний и маршрут эскалации; к ПОД/ФТ она не сводится. ОПДС работает с национальными перечнями Росфинмониторинга и решениями Межведомственной комиссии (МВК) при Росфинмониторинге; международные перечни (Управление по контролю над иностранными активами Министерства финансов США, «Office of Foreign Assets Control», OFAC; Европейский союз, EU; Организация Объединённых Наций, UN) применяются по собственной политике ОПДС и требованиям банков-корреспондентов. Если клиент, бенефициар или контрагент попадает в применимый перечень, операцию останавливают до исполнения.

Российский банк не может ограничиться национальными перечнями, даже если сам в списке SDN США не значится. Любой трансграничный расчёт проходит через банк-корреспондент в валюте перевода; ОПДС проверяет исходящие платежи, а банк-корреспондент повторно сверяет входящие сообщения с OFAC SDN, EU Consolidated и UK Sanctions List и обязан заблокировать средства при совпадении[2]. Пропущенное совпадение грозит остановкой операции и полным разрывом корреспондентских отношений. Механизм давления на корреспондентов разобран в разделе 28.2.

28.1 Национальные перечни

Для российского ОПДС — банка или НКО (см. гл. 25) — первичны три национальных источника. Главный — перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму; ведёт его Росфинмониторинг, а меры по замораживанию средств применяются по подпункту 6 пункта 1 статьи 7 115-ФЗ (см. гл. 27; операции с лицами из перечня дополнительно подлежат обязательному контролю по статье 6). Параллельно ведётся перечень лиц, в отношении которых имеются сведения об их причастности к распространению оружия массового уничтожения. Третий источник — решения МВК о замораживании (блокировании) денежных средств или иного имущества [351].[3]

Перечни Росфинмониторинга обновляются регулярно; после публикации обновлённого перечня ОПДС обязан незамедлительно, но не позднее 24 часов с момента размещения информации, сверить клиентов с обновлённым перечнем и применить меры к клиентам, попавшим в него [351, 597].[4]

[2] Именно входящая проверка на стороне корреспондента перекрывает канал для отправителя: миновать фильтр получателя невозможно. Технические попытки обойти его описаны в разделе 28.6.

[3] Точные наименования перечней, формат публикации и периодичность обновления сверяются по сайту Росфинмониторинга и по действующей редакции 115-ФЗ [597, 598].

[4] Срок установлен 115-ФЗ в редакции 462-ФЗ (в силе с 14.06.2026): заморозка в течение суток независимо от рабочего или выходного дня; специальные правила исчисления сроков, ранее установленные приказами Росфинмониторинга, отменены с 29.03.2026.

28.2 Международные перечни и их статус для ОПДС

ОПДС применяет перечни ООН, ЕС, OFAC SDN и прочие источники по собственной политике риска и требованиям банков-корреспондентов; национальные перечни эти источники не подменяют [316, 599, 600].

Платёж в валюте юрисдикции, применяющей санкции, проходит через банк-корреспондент, который соблюдает ограничения своей юрисдикции. Национальный закон может и не обязывать ОПДС проверять контрагента по OFAC SDN, но отказ корреспондента в исполнении всё равно остановит расчёт. Поэтому ОПДС включает международные перечни в собственную проверку ради устойчивости канала расчётов.

Executive Order 14114, подписанный 22 декабря 2023 года, дал OFAC право вводить вторичные санкции против иностранного финансового института за значительные транзакции в интересах российского военно-промышленного комплекса [317]. 15 января 2025 года OFAC впервые применил эту норму к киргизскому Керемет-Банку за обслуживание подсанкционного Промсвязьбанка [601]; с 31 декабря 2024 по 30 апреля 2025 года банк потерял свыше 40 % клиентских средств [602]. Турецкие банки в 2024 году разорвали корреспондентские связи почти со всеми российскими кредитными организациями [603]. Многим иностранным банкам оказалось дешевле выйти из российского направления полностью, чем проверять каждую транзакцию на риск вторичных санкций.

Помимо OFAC SDN, EU Consolidated и UN Consolidated, ОПДС, работающий с международными корреспондентами, сверяет клиентов и с другими самостоятельными перечнями.

Council Regulation (EC) No 2580/2001. Террористический список ЕС, обновляемый Советом не реже раза в шесть месяцев [604]. В него входят лица, организации и группы, причастные к терроризму; для них ЕС применяет заморозку активов и запрет на предоставление финансовых услуг отдельно от прочих санкционных списков ЕС.

UK Sanctions List. Единый британский список с 28 января 2026 года, заменивший прежний OFSI Consolidated List of Financial Sanctions Targets [605, 606]. Он объединяет финансовые, иммиграционные, торговые и транспортные санкции; по нему проверяют контрагентов корреспонденты, проводящие расчёты в фунтах.

DFAT Consolidated List. Австралийский сводный перечень, который ведёт Australian Sanctions Office при Department of Foreign Affairs and Trade. Подотчётные лица (*reporting entities*) по AML/CTF Act 2006 обязаны до предоставления услуги проверить, нет ли клиента и связанных лиц в списке: действующие подотчётные лица — с 31 марта 2026 года, новые подотчётные лица второго этапа реформы (*tranche 2*: юристы, бухгалтеры, риелторы) — с 1 июля 2026 года [607—609].

MAS Targeted Financial Sanctions. Сингапурский санкционный список на основании Financial Services and Markets Act 2022 и Terrorism (Suppression of Financing) Act 2002. Реализует резолюции Совета Безопасности ООН и собственные решения регулятора MAS; финансовые институты Сингапура обязаны замораживать активы лиц из списка без отдельного административного акта [610].

Состав перечней зависит от юрисдикций расчётов ОПДС: ограничения банка-корреспондента в валюте перевода важнее национального закона самого ОПДС.

SDN и SSI

Минфин США ведёт семейство санкционных перечней с разной правовой нагрузкой.

SDN (Specially Designated Nationals) — полная блокировка активов. Любая операция через юрисдикцию США или участников американской финансовой системы с лицом из списка SDN запрещена; американская организация обязана заморозить активы и отчитаться OFAC в течение 10 рабочих дней. SSI (Sectoral Sanctions Identifications) — секторальные санкции по Executive Order 13662: ограничения для отдельных секторов российской экономики заданы директивами [611, 612]. Активы лица из списка SSI не блокируются; запрещены конкретные категории операций по ограниченному составу инструментов.

Директива 1 (финансовый сектор) — новый долг сроком погашения свыше 14 дней (для долга, выпущенного с 28 ноября 2017 года; ранее — свыше 30 дней с 12 сентября 2014, свыше 90 дней с 16 июля 2014) или новое размещение акций (*equity*).

Директива 2 (энергетический сектор) — новый долг сроком свыше 60 дней (с 28 ноября 2017; ранее — свыше 90 дней). Акции не ограничены.

Директива 3 (оборонный сектор) — новый долг сроком свыше 30 дней. Акции не ограничены.

Директива 4 — запрет на поставку товаров, услуг (кроме финансовых) и технологий в поддержку разведки или добычи на глубоководных, арктических шельфовых и сланцевых проектах в России.

Санкционный фильтр обязан различать классы. Платёж `pacs.008` в евро с контрагентом из списка SSI по Директиве 1 проходит как обычная торговая операция; тот же контрагент по новому облигационному выпуску со сроком погашения 31 день — нет. Сопоставление превращается из бинарного в матрицу «лицо $\times$ тип операции $\times$ срок $\times$ продукт». Нарушения по SSI возникают из запрещённой схемы расчёта при контрагенте, который сам по себе допустим.

Правило 50 % OFAC

Юридическое лицо бывает заблокировано, даже когда его имя не даёт совпадения. Правило 50 % OFAC, в действующей редакции с 13 августа 2014 года, распространяет блокировку с явных записей в списке SDN на любую организацию, у которой одно или несколько таких лиц владеют 50 % или более суммарно: прямо, косвенно через цепочку промежуточных компаний или агрегированно по нескольким санкционным владельцам [613].

Компания X не в списке SDN; её 30 % владеет санкционное лицо A напрямую, ещё 25 % владеет санкционное лицо B через холдинг Y (контролируемый B на 80 %). Прямое и косвенное владение санкционными лицами суммируется: $30 + 25 \times 0{,}8 = 50\,\%$. Компания X заблокирована по правилу 50 %, хотя в списке SDN её нет, а явных владельцев A и B в публичных реестрах может вообще не быть.

OFAC не публикует производный список таких компаний; обязанность построить граф владения (*ownership graph*) возложена на ОПДС. Санкционная проверка выходит за пределы сопоставления имён (*name matching*) и требует той же работы по построению графа, что и KYB с идентификацией конечного бенефициарного владельца (*UBO*; см. раздел 26.3). Коммерческие провайдеры (LexisNexis, Refinitiv, Dow Jones, Sayari) поддерживают индексы владения; банк собирает такой граф по данным KYB и открытых реестров бенефициарных владельцев. Правило 50 %

Бюро промышленности и безопасности Минторга США (BIS) для экспортного контроля (*Affiliates Rule* от 29 сентября 2025 года) построено по аналогичной схеме, но применяется отдельно от правила OFAC; с 10 ноября 2025 по 9 ноября 2026 года его действие приостановлено [614].

14-й и 15-й пакеты ЕС

Платёжную инфраструктуру санкции ЕС затронули ещё в 2022 году: Регламент (EU) 2022/345 отключил ряд российских банков от SWIFT [615]. 14-й пакет ЕС от 24 июня 2024 года ввёл запрет для юрлиц ЕС вне России на использование Системы передачи финансовых сообщений Банка России (СПФС — российский аналог SWIFT) [616]. Тот же пакет ввёл новые механизмы: Annex XLIV — список пользователей СПФС из третьих стран, подпадающих под санкции автоматически при внесении; Annex XLV — механизм включения в список финансовых институтов и провайдеров криптоактивов из третьих стран, вовлечённых в обход санкций.

Прежняя санкция накладывалась на физлицо или компанию — проверка строилась по имени. Annex XLIV и XLV нацелены на участие в инфраструктуре — платёжный шлюз, криптообмен, банк-корреспондент с определённой ролью. Проверка переходит от идентификаторов сторон к атрибутам самой транзакции: маршруту сообщения, банковскому шлюзу, использованному криптомосту. Для банковских транзакций эти атрибуты доступны в ISO 20022 (раздел 28.5); для криптомостов ту же задачу решает блокчейн-аналитика: сервисы Chainalysis, Elliptic, TRM Labs (см. раздел 27.5) размечают адреса и трассируют переводы между блокчейнами (*cross-chain*) в реальном времени.

28.3 Проверки по 860-П

860-П встраивает санкционную проверку в правила внутреннего контроля (ПВК) кредитной организации как обязательную автоматизированную функцию [577].

Кредитная организация обязана вести регулярную автоматизированную сверку клиентов и их контрагентов с актуальной версией перечней Росфинмониторинга и решений МВК, фиксировать результат каждой сверки и уровень совпадения по каждой паре. В 24-часовой срок применения мер по 115-ФЗ и в ежедневное обновление санкционного индекса банк укладывается только с автоматическим движком и журналом решений; ручной разбор такого объёма физически невозможен. Полный разбор 860-П как ядра ПВК — в гл. 27.

860-П заменяет 375-П, действовавшее с 2012 года. Перечни и решения МВК остаются исходными данными; новое в 860-П — требования к процедуре проверки: автоматизированное сопоставление, регистрация уровня совпадения, журнал снятия блока. Сценарий «раз в день скачать CSV и сверить вручную» с 860-П несовместим.

28.4 Архитектура проверки

Сверка с санкционными перечнями событийная: она выполняется по справочнику клиентов и контрагентов и запускается изменением записи или обновлением перечня. На горячем пути авторизации остаётся только проверка двух флагов — у клиента и у контрагента.

В каждой записи справочника хранится результат последней сверки — флаг состояния и ссылка на запись перечня при совпадении. Авторизация читает эти два поля (флаг клиента и флаг контрагента) и продолжает обычный путь, если оба значения — «не в перечне». Нечёткое сопоставление имён и вся вычислительная нагрузка вынесены в события сверки. Сверку запускают события справочника и перечня.

Загрузка справочника. При первом подключении к актуальному перечню каждая запись справочника проходит нормализацию и сравнение, флаг сохраняется в справочнике.

Ввод нового клиента или контрагента. Запись проверяется один раз сразу после ввода; флаг сохраняется на записи.

Изменение существующей записи. Повторно проверяется только эта запись; флаг обновляется по новому результату.

Обновление перечня. После публикации обновлённого перечня Росфинмониторинга весь справочник сверяется с инкрементом новой версии, и меры применяются к попавшим в перечень не позднее 24 часов с момента размещения обновления [351]. По 860-П каждое событие сверки создаёт запись в журнале с уровнем совпадения.

Записи с нечётким совпадением выше порога автоматически попадают в очередь ручной эскалации; маршрут разбора и критерии снятия блока описаны в разделе 28.7. Типовые ориентиры для порога Jaro-Winkler разобраны в разделе 28.4.

Ядро события сверки — нечёткое сопоставление пары строк. В минимальной реализации нормализация сворачивает имя к канонической форме (удаление диакритики через одну из форм нормализации Unicode — NFKD, Normalization Form Compatibility Decomposition [617], нижний регистр, отбрасывание пунктуации и пробелов), после чего пара строк сравнивается функцией схожести строк. Значение выше порога означает совпадение; ниже — запись считается «не в перечне». Рабочая система применяет более сложные методы сопоставления:

```
import unicodedata
from dataclasses import dataclass
from difflib import SequenceMatcher


@dataclass(frozen=True)
class Hit:
  query: str  # как пришло из CMS
  candidate: str  # имя из санкционного перечня
  score: float  # 0..1


def normalize(name: str) → str:
  # NFKD раскладывает букву с диакритикой на базовую + комбинирующий
  # знак. Например, "ё" → "е" + диакритика "..".
  decomposed = unicodedata.normalize("NFKD", name)
  # Категория Mn = nonspacing mark (диакритика). Отбрасываем.
  no_diacritics = "".join(c for c in decomposed if unicodedata.category(c) ≠ "Mn")
  # Lowercase + только буквы и цифры; пробелы, дефисы, апострофы выпадают.
  return "".join(c.lower() for c in no_diacritics if c.isalnum())


def screen(
  query: str,
  watchlist: list[str],
  threshold: float = 0.85,
) → list[Hit]:
  q_norm = normalize(query)
  if not q_norm:
    return []
  hits: list[Hit] = []
  for candidate in watchlist:
    c_norm = normalize(candidate)
    if not c_norm:
      continue
    # SequenceMatcher ищет совпадающие блоки алгоритмом Ratcliff-Obershelp;
```

(продолжение)

```
    # .ratio() -- метрика 2*M/T на этих блоках (M -- сумма их длин,
    # T -- сумма длин обеих строк).
    score = SequenceMatcher(None, q_norm, c_norm).ratio()
    if score >= threshold:
      hits.append(Hit(query=query, candidate=candidate, score=score))
  return hits
```

Метрики нечёткого сопоставления

Сопоставление имён в рабочей системе сводится к выбору метрики и порога. Базовый набор метрик санкционной проверки — редакторская дистанция Левенштейна, расширение Дамерау — Левенштейна с транспозицией, мера Jaro и Jaro-Winkler с бонусом за общий префикс.

Levenshtein. Минимальное число вставок, удалений и замен, превращающих одну строку в другую [618]. Чувствительна к длине строки и к любому изменению независимо от причины.

Damerau-Levenshtein. Расширение Левенштейна с операцией транспозиции соседних символов: перестановка двух соседних букв стоит 1 вместо 2 [619]. Отделяет клавиатурную опечатку от двух независимых правок.

Jaro. Доля совпадающих символов в окне ширины $\lfloor \max(|a|, |b|)/2 \rfloor - 1$ со штрафом за транспозиции. Значение в $[0, 1]$, в отличие от целочисленной редакторской дистанции [620].

Jaro-Winkler. Модификация Jaro: бонус за общий префикс длиной до четырёх символов с коэффициентом $p = 0{,}1$ [621]. Имена с совпадающим началом получают прибавку: ошибки чаще встречаются в конце имени, чем в начале.

В Python все четыре метрики, а также фонетические коды Soundex и Metaphone, доступны в пакете `jellyfish` [622]. На типичных парах транслитерированных русских фамилий метрики расходятся так (табл. 41).

Таблица 41 — Метрики на парах с разной природой расхождения.

Пара	Lev	DL	Jaro	JW
IVANOV — IVANOV	0	0	1,000	1,000
IVANOV — IVANOFF	2	2	0,849	0,910
IVANOV — YVANOV	1	1	0,889	0,889
IVANOV — IVAN-OFF	3	3	0,819	0,892
IVANOV — IVAONV	2	1	0,944	0,961

Только Damerau-Levenshtein считает транспозицию NO $\leftrightarrow$ ON (пара IVAONV — IVANOV) одной операцией. Jaro-Winkler даёт вес общему префиксу **IVAN**: пара IVANOV — IVANOFF получает прирост $+0{,}061$ против чистого Jaro благодаря бонусу за четыре совпадающих начальных символа. Пара IVANOV — YVANOV того же бонуса не получает, потому что расходится на первом символе.

Типовой порог Jaro-Winkler в санкционной проверке — около $0{,}85$. У Levenshtein и Damerau-Levenshtein порог задаётся относительно длины имени: одна-две правки на короткое имя.

Фонетические алгоритмы Soundex (Russell 1918 [623]) и Metaphone (Philips 1990 [624]) кодируют имя в короткую строку, и сопоставление сводится к сравнению кодов. Оба алгоритма построены под английскую фонологию и для кириллицы без предварительной транслитерации дают непригодный результат. В санкционной

Таблица 42 — Транслитерация русских имён: сравнение стандартов.

Исходное	ISO 9:1995	BGN/PCGN	ICAO 9303
ЕВГЕНИЙ	EVGENIJ	YEVGENIY	EVGENII
ЕКАТЕРИНА	EKATERINA	YEKATERINA	EKATERINA
ЮРИЙ	ÛRIJ	YURIY	IURII
ЦАРЁВ	CARËV	TSARËV	TSAREV
ЩУКИН	ŜUKIN	SHCHUKIN	SHCHUKIN
ФЁДОРОВ	FËDOROV	FËDOROV	FEDOROV

проверке они применяются поверх транслитерированных форм как дополнение к метрикам редакторской дистанции, не как самостоятельный фильтр.

Стандартизация транслитерации

Стандарт транслитерации, который применяет CMS, определяет, что попадает в очередь ручного разбора. Один и тот же человек в разных формах транслитерации даёт разные строки, и Jaro-Winkler возвращает разные значения — иногда выше порога, иногда ниже.

Российские имена латинизируют по следующим стандартам.

ISO 9:1995 (тождествен ГОСТ 7.79-2000 системе A) — одна латинская буква с диакритикой за каждую кириллическую (Ë, Ž, Č, Š, Ŝ, Û, Â). Даёт самые короткие строки и не использует контекстных правил; полностью обратимо без потери буквы [625].

BGN/PCGN 1947 — стандарт США (Board on Geographic Names) и Великобритании (Permanent Committee on Geographical Names) для документов и карт. Шипящие раскрываются в диграфы (KH, TS, CH, SH, SHCH); сохраняется диакритика для ё. Единственное контекстное правило: E и Ë транслитерируются как ye, yë в начале слова, после гласных и после й, ъ, ь, иначе e, ë [626]. Обратимость частичная.

ICAO Doc 9303 part 3 — стандарт ИКАО для машиночитаемой зоны (MRZ) паспорта. Только ASCII A-Z, без диакритики и без контекстных правил; ь не передаётся, ё транслитерируется как e (сливается с e) [627]. Обратимости нет.

На имени ЮРИЙ расхождение становится критическим: между YURIY (BGN/PCGN) и IURII (ICAO) Jaro выдаёт $0{,}733$ — ниже типового порога $0{,}85$. Человек с внутренним документом, оформленным по BGN/PCGN, сопоставляется с санкционным перечнем, где это же имя записано в форме ICAO, только после нормализации обеих сторон к единому стандарту.

Это расхождение видно в карточной эмиссии: один банк требует от клиента вписать имя «как в заграничном паспорте» — то есть именно по ICAO Doc 9303, и ответственность за разночтение в международной идентификации переносится на сам документ. Другой банк генерирует имя по внутренней таблице, иногда не совпадающей ни с одним международным стандартом. ЕВГЕНИЙ Иванов получает разные формы для своей карты: в одном банке YEVGENIY по BGN/PCGN, во втором — EVGENII по ICAO, в третьем — EVGENIJ по ISO 9. Каждая форма правильна по своему стандарту; санкционная проверка зависит от того, какую из трёх форм видит CMS банка и какие формы внесены в санкционный индекс. Различие в одном символе на коротком имени даёт перепад Jaro-Winkler в $0{,}05$–$0{,}08$ — достаточно, чтобы пара оказалась по разные стороны типового порога $0{,}85$.

Все три стандарта реализованы в Python-пакете `iuliia` [628].

Тот же эффект виден на китайских, арабских и корейских именах. Одну и ту же китайскую фамилию пиньинь записывает как *Zhang*, Уэйда-Джайлз — *Chang*, кантонская романизация — *Cheung*; одно арабское имя становится *Mohammad*, *Mohamed*, *Muhammad* или *Mohammed* в зависимости от стандарта латинизации (UNGEGN, ALA-LC, BGN/PCGN). OFAC SDN хранит записи в собственных формах, коммерческие санкционные индексы партнёров — в своих. Совпадение формы имени между CMS и санкционным индексом не гарантировано ни для одной из этих систем письма.

28.5 ISO 20022 и санкционная проверка

22 ноября 2025 года SWIFT завершил период сосуществования форматов: трансграничные платежи между финансовыми институтами идут только в ISO 20022 MX [629]. MT103 (клиентский перевод) и MT202 (межбанковский перевод) заменены на `pacs.008` и `pacs.009` соответственно. Выписки MT940 срок 22 ноября не затронул: они остаются в сети параллельно с `camt.053`.

MT-сообщения хранили данные сторон в неструктурированном текстовом блоке: имя или наименование контрагента, юридический адрес и страна шли в поле `50K`: через перенос строки, без структурной разметки. Санкционный фильтр извлекал имя эвристиками и сравнивал «сырые» строки. MX-сообщения (CBPR+ — Cross-Border Payments and Reporting Plus) задают структурированные поля [630]:

- Nm — имя;
- PstlAdr — почтовый адрес с townName, country code, subdivision;
- LEI — Legal Entity Identifier для юрлиц;
- Id/OrgId/AnyBIC — идентификатор организации.

Проверка разбирает имя, адрес, страну и LEI как отдельные атрибуты. Точность сопоставления выросла: имя и адрес разделены, код страны в отдельном поле проверяется по стране-юрисдикции, LEI даёт детерминированный ключ сопоставления для юридических лиц с зарегистрированной идентификацией. Одновременно выросла ответственность ОПДС: неполное или некорректное структурированное поле видно сразу, «общий текст» его не прикрывает, и банк-отправитель обязан проверить наличие обязательных атрибутов до передачи сообщения дальше.

SWIFT SR 2026 вводит отклонение (NAK) платёжных сообщений CBPR+ с полностью неструктурированными почтовыми адресами; «гибридный» формат остаётся допустимым: townName и country code обязательны как структурированные поля, остальные элементы адреса допустимы в неструктурированных строках (`AdrLine`, до двух строк по 70 символов). Исключения сохранены для выписок и уведомлений (`camt.052/053/054`, `admi.024`, `camt.025`, `camt.060`). Срок 14 ноября 2026 года SWIFT 27 августа 2026 года отложил вместе со всеми платёжными изменениями SR 2026; новый график обещан к декабрю 2026 года [631].

Около 300 российских банков сохраняют подключение к SWIFT, и трансграничные платежи для корпоративных клиентов вне санкционных списков проводятся через них по ограниченному набору официально документированных маршрутов. Российские дочерние банки западных групп — АО Райффайзенбанк (Raiffeisen Bank International) и АО ЮниКредит Банк (UniCredit) — под санкции ЕС не подпадают и остаются основным каналом расчётов в евро; ЦБ РФ включает их в список системно значимых. Газпромбанк был основным каналом энергетических платежей, подпадавших под исключение ЕС для нефти и газа, пока OFAC не включил его в список SDN 21 ноября 2024 года по Executive Order 14024 [632]; после истечения *wind-down* по General License 113 20 декабря 2024 года долларовые расчёты для него

закрылись [633]. Регламенты ЕС платежи в евро с Газпромбанком не запрещают, но круг корреспондентов, готовых работать с ним после включения в список SDN, резко сузился.

Помимо адресных банковских санкций OFAC и ЕС сохраняют набор узких исключений: General License 6D OFAC разрешает поставки в РФ сельскохозяйственной продукции и медицинских товаров; GL 55F — морскую перевозку нефти проекта Sakhalin-2 для импорта в Японию и операции с Газпромбанком по этому проекту до 18 декабря 2026 года; GL 53A — операции дипломатических и консульских представительств РФ с Газпромбанком [634]; статья 12h Регламента ЕС 833/2014 выводит из-под его запретов работы по проекту АЭС Paks II в Венгрии [635]. Сам Росатом как организация под целевой запрет ЕС не подпадает — его дочерние компании включаются в списки каждая отдельно.

28.6 Wire stripping

Wire stripping — удаление или подмена корреспондентским банком полей `50K` (отправитель), 59 (бенефициар), 56/57 (посредники) в исходящем SWIFT MT-сообщении, в которых видно имя или BIC санкционного контрагента, чтобы следующий корреспондент на маршруте через США или ЕС не получил совпадения на фильтре OFAC или EU. Схему выполняет корреспондент, через которого санкционное лицо отправляет валютный платёж: он переписывает поля, заменяет имя нейтральным юрлицом из той же группы и направляет «очищенное» сообщение дальше по маршруту. Корреспондент получает комиссию с санкционного клиента, а фильтр следующего банка видит сообщение, неотличимое от законного перевода.

Standard Chartered Bank с 2001 по 2007 год систематически удалял санкционные идентификаторы (SWIFT/BIC иранских контрагентов) из MT103 и MT202 на корреспондентском маршруте через Нью-Йорк, чтобы пройти проверку по спискам OFAC в американских клиринговых банках. NYDFS в 2012 году назначил штраф $340 млн и опубликовал детальный анализ схемы [636]. Урегулирование 2012 года практику не прекратило: в 2019 году тот же банк по единому соглашению с NYDFS, DOJ, OFAC, ФРБ Нью-Йорка и британским FCA выплатил ещё $1,1 млрд за нарушения по Бирме, Кубе, Ирану, Судану и Сирии в период 2008–2014 годов через дубайский филиал и онлайн-платформу «Straight-to-Bank» [637].

BNP Paribas повторил тот же сценарий в большем масштабе. С 2004 по 2012 год банк использовал *wire stripping* и скрытую маршрутизацию через сеть корреспондентов для обхода санкций США против Судана, Ирана и Кубы [638]. Deutsche Bank в 2015 году получил аналогичное предписание NYDFS: штраф $258 млн, из них $200 млн в пользу NYDFS и $58 млн в пользу ФРС [639].

Структурная валидация сама по себе не исключает *wire stripping*: банк-корреспондент формирует исходящее MX-сообщение по входящей инструкции (инструкция приходит к нему по любому транспорту), и парсер получающего банка увидит структурно валидное `pacs.008`/`pacs.009` независимо от того, указан в поле `Nm` реальный отправитель или подставное юрлицо. Подмену ограничивают правила, надстроенные над транспортной схемой.

Прозрачность покрывающих сообщений (*cover payment transparency*). MT202COV (введён SWIFT 21 ноября 2009 года) [640] и ISO 20022 `pacs.009` со связанной `pacs.008` требуют, чтобы межбанковское покрывающее сообщение (*cover*) несло данные *исходного клиентского перевода*. До введения MT202COV корреспондент мог

провести MT103 с санкционным клиентом через свои внутренние счета или сателлитный банк, а в Нью-Йорк для долларового клиринга отправить отдельный MT202 без клиентских данных — американский клиринг видел только межбанковскую часть маршрута и не получал данных для фильтра OFAC. На этом разделении платежа BNP Paribas строил суданские платежи через сеть сателлитных банков, в основном арабских [641].

Travel Rule. Рекомендация 16 FATF и для ЕС Регламент (EU) 2023/1113 обязывают каждое платёжное сообщение нести полные данные отправителя и бенефициара (имя, счёт, адрес или идентификатор); банк-получатель по риск-ориентированным процедурам решает, исполнить, отклонить или приостановить перевод с неполной информацией [573, 574]. Скрытие имени само по себе становится нарушением, даже без совпадения на санкционном фильтре.

Машиночитаемый аудит. Код страны, LEI и BIC в отдельных полях позволяют надзорному органу или банку-корреспонденту проверить массив сообщений ex post по детерминированному фильтру (страна = IR, BIC из списка SDN) без разбора свободного текста. Автоматизированный поиск снижает стоимость контроля, и систематическое применение схемы выявляется по статистике потоков, а не по отдельному сообщению.

Эти правила пресекают именно «очистку» существующих полей. Подмена имени реального клиента на юрлицо из той же группы остаётся отдельным способом обхода: банк-отправитель заполняет обязательные поля синтаксически правильным, но ложным значением. Схема сообщения не отличает подлинного отправителя от подложного; против такого сценария требуется KYC на стороне банка-отправителя (см. гл. 26).

LEI обходит проблему транслитерации, но не решает её: совпадение проверяется посимвольно по 20-значному коду, имя в процедуре не участвует. Само поле юридического наименования (*legal name*) в LEI-реестре хранится в исходной графике (для российских юрлиц — кириллицей), а ASCII-транслитерация опциональна и заполняется локальным регистратором по усмотрению, так что многовариантность имени сохраняется и внутри LEI-данных. LEI помогает только при наличии кода и у отправителя в MX-сообщении, и у санкционного субъекта в перечне; OFAC SDN и EU Consolidated указывают LEI не для всех записей, а физлица в LEI не входят по определению.

28.7 Ложные срабатывания и маршрут разбора

Ложноположительные совпадения (гл. 29) попадают в отдельную очередь: система помечает запись справочника как требующую проверки, аналитик изучает контекст и либо снимает блок, либо эскалирует случай. Маршрут должен быть формализован, иначе одинаковые срабатывания приводят к разным решениям. Распространённые имена и совпадения между кириллицей и латиницей создают большой поток срабатываний; значительная доля работы аналитика — быстро отделить заведомо ложные совпадения [642]. Логика сопоставления и пороги срабатывания настраиваются по собственной оценке риска ОПДС, зафиксированной в правилах внутреннего контроля по 115-ФЗ.

Аналитик получает карточку совпадения с атрибутами операции (страна, сумма, продукт, история клиента), оценкой схожести по основной метрике и ссылкой на запись в перечне. Регламент разрешает аналитику самостоятельно снять блок с обоснованием в журнале и пропустить транзакцию; эскалация в службу комплаенс

обязательна, если совпадение касается санкционных перечней с правовыми последствиями (статья 6 115-ФЗ, OFAC SDN, EU Consolidated), если клиент уже фигурировал в эскалациях или если запрос инициирован банком-корреспондентом.

Журнал решений — такая же часть санкционного контроля, как и алгоритм сопоставления. Доказать отсутствие нарушений можно только журналом.

29 Фрод

Универсального признака риска нет; атака всё чаще маскируется под нормальное поведение. Система анализирует устройство, историю аккаунта, частоту попыток, маршрут доставки и поведение после оплаты и формирует из этих слабых признаков общую оценку риска. Слишком строгий фильтр повышает цену ошибочного отказа, а слишком мягкий пропускает больше фрода.

29.1 Модель угроз

Карточный фрод устроен как разделённый рынок: одни участники крадут данные, другие проверяют, какие из них ещё работают, третьи монетизируют подготовленную атаку. Фильтр, хорошо выявляющий карточный перебор, не выявит злоупотребление chargeback, поэтому защиту строят от перечня классов атак.

Самый старый класс атак — скимминг. Он работает, пока в системе сохраняется *fallback* на магнитную полосу (подробный разбор сценария — раздел 7.9). Накладка на терминале или банкомате считывает данные полосы; украденные дампы (*dumps*) попадают на закрытые площадки и превращаются в клон карты. Чип EMV (Europay/Mastercard/Visa, см. гл. 7) резко снизил ценность такого клона: каждая операция требует новой криптограммы, которую нельзя скопировать. Магнитная полоса исчезла не везде и не одновременно, и пока *fallback* доступен, скимминг сохраняет силу [91].

Следующий класс атак — фрод без предъявления карты (*card-not-present*, CNP) и карточный перебор (*carding*). В электронной коммерции у атакующего есть номер карты (Primary Account Number, PAN; см. гл. 9), срок действия и трёхзначный проверочный код на обороте (Card Verification Value, CVV/CVV2), полученные из утечки, через фишинг, вредоносное ПО или на теневом рынке. Дальше начинается *carding*: серия мелких тестовых списаний проверяет, какие реквизиты ещё работают, а за успешными тестами следует крупная покупка [643]. Атака оставляет плотный повторяющийся ритм и хорошо заметна в частотных проверках; такие правила срабатывают до первой дорогой операции [644].

Отдельный класс атак — захват учётной записи (Account Takeover, ATO). Злоумышленник входит через уже установленное доверие: массовый перебор утёкших пар логин/пароль (*credential stuffing*), фишинг, социальная инженерия, иногда подмена SIM-карты. Он получает доступ ко всему, что система раньше связывала с легитимным клиентом: истории покупок, сохранённым картам, адресам доставки. Отдельная транзакция выглядит почти нормальной, и поводом для подозрения становится резкая смена устройства, географии, канала входа или адреса доставки [643].

Дружественный фрод (*friendly fraud*) совершает сам держатель карты: он оплачивает покупку, получает товар или услугу и затем заявляет, что операция была несанкционированной. Такой фрод характерен для цифровых товаров, подписок и сервисов с нематериальной поставкой, где труднее показать момент потребления. Связная история устройства, аккаунта, использования услуги и доставки становится доказательной базой в спорах о chargeback (см. раздел 32.4) [645]; без неё спор сводится к слову против слова.

Фрод *bust-out* монетизирует накопленное доверие: клиент или продавец сначала ведёт себя образцово, увеличивает лимиты или оборот, а затем резко меняет

профиль поведения и выводит деньги из системы. Для эмитента это похоже на кредитный обман: несколько карт, аккуратная история, постепенный рост лимита и затем дефолт. В эквайринге сценарий другой: спокойный старт, быстрый рост оборота, всё меньше возвратов и внезапное исчезновение продавца. Такие случаи видны только там, где у системы есть длинная история поведения и мониторинг после подключения; короткий период наблюдения их не выявляет [48, 643].

Набор наблюдаемых признаков меняется от атаки к атаке: в одних сценариях важнее устройство, в других аккаунт, история доставки и потребления или профиль продавца. Защита поэтому собирается из специализированных проверок под каждый класс атак.

29.2 Пороговые проверки и статические правила

Первый рубеж защиты работает быстрее всех, потому что ему нужно принять решение до того, как операция превратится в ущерб. Эту задачу решают пороговые проверки (*velocity checks*) и статические правила. Они отвечают на простые вопросы: не слишком ли много операций приходит с одного IP, не появилось ли на одном устройстве подозрительно много карт, не отклонилась ли сумма от привычной истории клиента. Правило сравнивает текущую операцию с заранее заданным порогом и за миллисекунды решает, пропустить её или отклонить. Жёсткие пороги отклоняют нормальные операции, мягкие пропускают атаку.

Базовые правила оценивают частоту, концентрацию и резкое отклонение от профиля. Сколько операций пришло с одного IP за час, сколько попыток прошло по одной карте за десять минут, сколько карт появилось на одном устройстве за сутки, насколько текущая сумма выбивается из профиля аккаунта. Такие проверки дёшевы, быстро исполняются и легко объясняются бизнесу, комплаенсу и регулятору.

В коде частотная проверка сводится к скользящему окну: события по ключу (карта, IP, устройство) хранятся в очереди, события старше окна вытесняются, превышение порога — отказ. Отклонённые попытки тоже учитываются — иначе атакующий обходит проверку, продолжая перебор сразу после достижения порога. Источник времени вынесен в параметр (`now`): в рабочей системе туда передают `time.monotonic`, а в тестах — управляемые часы.

```
from collections import defaultdict, deque
from collections.abc import Callable
from dataclasses import dataclass, field


@dataclass
class VelocityRule:
  window_sec: float
  max_events: int
  now: Callable[[], float]
  _events: defaultdict[str, deque[float]] = field(
    default_factory=lambda: defaultdict(deque)
  )

  def check(self, key: str) → bool:
    timeline = self._events[key]
    now = self.now()
    cutoff = now - self.window_sec
    while timeline and timeline[0] < cutoff:
      timeline.popleft()
    timeline.append(now)
    return len(timeline) <= self.max_events
```

Атакующий умеет дробить поток под пороги, менять IP, растягивать серию во времени и подмешивать легитимный шум. Правило не учитывает контекст: крупная покупка в аэропорту перед вылетом для одного клиента норма, а для другого — сильная аномалия.

Отдельная категория правил выявляет карточный перебор (*carding checks*). Злоумышленник начинает с серий микросписаний или авторизаций на символические суммы с одного IP, устройства или подсети, иногда по десяткам разных карт. Пока атака проверяет, какие реквизиты ещё работают, она оставляет повторяющийся ритм, который трудно скрыть, и частотные правила выявляют её именно по нему.

29.3 Цифровой слепок устройства и поведенческая аналитика

Цифровой слепок устройства (*device fingerprinting*) — набор признаков браузера или телефона, по сочетанию которых система распознаёт конкретное клиентское окружение. В него входят заголовок `User-Agent`, размер экрана, часовой пояс, набор шрифтов, характеристики WebGL и особенности рендеринга `canvas` и `audio`. Отдельный признак слаб, устойчивый профиль даёт их комбинация. Если браузер скрывает или специально искажает эти атрибуты, точность падает, но слепок остаётся сильным признаком риска [646].

Слепок становится полезнее с накоплением истории. Устройство, которое месяцами используется в нормальных покупках, набирает доверие. Новый слепок, возникший при дорогой покупке и с новым адресом доставки, усиливает подозрение. На той же истории строится доказательство связи клиента с прежними операциями для разбора chargeback.

Поведенческая аналитика добавляет данные текущей сессии — скорость набора, траекторию мыши, время заполнения формы и паузы между действиями. У человека, вводящего свою карту, и у бота, перебирающего украденные реквизиты, статические признаки могут совпадать, а динамика поведения расходится; анализ строит для них разные поведенческие профили. Данные собираются пассивно и не усложняют оформление покупки. Зато браузеры с усиленной защитой приватности сокращают набор сигналов, а опытный атакующий имитирует часть поведения, поэтому поведенческие сигналы используют только в связке со слепком устройства.

На мобильных платформах для сопоставимой полноты данных нужен отдельный комплект разработчика (Software Development Kit, SDK). Слепок устройства подделать полностью трудно, а подделать и при этом не оставить новых аномалий ещё труднее. Этот же набор сигналов продавец передаёт эмитенту: EMV 3-D Secure (см. гл. 11) отдельно выделяет данные об устройстве (*device information*), о держателе карты и аккаунте (*cardholder account information*), о признаках риска со стороны продавца (*merchant risk indicator*) и о доставке (*shipping and delivery information*) для оценки риска на стороне сервера управления доступом эмитента (Access Control Server, ACS) [647].

29.4 Машинное обучение в антифроде

Машинное обучение (*machine learning*, ML) учитывает множество слабых признаков: время суток, сумму, географию, расстояние от предыдущей операции, профиль продавца, историю устройства. Там, где по отдельности всё выглядит нормально, модель выявляет редкую комбинацию. Модель воспроизводит только шаблоны обучающей выборки и устаревает по мере того, как злоумышленники меняют поведение, поэтому ML работает вместе с правилами: модель ловит слабые комбинации признаков, а правила закрывают стабильные и нормативно заданные случаи.

В реальном потоке легитимных операций гораздо больше, чем мошеннических, поэтому доля верных ответов (*accuracy*) ничего не говорит о качестве модели антифрода: модель, отвечающая «легитимно» на каждый запрос, формально выглядит почти идеальной, но бесполезна. Каждое решение модели попадает в одну из клеток матрицы несоответствий (*confusion matrix*): **TP** (*true positives* — мошеннические операции, которые модель верно заблокировала), **FP** (*false positives* — честные операции, ошибочно заблокированные), **TN** (*true negatives* — честные операции, верно пропущенные) и **FN** (*false negatives* — мошеннические операции, ошибочно пропущенные). На этих счётчиках строятся базовые метрики:

$$\mathrm{precision} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}}, \qquad \mathrm{recall} \equiv \mathrm{TPR} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}, \qquad \mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}}.$$

Precision — доля настоящего фрода среди заблокированных; TPR (*recall*, полнота) — доля пойманного фрода среди всех мошеннических операций; FPR — доля ложных блокировок среди всех легитимных. Компромисс между *precision* и *recall* сворачивают в F1:

$$F_1 = 2 \cdot \frac{\mathrm{precision} \cdot \mathrm{recall}}{\mathrm{precision} + \mathrm{recall}}.$$

Зависимость от порога модели показывают кривые: PR (*precision* от *recall*) с PR-AUC и **ROC** (Receiver Operating Characteristic — TPR от FPR) с ROC-AUC от 0,5 у случайного классификатора до 1 у идеального [648, 649]. На рис. 59 две рабочие точки этой ROC соответствуют публичным порогам Stripe Radar 65 и 75 [650]; сами значения TPR и FPR в этих точках иллюстративны на типичной CNP-кривой, потому что *Visa Advanced Authorization*, *Mastercard Decision Intelligence*, *Adyen RevenueProtect*, Forter и Riskified конкретных чисел публично не раскрывают. Рабочая зона FPR 2–10 % — диапазон, который по опросу MRC 2024 называют CNP-ТСП [651]; базовая доля фрода по картам EU/EEA в 2024 году — 0,033 % от оборота [652]. Такая низкая базовая доля обрушивает точность блокировок (*precision*) даже при высоком TPR: при базе $0{,}033\,\%$ у модели с $\mathrm{TPR} = 0{,}9$ и $\mathrm{FPR} = 0{,}02$ среди заблокированных окажется на два порядка больше честных операций, чем мошеннических.

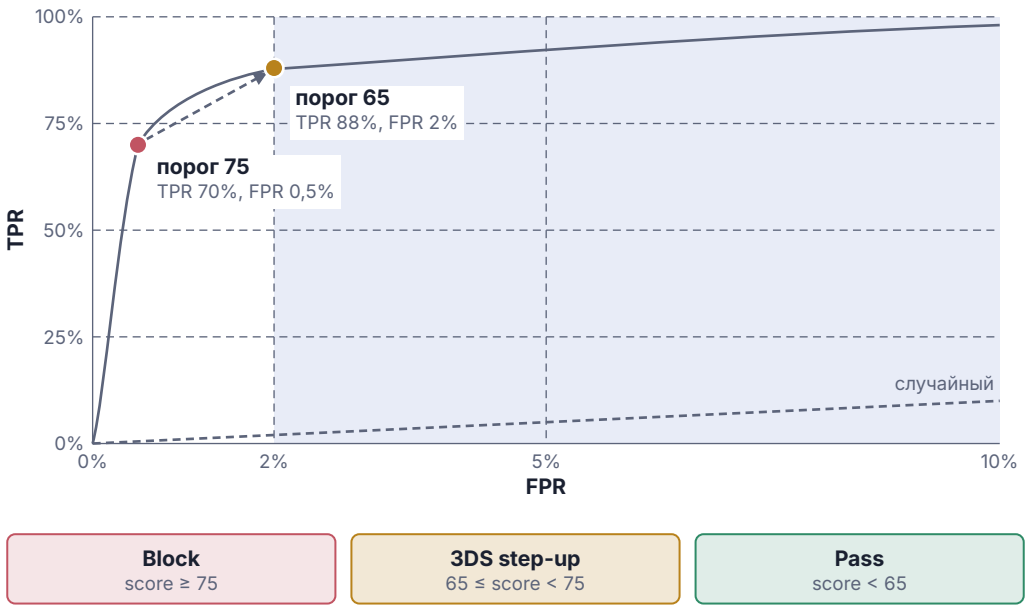


Рис. 59 — ROC-кривая скоринга с рабочими точками для порогов Stripe Radar 65 и 75 и зоной FPR 2–10 %.

Для рабочего антифрода хватает градиентного бустинга (*gradient boosting* — ансамбль решающих деревьев, в котором каждое следующее дерево обучается на ошибках предыдущего): он проще в обучении, легче объясняется и хорошо работает на табличных данных. Признаки остаются простыми: окна по времени, агрегаты по продавцу, скользящие суммы, расстояние от предыдущей транзакции. Открытая литература показывает то же: на табличных наборах данных о фроде сильными базовыми моделями остаются деревья и градиентный бустинг, а качество и отбор признаков влияют на итоговые *precision* и *recall* не меньше, чем выбор архитектуры [653, 654].

Конкретный вектор признаков для одной транзакции CNP: сумма транзакции; отношение суммы к среднему чеку держателя карты за 90 дней; количество транзакций этой карты за последний час и за сутки; расстояние в километрах между текущим IP и IP предыдущей операции; время с предыдущей операции в минутах; возраст аккаунта у продавца в днях; совпадение страны банковского идентификационного номера эмитента (Bank Identification Number, BIN) и страны IP; совпадение хэша устройства с ранее виденным; код категории торговой точки (Merchant Category Code, MCC; см. гл. 14); результат проверки трёхзначного кода с обратной стороны карты (CVV2); результат сверки адреса держателя с данными эмитента (Address Verification System, AVS [655]); количество отказов по этой карте за 24 часа; количество уникальных продавцов за последний час; время суток, нормализованное к часовому поясу держателя. Набор из 15–25 таких признаков покрывает большинство известных шаблонов атак.

Модель возвращает скор — нормализованную оценку в $[0, 1]$ или её масштабированную копию (Stripe Radar отдаёт целое 0–99, упомянутые на рис. 59 пороги соотносятся именно с этой шкалой). Действие назначается правилами после скоринга: при низких значениях транзакция проходит без дополнительной проверки, средние направляются на проверку 3DS в сценарии *challenge* или в ручную очередь,

высокие получают автоматический отказ. Пороги калибруются под целевую долю FPR, конкретные числа оператор подбирает эмпирически по собственным данным; универсальных значений для произвольного потока не существует.

В рабочую систему порог вводят через несколько этапов: *shadow mode* (модель работает, действия не применяются, результат сравнивается с действующей логикой), затем A/B-эксперимент на доле трафика, затем полное развёртывание (*rollout*). Порог, изменённый напрямую без проверки в *shadow mode*, с момента смены даёт всплеск ложных блокировок или пропусков.

Главная проблема в эксплуатации — дрейф концепции (*concept drift*). Мошенники подстраиваются под то, что модель уже выявляет, и через несколько недель недавний признак перестаёт работать, а давно не переобучавшаяся модель деградирует. Поэтому защита от фрода устроена как непрерывный процесс: контроль качества на скользящем окне, регулярное переобучение, сравнение новой и старой версии на отложенных данных [656].

Подтверждённая метка «это был фрод» приходит не с авторизации, а из цикла оспаривания (см. раздел 32.1): *chargeback* эмитент инициирует за дни, но финальный исход спора закрепляется через 60–120 дней. До тех пор полная разметка недоступна, и для свежих транзакций приходится опираться на прокси-метки: ручные проверки аналитиков, отчёты держателей карт в банк и сигналы от карточной сети. Поэтому модель переобучается чаще, чем приходят финальные метки: быстрый цикл по прокси-меткам (дни) выявляет свежий шаблон атаки, медленный по окончательным меткам *chargeback* (кварталы) защищает от систематической ошибки разметки.

Службе поддержки, аналитикам и бизнесу нужна понятная причина отказа, а ответ «модель сказала нет» не помогает ни восстановить платёж, ни улучшить систему. В рабочих системах используют SHAP (SHapley Additive exPlanations — метод объяснения предсказаний на основе значений Шепли из теории игр) и LIME (Local Interpretable Model-agnostic Explanations — локальная линейная аппроксимация модели вокруг конкретной точки), показывающие вклад отдельных признаков в итоговое решение [657, 658].

29.5 Гибридные системы: правила и модель

Рабочая антифрод-система гибридна: правила быстро отсекают грубые атаки, модель аккуратнее работает с пограничными случаями, а правила после скоринга переводят численную оценку в конкретное действие. Внутри одного эквайрингового потока такая схема воспроизводится у каждого участника антифрода, но набор данных у каждого свой.

У ТСП есть точка ввода и собственные правила предварительного отсева (*pre-screening*): запреты по стране доставки, по MCC, по BIN, лимиты на стоимость заказа. Сам слепок устройства, на который опирается дальнейшая логика, собирает не ТСП, а встроенный в страницу оплаты скрипт PSP, вендора антифрода (Sift, Forter, Signifyd, Kount, Riskified) или iframe ACS эмитента через 3DS Method URL. У PSP и эквайера — готовая ML-модель и маршрутизация решений в потоке эквайринга. У карточной сети — собственные сервисы оценки риска (*Visa Advanced Authorization*, *Mastercard Decision Intelligence*), видящие весь трафик через сеть. У эмитента — финальный механизм оценки риска авторизации и RBA-логика в ACS (см. раздел 29.6).

Предварительный отсев (*pre-screening*) блокирует очевидные случаи: карточный перебор, карту из стоп-листа, явное превышение порога частоты. Скоринговый

модуль (*scoring engine*) выдаёт оценку риска для операций, прошедших первичный фильтр. Правила после скоринга (*post-scoring rules*) переводят оценку в действие: высокие значения ведут к блокировке, средние требуют дополнительной верификации или проверки через 3DS, а низкие проходят дальше.

Бюджет задержки у этапов разный. Правила *pre-screening* отрабатывают за единицы миллисекунд, потому что любая задержка напрямую увеличивает время ответа на авторизацию. Скоринг ML допускает 20–50 мс, поскольку включается только после быстрого отсева. Модуль решений сравнивает скор с порогами и применяет правила *post-scoring*, поэтому задержки почти не добавляет.

Правила остаются в системе даже после того, как модель показывает хорошее качество. Регуляторные требования напрямую обязывают блокировать определённые категории операций по формализованному признаку, и модель явного правила не заменяет. При разборе chargeback или ответе на запрос регулятора нужна объяснимая причина отказа в формулировке вида «транзакция превысила порог по частоте»: такая формулировка документируется и проверяется, а ссылку на решение модели регулятор не примет.

Исходы транзакций, ручные проверки, оспаривания и подтверждённые случаи фрода возвращаются и в обучающую выборку, и в набор правил. Иначе модель теряет чувствительность к свежим атакам и деградирует под *concept drift*.

Выбор архитектуры антифрода зависит от объёма и зрелости системы; единого порога транзакций в месяц нет. На малом потоке собственная модель ML нецелесообразна: обучающая выборка мала, *concept drift* незаметен, а стоимость содержания модели сопоставима с потерями от фрода. Достаточно набора правил, предоставляемых PSP (см. раздел 2.2). Готовое решение PSP, например Stripe Radar, поставляется как ML-модель, конфигурируемые правила и пороги (по умолчанию 65 и 75 на шкале 0–99, см. рис. 59) [650]. На среднем потоке имеет смысл гибридная схема, в которой готовая модель от PSP или вендора дополняется собственными правилами под специфику бизнеса. На больших объёмах собственная модель окупается: данных достаточно для обучения, *concept drift* заметен в реальном времени, контроль над порогами даёт прямой финансовый эффект. Конкретные числовые пороги перехода между этими вариантами оператор устанавливает по собственным метрикам потерь от фрода и стоимости владения моделью.

29.6 Скоринг и 3DS RBA

Риск-ориентированная аутентификация (Risk-Based Authentication, RBA) в 3DS v2 (см. раздел 11.4) определяет, запросить ли у держателя подтверждение (*challenge*) или пропустить операцию по сценарию *frictionless*. Задача продавца — передать эмитенту контекст, повышающий точность решения.

В 3DS v2 запрос аутентификации содержит набор структурированных данных от продавца и 3DS Server. EMVCo отдельно выделяет *cardholder account information*, *merchant risk indicator*, *shipping and delivery information* и *device information*; ACS собирает из них контекст и применяет собственную модель [647, 659].

Антифрод продавца вычисляет оценку риска, но поля для самого скора в 3DS-запросе нет: продавец передаёт её через индикатор запроса *challenge* (*3DS Requestor Challenge Indicator*) и контекстные атрибуты протокола. При высоком риске продавец просит *challenge*, при низком — даёт эмитенту основания для *frictionless*. Решение принимает ACS эмитента по своей модели, запрос продавца для неё — сигнал,

а не команда; качественный контекст заметно сокращает долю как пропущенного фрода, так и ненужных *challenge*.

На стороне сетей и сетевых провайдеров работают собственные сервисы оценки риска: у Visa это *Visa Advanced Authorization* (VAA) и *Visa Consumer Authentication Service* (VCAS), у Mastercard — *Decision Intelligence*. Эмитент получает от них дополнительную оценку, отделяющую легитимный поток от серии тестовых и атакующих попыток; для продавца это ещё один сигнал в общей авторизационной логике [644, 660].

29.7 Стоимость ложноположительных срабатываний

Настройка антифрода — выбор между ошибками матрицы несоответствий: ложноположительным срабатыванием (*false positive*, FP — числитель FPR) и ложноотрицательным (*false negative*, FN); система, не пропускающая ни одной атаки, неизбежно отклоняет слишком много нормальных операций. Доля пропущенного фрода —

$$1 - \mathrm{TPR} = \frac{\mathrm{FN}}{\mathrm{TP} + \mathrm{FN}}.$$

Пропущенный фрод заметнее ошибочной блокировки: каждая мошенническая операция даёт прямой убыток и часто заканчивается chargeback. Цена ошибочной блокировки менее видна: упущенная выручка и ушедший клиент не попадают в ту же отчётность, что и *chargeback*.

По данным совместного отчёта Европейского центрального банка (ЕЦБ) и Европейского банковского управления (European Banking Authority, EBA) за 2024 год, доля фрода в общем объёме карточных операций с картами, выпущенными в EU/EEA, составила 0,033 %, а около 83 % стоимости фрода пришлось на операции, инициированные удалённо (*remote*, аналог CNP) [652]. По рынку России сопоставимые агрегированные показатели публикует ФинЦЕРТ (Центр взаимодействия и реагирования Департамента информационной безопасности Банка России) в «Обзоре операций, совершённых без добровольного согласия клиентов финансовых организаций», причём документ охватывает все электронные средства платежа (ЭСП), а не только карты [44]. Антифрод и работа со спорами связаны мониторинговыми программами сетей: пропущенный фрод увеличивает долю chargeback и переводит ТСП под надзор VAMP и MC ECP (детальные пороги, формулы и санкции — в разделе 32.6). Универсальных публичных бенчмарков по *false positive rate* для скоринга ML и систем только на правилах нет; разница между ними измеряется на собственном потоке оператора. Каждый лишний процентный пункт FPR обходится в

$$\Delta R_{\text{день}} \approx N \cdot \mathrm{AOV} \cdot \Delta_{\mathrm{FPR}},$$

где N — объём транзакций в день, AOV (Average Order Value) — средний чек, Δ_{FPR} — приращение доли ложных блокировок (для одного процентного пункта — $0{,}01$).

Когда легитимная транзакция ошибочно блокируется, клиент обращается в поддержку, а продавец теряет текущую оплату и будущие покупки этого человека. Отказ дорог и эмитенту: по данным Visa, держатели, получившие отказ, в четыре раза чаще перестают пользоваться картой [644].

При выявлении фрода *precision* и полнота (*recall*) считаются для класса мошеннических операций, а не для общего потока. Чем ниже порог, тем больше блокировок и меньше пропущенного фрода, но больше ошибочных отказов; повышение порога даёт обратный эффект. Оптимальная точка зависит от экономики продукта: чем дороже пропущенный фрод относительно упущенной маржи, тем строже фильтр. Цифровой товар с высокой маржой и нулевой себестоимостью допускает мягкий фильтр, физическая доставка с дорогим возвратом требует строгого.

Платёжный шлюз с высокой долей цифровых подписок поддерживает FPR

весь чек, а пропущенный фрод стоит чека и комиссии за *chargeback* без потери товара. Маркетплейс физических товаров с доставкой и возвратом за счёт продавца выбирает FPR ближе к верхней границе диапазона MRC 2024 (см. рис. 59): пропущенный фрод стоит ему чека, потерянного товара и доставки, а ложная блокировка — только маржи с чека. Конкретные значения — авторская оценка типовой настройки; публично нормированных бенчмарков по сегментам рынок не раскрывает. Стоимость каждой ошибки команда антифрода переводит в рубли и считает на собственном потоке: упущенная маржа $m \cdot \mathrm{AOV}$ от ложной блокировки (где m — доля валовой маржи в чеке) против полной стоимости пропущенного фрода — возврата AOV, комиссии процессора за chargeback (*chargeback fee*, типично 10–50 USD, у ТСП высокого риска до 100 USD [661]), потерянного товара и доставки, плюс вклад в долю chargeback (*chargeback ratio*) по VAMP/MC ECP, после превышения порога которой платёжная сеть начисляет штраф. Точка безразличия (*indifference point* — равенство стоимостей ложной блокировки и пропущенного фрода) даёт верхний предел разумного FPR, выше которого настройка фильтра уже не окупается даже при нулевом пропуске атак.

ПРАКТИКА

Стоимость *false positive* считают явно, складывая упущенную транзакцию, риск потерять клиента и расходы поддержки. Такой расчёт выявляет случаи, когда система настроена агрессивнее, чем бизнесу выгодно.

30 Подписки и сохранённые реквизиты

Подписка начинается с первого согласия на хранение реквизитов. Для продукта январский платёж и февральское автосписание продолжают одну услугу, но для эмитента это две разные авторизационные ситуации. Когда связь между ними обрывается, эмитент теряет контекст, карточная сеть считает операцию подозрительной, а клиент получает отказ по штатному платежу.

30.1 Сохранённые реквизиты и SCF

До появления единых правил ТСП решали повторные списания каждый по-своему: кто-то хранил номер карты (Primary Account Number, PAN), кто-то полагался на токенизацию, кто-то каждый месяц отправлял обычный запрос и рассчитывал, что эмитент восстановит контекст. Эмитент не получал главный признак: продолжает ли операция согласованную цепочку или проходит без явного участия клиента.

Без контекста «тихая» транзакция, инициированная ТСП (merchant-initiated transaction, MIT), для эмитента выглядела как обычный запрос без присутствия карты (card-not-present, CNP). ТСП мог начать регулярные списания без явного согласия клиента или продолжить их после его отмены, и эмитент не мог этого различить. SCF сделал контекст первого согласия обязательным полем авторизационного сообщения.

Visa и Mastercard ввели Stored Credential Framework (SCF) — набор правил, по которым карточная сеть различает первое согласие клиента и последующие списания; контекст первого согласия становится видимым в авторизационном сообщении [46, 662]. Реквизиты остаются у ТСП, но каждая операция должна содержать явную связь с исходным согласием клиента.

В авторизационном сообщении эта связь выражается несколькими признаками: первичным или последующим использованием сохранённых реквизитов, типом операции и ссылкой на исходную авторизацию, связывающей всю цепочку [46, 663]. Visa использует Stored Credential Transaction Indicator со значением `initial` при первой транзакции, инициированной клиентом (customer-initiated transaction, CIT), и `subsequent` при последующей MIT. Вместе с ним передаётся тип инициатора (cardholder-initiated или merchant-initiated) и причина MIT — регулярные (recurring), рассрочка (installment) или внеплановые (unscheduled) [662, 663]. Mastercard кодирует ту же информацию через POS Entry Mode (DE 22) и подэлемент 22 поля данных 48 (Data Element 48, DE 48) с индикатором CIT/MIT и требует передавать Trace ID исходной CIT в каждой последующей MIT; точные подполя сверяются по действующей редакции правил обработки транзакций (Transaction Processing Rules, TPR) [46].

Клиент оформляет месячную подписку. Первый платёж идёт как CIT с indicator = `initial` и получает от карточной сети идентификатор сетевой транзакции (Network Transaction ID, NTID у Visa; Trace ID у Mastercard — функциональный аналог NTID для соответствующей сети) [468]. Через 30 дней ТСП отправляет MIT с indicator = `subsequent`, типом `recurring` и ссылкой на NTID первой CIT. Когда ТСП не передаёт ссылку на исходную авторизацию или указывает неверный тип, эмитент видит запрос без контекста и вправе применить стандартную политику CNP, вплоть до отказа (см. рис. 62). При аудите карточная сеть квалифицирует такую операцию как нарушение правил SCF [13, 46].

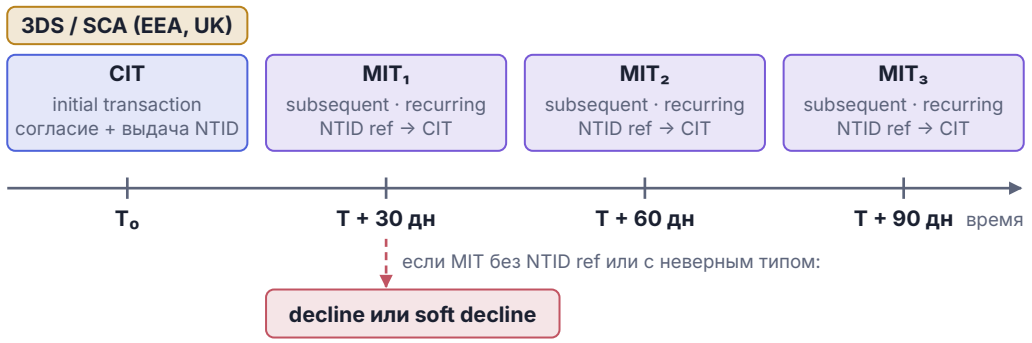


Рис. 60 — SCF на временной шкале: CIT с выдачей NTID и серия MIT со ссылкой на NTID; отсутствие NTID ведёт к отказу.

30.2 CIT и MIT

Контекст обрывается: клиент оформил услугу и согласился на сохранение реквизитов, а через неделю или месяц ТСП списывает очередной платёж уже без его участия.

В CIT клиент сам нажимает кнопку оплаты, вводит данные карты, проходит аутентификацию, когда её требуют правила рынка. Так проходит первый платёж за подписку, оформление Card-on-File (CoF, модель хранения реквизитов карты у ТСП для последующих списаний) или покупка, после которой ТСП получает право сохранить реквизиты. Система фиксирует исходную точку цепочки и получает связующий идентификатор исходной авторизации. В документации сети или шлюза этот идентификатор называется *transaction identifier*, *network transaction ID*, `previousTransactionID` или Trace ID [46, 663, 664].

Согласие клиента возникает в CIT, но сохранение реквизитов не даёт ТСП права на любые будущие списания. Идентификатор нужно хранить и передавать в каждой последующей операции, иначе связь между первым согласием и следующими списаниями исчезнет из авторизационного контекста [46, 663].

MIT — списание без активного участия клиента: ежемесячная подписка, доначисление по уже оказанной услуге или платёж по ранее согласованной схеме. Запрос инициирует ТСП, но он должен передать эмитенту признак продолжения существующей цепочки. Поэтому MIT всегда сопровождается признаками SCF, типом операции, заданным карточной сетью, и идентификатором исходной авторизации [46, 664].

MIT без корректных признаков SCF эмитент видит как новую CNP-операцию без контекста и вправе отклонить, даже когда биллинг ТСП считает её штатной. В европейском трафике при удалённом оформлении мандата на серию MIT (мандат — согласие клиента на регулярные списания по сохранённым реквизитам) строгая аутентификация клиента (strong customer authentication, SCA) применяется на этапе создания мандата, а последующие MIT должны быть корректно помечены и связаны с исходной авторизацией [46, 665].

30.3 Идентификатор исходной авторизации и цепочка согласия

Токен отвечает на вопрос, каким реквизитом платить, а идентификатор исходной авторизации — на вопрос, с каким ранее данным согласием связано текущее автосписание. Токен обновляется при перевыпуске карты, а идентификатор цепочки хранится отдельно от самих реквизитов. Mastercard в Европейской экономической зоне (ЕЭЗ), Великобритании и Гибралтаре требует в последующих запросах авторизации по регулярным платежам передавать уникальный Trace ID из ответа на исходную авторизацию, а эмитент должен уметь по нему восстановить исходную транзакцию [46]. У Visa аналогичное требование: после начальной операции нужно сохранить идентификатор транзакции (*transaction identifier*) для всех последующих операций [663].

Visa возвращает NTID в ответе на авторизацию (*Transaction Identifier* в DE 62.2, до 15 цифр, генерирует VisaNet); Mastercard использует термин Trace ID и требует передавать его в DE 48 SE 63 последующих авторизаций — 15 символов фиксированной структуры FNC · BRN · MMDD · spaces. С 2026 года Mastercard вводит параллельный 22-символьный *Transaction Link ID* (TLID): хранение с 2 июня, передача с 23 октября; Trace ID пока сохраняется [46, 663, 666]. Trace ID не равен ARN (DE 31, 23 цифры). Индикаторы CoF/MIT передаются у Visa через SCF (C/R/I) в поле POS Environment DE 126.13; у Mastercard — через DE 48 SE 22 (SF1, SF5); POS Entry Mode 10 — единый код *Credentials on File* для обеих сетей [47, 667, 668]. У Cybersource и других шлюзов поле называется `previousTransactionID` или `networkTransactionID` — разные имена для одного и того же идентификатора.

Хранить идентификатор нужно на уровне подписки. Каждая последующая MIT ссылается на одну и ту же исходную CIT, поэтому идентификатор действует столько же, сколько сама подписка. Когда система хранит его только в записи последней транзакции, при любом сбое записи цепочка обрывается. Поэтому в модели подписки создают отдельное поле, которое заполняется при первой CIT и не перезаписывается последующими ответами [664].

При миграции между провайдерами платёжных услуг (payment service provider, PSP) ТСП переносит токены и историю подписок; идентификатор исходной CIT часто остаётся у прежнего PSP. В следующем цикле ТСП отправляет MIT без ссылки на исходную CIT, и связь между первым согласием и списанием обрывается [46, 664].

Если исходная CIT оформлена некорректно, правки в последующих MIT цепочку согласия не восстановят: идентификатор приходится получать заново через новую CIT с подтверждением клиента.

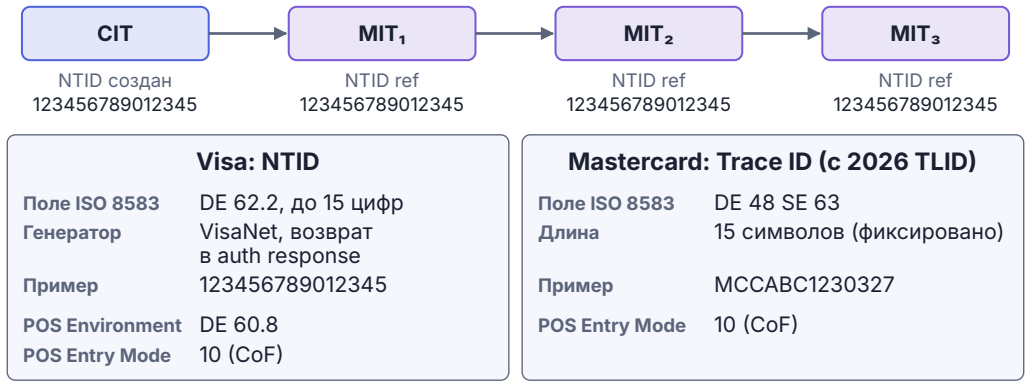


Рис. 61 — Цепочка NTID/Trace ID: форматы полей Visa и Mastercard, индикаторы CoF/MIT, POS Entry Mode 10.

Связка CIT → MIT работает не только в авторизации. В 3DS списания по подписке идут как 3RI-запросы со ссылкой на DS Transaction ID исходной аутентификации (см. гл. 11, раздел о 3RI). В спорах Visa Compelling Evidence 3.0 (см. раздел 32.5) та же ссылка подтверждает, что текущее списание относится к клиенту с подтверждённой историей.

30.4 Мягкий отказ и повторная попытка

Классификация мягких и жёстких отказов и стратегии повторов разобраны в гл. 33. При мягком отказе по MIT ТСП выбирает одно из допустимых действий: новая аутентификация, повтор в разрешённый интервал, обработка кода рекомендаций ТСП (Merchant Advice Code, MAC) или уведомление клиента [13, 46].

Когда отказ требует аутентификации, клиент проходит её заново; ту же MIT не повторяют так, будто аутентификация уже пройдена. Европейское регулирование и правила карточных сетей здесь совпадают: SCA выполняется при создании мандата, и никакая серия повторов её не заменяет [46, 665].

Visa устанавливает для подписочных платежей отдельные требования к уведомлению держателя карты — например, при окончании пробного или промопериода ТСП обязан предупредить клиента не менее чем за 7 календарных дней до первого полного списания; для повторной отправки любой отклонённой авторизации, включая MIT, Visa ограничивает количество попыток по кодам отказа (*decline*): до 20 за 30 дней по Category 2–4, по Category 1 повтор запрещён [13]. Mastercard взимает сбор Excessive Authorization Attempts с любых отклонённых авторизаций сверх 10 попыток за 24 часа или 35 попыток за 30 дней по одному PAN у одного ТСП [669, 670] и требует учитывать MAC, который определяет допустимый интервал и возможность повтора [46]. Эти лимиты установлены на уровне, после которого совокупная доля успешных повторов перестаёт расти, а нагрузка на авторизационную инфраструктуру — продолжает.

Коды MAC 24–30 задают минимальное время ожидания перед повтором: MAC 24 — 1 час, MAC 25 — 24 часа, MAC 26 — 2 дня, MAC 27 — 4 дня, MAC 28 — 6 дней, MAC 29 — 8 дней, MAC 30 — 10 дней. Код 24 рассчитан на временное ограничение баланса, которое исчезнет к следующему расчётному дню, а старшие коды — на ситуацию, когда держатель ждёт пополнения в следующем расчётном цикле. MAC 03 (*Do not*

try again) полностью запрещает повторную отправку по этим реквизитам, а MAC 01 (*New account information available*) указывает, что реквизиты устарели и ТСП должен получить обновлённые данные через сервис Mastercard Automatic Billing Updater (ABU; см. раздел 30.5) или от клиента [46, 287, 671]. Mastercard отслеживает повторные попытки после запрета и взимает с ТСП сбор за каждый повтор после MAC 03.

Visa использует схожую логику через категории кодов отказа (Category 1–4). Отказ с кодом, требующим аутентификации, возвращает клиента в 3DS-цикл; повторная MIT не запускается. Отказ с кодом, допускающим повтор, подпадает под лимит в 20 попыток за 30 дней [13].

Классификатор MAC по коду из DE 48 (Additional Data — Private Use) сводит ответ к решениям: остановить повторы (MAC 03), запросить обновление реквизитов через ABU или Visa Account Updater (VAU; MAC 01) или повторить через предписанный интервал (MAC 24–30). Незнакомый код классификатор трактует как STOP: неучтённый ответ не порождает повторов, за которые карточная сеть взыскала бы сбор. Без такого классификатора биллинг либо повторяет слишком часто и платит сборы за повторы, либо прекращает попытки слишком рано и теряет подписчиков:

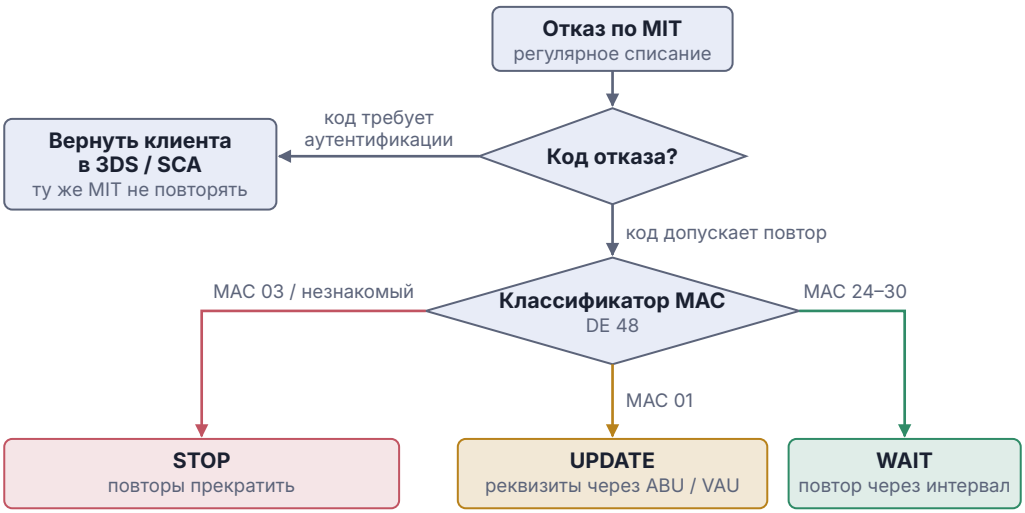


Рис. 62 — Дерево решений по MAC: STOP (03), UPDATE (01), WAIT (24–30).

```python
from dataclasses import dataclass
from enum import Enum

HOUR = 3600
DAY = 24 * HOUR


class Action(Enum):
  RETRY = "retry"  # повтор разрешён, ждать wait_seconds
  STOP = "stop"  # запрет повторов по этим реквизитам
  REFRESH = "refresh"  # реквизиты устарели, получить новые (ABU/VAU)


# Merchant Advice Code -- проприетарный код Mastercard, передаётся в DE 48
# (Additional Data -- Private Use) авторизационного ответа.
# 03 -- Do not try again; 01 -- New account information available;
# 24-30 -- временный отказ, повтор после ожидания.
MAC_DO_NOT_TRY_AGAIN = "03"
MAC_NEW_ACCOUNT_INFO = "01"
```

(продолжение)

```
WAIT_BY_MAC: dict[str, int] = {
  "24": 1 * HOUR,
  "25": 1 * DAY,
  "26": 2 * DAY,
  "27": 4 * DAY,
  "28": 6 * DAY,
  "29": 8 * DAY,
  "30": 10 * DAY,
}

@dataclass(frozen=True)
class Decision:
  action: Action
  wait_seconds: int = 0  # имеет смысл только для Action.RETRY

def classify(mac: str) → Decision:
  if mac == MAC_DO_NOT_TRY_AGAIN:
    return Decision(Action.STOP)
  if mac == MAC_NEW_ACCOUNT_INFO:
    return Decision(Action.REFRESH)
  wait = WAIT_BY_MAC.get(mac)
  if wait is not None:
    return Decision(Action.RETRY, wait_seconds=wait)
  # Неизвестный MAC -- безопасный вариант: не повторять автоматически.
  return Decision(Action.STOP)
```

30.5 Обновление реквизитов

Сервисы обновления реквизитов нужны, когда клиент не менял подписку, но эмитент перевыпустил карту. Старый PAN больше не проходит авторизацию; ТСП продолжает отправлять списания по устаревшим данным.

VAU и ABU — сервисы соответственно Visa и Mastercard, которые передают ТСП обновлённые реквизиты от участвующих эмитентов, когда карта истекла или была перевыпущена [672, 673]. В правилах Mastercard участие в ABU обязательно для эмитентов, с исключениями по отдельным типам карт, а ТСП подключаются добровольно [46]. Visa называет аналогичный механизм управлением жизненным циклом реквизита (*credential lifecycle management*): PAN и сетевые токены обновляются в реальном времени до очередного списания [674].

Пакетное обновление работает по расписанию: ТСП или PSP отправляет файл с реквизитами, эквайер передаёт ответы VAU в течение двух рабочих дней, а ТСП обязан применить их в течение пяти рабочих дней после получения [675]. Для подписок с месячным циклом этого достаточно, если файл отправляется заблаговременно. Обновление в реальном времени встроено в сам авторизационный запрос: когда реквизиты устарели, ответ содержит обновлённые данные, и ТСП сохраняет их сразу. У Visa это Real Time VAU [673]; Mastercard передаёт обновления через Payment Account Management API, который снабжает ABU данными от эмитента по мере перевыпуска [46]. С 01.04.2025 Mastercard повысил штраф Credential Continuity Program — $0,09 за каждую транзакцию по устаревшим реквизитам, если ТСП не подключён к ABU или игнорирует обновления; ставка выросла втрое от прежних $0,03 [669].

Покрытие зависит от участия эмитента. Не каждый банк подключён к ABU или VAU, не каждый тип карты участвует в процессе обновления. Visa рекомендует подключать все идентификационные диапазоны эмитента (Bank Identification Number, BIN), включая перезагружаемые предоплаченные карты (*reloadable prepaid*), но неперезагружаемые предоплаченные карты и продукты малых эмитентов остаются вне сервиса, если эмитент или программа карты не участвует в обновлении. Обновление

Таблица 43 — Account Updater (VAU/ABU) и сетевая токенизация: сравнение

Параметр	Account Updater: Visa VAU / Mastercard ABU	Сетевая токенизация: Network Tokens
У продавца хранится	PAN и срок действия	токен сети, PAN не виден
Кто инициирует	эмитент → сеть → продавец	сеть меняет PAN под токеном
Канал доставки	batch-файлы или real-time в авторизации	прозрачно при авторизации
Что обновляется	PAN, expiry в базе продавца	исходный PAN у сети, токен прежний
Покрытие	участвующие BIN, не все типы карт	все токенизированные карты
Цена неучастия	Mastercard: $0,09 за устаревшую	штрафа сети нет

реквизитов снижает технический отток; для карт вне покрытия остаётся ручной запрос новых данных у клиента.

Сетевые токены меняют ответственность за обновление: когда ТСП хранит не PAN, а сетевой токен, при перевыпуске карты привязка обновляется автоматически — токен остаётся прежним, исходный PAN (underlying PAN, реальный номер карты, на который сеть отображает токен) обновляется на стороне карточной сети [674]. Пакетные файлы для токенизированных реквизитов не нужны.

ТСП отправляет MIT по карте с истёкшим сроком, а сервис обновления реквизитов (ABU/VAU) недоступен — пакетный файл не обработался или запрос в реальном времени вернул ошибку. Эмитент отклоняет по коду 54 (Expired Card). ТСП должен уведомить клиента и попросить обновить реквизиты вручную. Когда ТСП вместо этого повторяет тот же запрос, он расходует лимит попыток и платит карточной сети сбор за избыточные повторы.

Другой случай: сетевой токен обновился при перевыпуске карты, underlying PAN изменился на стороне TSP, но первая же MIT по обновлённому фондирующему PAN (Funding PAN, FPAN — реальный номер карты, в который сеть детокенизирует токен при авторизации) получает отказ с кодом 62 (Restricted Card), потому что новая карта выпущена с ограничениями по коду категории ТСП (Merchant Category Code, MCC) или по каналу CNP. Токен действителен, но авторизация не проходит; повтор бесполезен, потому что ограничение задано на стороне эмитента. После такого отказа ТСП уведомляет клиента, запрашивает новый платёжный инструмент или, если такая возможность есть, обращается к эмитенту через PSP для отмены ограничения.

Отток из-за платёжных отказов (*involuntary churn*), то есть уход подписчика помимо его решения, по оценкам Recurly, Spreedly и других вендоров биллинга составляет 3–5 % подписочной базы в месяц; успешность ABU/VAU при обновлении реквизитов по тем же оценкам — 85–90 % для карт участвующих эмитентов. Это агрегированные показатели по портфелям подписочных продуктов; карточные сети таких данных не публикуют. Сетевые токены повышают долю успешных обновлений, потому что обновление происходит автоматически на стороне TSP и не зависит от пакетного цикла.

30.6 Биллинг-движки поверх карточного протокола

SCF, NTID, MIT, CIT, *recurring* против *unscheduled* задают **протокол карточной сети**. Биллинг-движок решает задачи, которых нет в сетевом протоколе: выставление счетов (invoicing), пропорциональное начисление при изменении тарифа (proration), повторные попытки списания при отказе (dunning), отмена и возврат, налоговая обработка.

Пограничные случаи (*edge cases* — изменение цикла, перерасчёт скидок, состояния заморозки (*freeze*), валютные конверсии при подписке в другой валюте, налоги по юрисдикции клиента) быстро выходят за пределы первоначальной спецификации самописного биллинга. Под эти задачи сформировался отдельный от PSP рынок готовых биллинг-движков.

Stripe Billing [676] — встроенное в Stripe решение, интегрированное с Payments и налоговым сервисом Stripe Tax; поддерживает модели по потреблению (*usage-based*) и по фиксированной цене (*fixed-price*), повторные попытки списания (*dunning*), декларирует восстановление 55 % неуспешных списаний в среднем по портфелю. Chargebee [677] и Recurly [678] — независимые SaaS-платформы, не привязанные к одному PSP; работают в сегменте B2B SaaS: Chargebee поддерживает гибкие модели ценообразования (*pricing*), Recurly специализируется на восстановлении выручки (*revenue recovery*) и ML-настройке dunning. Lago [679] — биллинг с открытым исходным кодом (*open source*) под AGPL-3.0, альтернатива Stripe Billing; версия для самостоятельного развёртывания (*self-hosted edition*) не ограничена по объёму. Kill Bill [680] — открытая платформа повторяющейся выручки (*recurring revenue*) под Apache 2.0, развивается с 2010 года; рассчитана на сложные схемы с собственными правилами начислений поверх ядра.

Движок выбирают по типу модели ценообразования (*usage-based*, *subscription* или гибрид), требованию к самостоятельному развёртыванию (*self-hosting*; открытый исходный код или SaaS) и независимости от конкретного PSP. Независимость от PSP важна, когда ТСП работает через несколько эквайеров параллельно: встроенные в один PSP движки не дают маршрутизировать списания между ними.

30.7 Снижение оттока в подписках

Отток подписчиков по платёжным отказам сокращается там, где сохранён технический контекст согласия. Корректная цепочка NTID сообщает эмитенту, что запрос — продолжение известного мандата: эмитент применяет менее строгую политику антифрода, и доля одобрений на MIT с корректным NTID выше, чем на запросах без истории.

Первая CIT должна пройти и зафиксировать согласие: идентификатор исходной авторизации и токен реквизита сохраняются на уровне подписки, а не в записи последней транзакции. Каждый последующий биллинговый цикл — MIT с корректными флагами SCF и ссылкой на ту же NTID. При перевыпуске карты сетевой токен или ABU/VAU обновляют реквизиты автоматически; для карт вне покрытия и отказов с MAC 01 данные получают только от клиента вручную.

Когда эмитент возвращает отказ, требующий аутентификации, MIT не повторяется — клиент проходит новый цикл CIT и даёт новое согласие. Для отказов с MAC 24–30 повтор идёт по предписанному интервалу, для MAC 03 — останавливается. Игнорирование этих сигналов ведёт либо к сборам карточной сети за избыточные повторы, либо к преждевременной отписке платёжеспособного клиента.

По картам с истёкшим сроком или ограничениями эмитента причина отказа уже не в сетевом протоколе: без уведомления клиент не узнает, что списание не прошло. Минимальный набор уведомлений по подписке должен включать дату следующего списания, информацию о неуспешной попытке и канал обновления реквизитов.

Когда у карты нет ни сетевого токена, ни записи в ABU/VAU, карточная сеть данные не обновит, и удержание подписчика зависит от прямого сообщения клиенту. Предупреждающие письма (*pre-dunning*) за 7–30 дней до истечения карты, ссылки на обновление реквизитов без повторной аутентификации (Stripe payment update link, Recurly Hosted Account Management Page) и баннеры внутри приложения возвращают часть подписчиков, которых без этих мер отказ перевёл бы в *involuntary churn* по истечении льготного периода (*grace period*). Метрика — доля восстановленных подписок (*recovery rate*) за 7–14 дней после первого отказа; по данным Recurly, базовая логика повторов восстанавливает около 53 % отклонённых списаний, оптимизированная — около 71 %, и 90 % восстановлений приходится на первые 10 дней [681]. Биллинг-движок связывает код отказа, MAC, момент разрешённого повтора и текст уведомления клиенту: без этой координации SCF/NTID сохраняют авторизационный контекст, но клиент не получает письма, не обновляет карту и отписывается после льготного периода.

ПРАКТИКА

Цепочка NTID — технический эквивалент письменного согласия: без неё каждое автосписание начинается с нуля.

31 Сверка

Когда деньги «теряются», расходятся записи о них. В журнале авторизаций покупка уже разрешена; в клиринговом файле её ещё нет; в банковской выписке видна только нетто-сумма после комиссий и взаимных вычетов. Сверка возвращает эти следы к одной операции.

Внутренний реестр обязательств из гл. 35 показывает, какое денежное состояние видит продукт. Сверка проверяет, совпадает ли эта внутренняя картина с внешними файлами сети, эквайера и банка. Если смешать эти два уровня, команда начнёт сравнивать несопоставимые величины и искать потери там, где есть разница между моделями учёта.

31.1 Расхождения между следами операции

Карточная операция оставляет несовпадающие следы. Авторизация фиксирует право провести операцию, клиринг закрепляет её окончательный денежное выражение, расчётная позиция сводит обязательства сети, а банковская выписка показывает фактическое движение средств с комиссиями и взаимными вычетами. Эти записи не обязаны быть идентичными.

Первое расхождение — между авторизацией и клирингом. Ресторан может авторизовать счёт на одну сумму, а после чаевых отправить в клиринг другую; отель сначала блокирует предварительный депозит, а потом предъявляет итоговую стоимость проживания; авиакомпания доначисляет часть сборов уже после исходной покупки. Сверка на этом уровне сводится к поиску пары: для каждой клиринговой записи нужно найти соответствующую авторизацию и проверить, укладывается ли расхождение в допустимые пределы [46, 55].

Второе расхождение — между клирингом и расчётной позицией. За день может пройти сто транзакций, но в расчётном отчёте эквайер увидит свёрнутую итоговую сумму. Сравнивать поток операций с результатом его нетто-свёртки нельзя. В публичных правилах Mastercard нетто-расчёт описан как базовая модель, а прямой двусторонний расчёт между участниками допускается как исключение; Visa формирует нетто-позицию расчёта для участников BASE II (файлового клирингового сервиса VisaNet в процессинговой сети Visa) через VisaNet Settlement Service [13, 15, 682].

Третье расхождение — между расчётной позицией и банковской выпиской. Расчётная позиция в системе сети может уже считаться закрытой, а движение по корреспондентскому счёту пройти позже, в другом расчётном дне или даже в иной валюте после пересчёта. Здесь сопоставляют расчётный файл и банковскую выписку по счёту урегулирования; отдельные транзакции на этом уровне не рассматриваются. Mastercard Rules требуют ежедневно сверять внутренние записи с расчётными отчётами сети и устранять расхождения на этом уровне [15].

Сценарий A (первое расхождение). День 1: ресторан авторизует 5 000 руб., холд создан. День 2: клиринговый файл приходит с суммой 5 200 руб. (чаевые 200 руб.); сверка сопоставляет запись по ARN (Acquirer Reference Number) и коду авторизации, но фиксирует расхождение в 200 руб.

Сценарий B (*orphan authorization* — авторизация без последующего клиринга). День 1: авторизация на 800 руб. в рознице с физическим присутствием карты (*retail*

card-present). День 3: клиринга на 800 руб. нет; срок представления (*presentment window* — период, в течение которого клиринговая запись должна быть передана сети после авторизации) ещё не истёк, запись ожидает клиринга. День 6: срок представления для *retail card-present* по Visa после реформы Authorization Framework от 13.04.2024 (5 календарных дней) истекает[1]; запись перемещается в очередь исключений как *orphan authorization*. Холд снимается автоматически.

Сценарий C (второе и третье расхождения). День 3: в расчётном файле сети нетто-позиция за день составляет 4 800 руб. (5 200 руб. клиринга минус 400 руб. встречных обязательств). Так проявляется второе расхождение. День 4: банковская выписка показывает зачисление 4 795 руб. Разница в 5 руб. объясняется комиссией за расчётное обслуживание, которая не видна в файле сети. Так проявляется третье расхождение.

С марта 2022 года международные сети Visa и Mastercard для карт российских эмитентов закрыты: такие карты обрабатываются только внутри России через ОПКЦ (операционный и платёжный клиринговый центр) НСПК (Национальная система платёжных карт) [5, 75]. Разделы 31.2–31.5 разбирают сверочные форматы и правила сетей в их международной редакции; разделы 31.7–31.8 — сверку внутрироссийских операций через НСПК, кобейджи и СБП. Для российских эквайеров, обслуживающих карты иностранных эмитентов, и для дочерних структур российских банков за рубежом применимы обе части.

31.2 BASE II и IPM

Клиринговые файлы сетей фиксируют завершённые транзакции в машинном формате; бухгалтерский результат появляется после разбора, агрегации и сопоставления с расчётом. В публичных правилах Visa этот формат описан через BASE II, у Mastercard — через IPM (Integrated Product Messages — семейство клиринговых форматов Mastercard, исторически обслуживаемых Global Clearing Management System, GCMS) [13, 283, 684]. После марта 2022 года BASE II и IPM в России остаются рабочими форматами для эквайеров, обслуживающих карты иностранных эмитентов, и для дочерних структур российских банков за рубежом; внутрироссийский трафик идёт через ОПКЦ НСПК (раздел 31.7).

Visa определяет BASE II как файловый сервис VisaNet, который собирает, проводит клиринг, рассчитывает и доставляет файлы финансовой и нефинансовой активности между Visa и участниками. В приложении к публичным правилам перечислены семейства форматов BASE II: Transaction Code (TC) групп 01–49 и 50–92 (каждая запись делится на подзаписи Transaction Code Record, TCR0–TCR7), а отдельно опубликованы материалы по VisaNet Settlement Service, который выдаёт нетто-позицию расчёта и расчётные отчёты для участников BASE II [13].

Mastercard, в отличие от Visa, публично раскрывает именно термин Integrated Product Messages (IPM) Clearing Formats как часть своих стандартов, а Transaction Processing Rules регулярно ссылаются на поля сообщения First Presentment/1240, описанные в руководстве IPM Clearing Formats [46, 684]. Клиринг передаётся отдельным от авторизации сообщением.

[1] До 13.04.2024 срок представления для *retail card-present* у Visa зависел от типа продукта, присутствия карты и сегмента ТСП [683]; после реформы все CP-операции и операции по инициативе ТСП (*merchant-initiated*) получили единый срок 5 календарных дней, для CNP-операций по инициативе держателя — 10 дней, при предварительной авторизации у lodging, vehicle rental, cruise line — 30 дней [13].

Visa BASE II и Mastercard IPM сообщают одно и то же: факт завершённой операции с её денежным выражением, но структура полей различается. В BASE II идентификаторы сопоставления находятся в Transaction Code (TC) и связке ARN с RRN (Retrieval Reference Number); в IPM/1240 для этого служат DE 31 (Data Element 31 — Acquirer Reference Data) и DE 48 (Additional Data) сообщения ISO 8583/IPM (см. [74]) [13, 46]. Валюта транзакции и валюта расчёта кодируются в разных полях, а формат представления суммы (с разделителем или без, с фиксированной точностью или плавающей) различается между сетями. В табл. 44 сведены состав DE для IPM 1240 First Presentment и подтверждённые позиции TCR 0 для Visa TC 05 в TC 33.A по Visa Acceptance Developer Portal [685] и Mastercard GCMS Reference Manual 2021 [14]. Внутренняя структура 23-значного ARN одинакова в обеих сетях: позиция 1 как *mixed use*, 2–7 — BIN эквайера, 8–11 — дата формата YDDD (год + порядковый день года), 12–22 — порядковый номер, 23 — проверка по алгоритму Луна [685].

Перед сопоставлением приведите каждую клиринговую запись к единой внутренней модели: общий идентификатор операции, сумма в минорных единицах валюты, дата обработки в одном часовом поясе, код валюты по ISO 4217 (международный стандарт трёхбуквенных и трёхзначных кодов валют) [84]. Без этого шага алгоритм сопоставления будет путать разницу форматов с денежным расхождением.

Парсер собирает клиринговую запись, извлекает поля сопоставления и передаёт их в механизм сверки. Разбирать Visa BASE II и Mastercard IPM одним парсером нельзя: каждой сети нужен свой адаптер или аккуратное промежуточное представление, иначе ошибка возникает ещё до бухгалтерии, на этапе разбора файла.

31.3 Нетто- и валовой расчёт

Сумма транзакций редко совпадает с тем, что пришло на расчётный счёт: карточные системы выдают результат нетто-свёртки; отдельные операции восстанавливаются из клиринговой детализации и правил сети. По умолчанию работает нетто-расчёт, валовой остаётся исключением.

В модели нетто-расчёта («netting» — итоговое сальдо взаимных обязательств за период) сеть сворачивает все позиции дня — покупки, возвраты и комиссии — в одну сумму, которую видит эквайер. Такая модель уменьшает количество отдельных переводов и делает расчётную инфраструктуру дешевле и проще в эксплуатации.

Валовой расчёт («gross settlement») проводит каждую операцию или небольшую группу операций отдельной расчётной позицией по полной сумме, без свёртки встречных обязательств. Учёт становится подробнее, а дисциплина сверки — строже.

ТСП не выбирает модель расчёта напрямую: базовую модель для участника определяет сеть, а эквайер закрепляет её в условиях договора. Mastercard описывает нетто-расчёт как стандартный; прямой двусторонний расчёт возможен, но требует отдельного соглашения между участниками [15]. Visa формирует нетто-позицию через VisaNet Settlement Service [13]. Для PSP или маркетплейса расчётная модель наследуется от эквайера, и менять её в одностороннем порядке нельзя. Для участников ПС Мир и для внутрироссийского трафика Visa/Mastercard нетто-позицию формирует ОПКЦ НСПК и передаёт в Банк России для расчёта по корсчетам [5, 75].

Нетто-свёртка содержит несколько компонентов: покупки, возвраты, *interchange fee* (межбанковская комиссия, которую эквайер платит эмитенту по каждой операции; ставки и категории публикуются сетями и регуляторами [20, 21]), *assessments* (сборы сети с эквайера за обработку объёма) и штрафные списания. Для сверки

Таблица 44 — Visa TC 05 в TC 33.A (TCR 0) и Mastercard IPM 1240 First Presentment: состав полей

Поле	Поз. / DE	Значение
Visa BASE II / TC 33.A → TC 05: Sales Draft, TCR0 (168 байт)		
Transaction Code	1–2	05 Sales Draft
TCR Sequence Number	4	0
Application Code	17–20	BASE
Message Identifier	21–35	ACQUIRER0000001
Account Number (PAN)	—	4242 4242 4242 4242
Acquirer Reference Number	—	72711493163001285828825
Acquirer Business ID	—	10054321
Purchase Date (MMDD)	—	0612
Destination Amount	—	100.00
Destination Currency Code	—	826 GBP
Merchant Name / City	—	STORE EXAMPLE / LONDON
Merchant Country / MCC	—	GBR / 5651
Auth Code	—	107090
POS Entry Mode	—	01
Action Code	135–146	5 (TC 05 clearing record)
Mastercard IPM 1240: First Presentment, Function Code 200		
Message Type Identifier	MTI	1240
Primary bitmap (DE 1–64)	BMP1	F000 0142 0CC1 E000
Secondary bitmap (DE 65–128)	BMP2	0200 0004 0000 0000
PAN	DE 2	5555 5555 5555 4444
Processing Code	DE 3	000000
Amount, Transaction	DE 4	000000010000 (=100.00)
Function Code	DE 24	200 First Presentment
MCC	DE 26	5651
Acquirer Reference Data	DE 31	72711493163001285828825
Retrieval Reference Number	DE 37	316300273056
Approval Code	DE 38	107090
Card Acceptor Terminal ID	DE 41	01234567
Card Acceptor ID Code	DE 42	1087654321
Additional Data (PDS)	DE 48	PDS 0023 / 0148 / 0158 / 0165
Currency, Transaction	DE 49	826 GBP
Currency, Reconciliation	DE 50	826
Currency, Cardholder Billing	DE 51	826
Message Number	DE 71	00000796
Transaction Originator Inst.	DE 94	024354

Одна успешная розничная покупка — два формата клиринга: 100,00 GBP, MCC 5651 (Family Clothing); PAN — тестовые номера Stripe; значения иллюстративные, состав полей — из первичных спецификаций. Поз. — позиция в записи TCR0 Visa, DE — элемент данных IPM Mastercard.

каждый компонент выделяют отдельно. Итоговая сумма по выписке должна складываться как покупки минус возвраты минус *interchange* минус *assessments* минус прочие удержания. Если не раскрыт хотя бы один компонент, разница между ожидаемой и фактической суммой становится неопознанным расхождением, которое команда расследует вручную каждый расчётный день.

Рис. 63 — Нетто- и валовой расчёт: 100 транзакций в одну позицию.

Если сеть работает по нетто-модели, искать в банковской выписке сумму всех покупок за день бессмысленно. Сначала сверяют клиринговый поток с расчётной позицией, а потом расчётную позицию с банковской выпиской.

ПРАКТИКА

Не сравнивайте авторизационный журнал сразу с банковской выпиской: авторизация ещё не стала клирингом, выписка уже отражает расчёт. Порядок сверки: авторизация против клиринга, клиринг против расчётной позиции, расчётная позиция против выписки.

31.4 Исключения

Каждую транзакцию, не сошедшуюся автоматически, относят к известному типу и направляют на автоматическую или ручную обработку.

Первый тип — расхождение суммы: в ресторане авторизовали одну сумму, а в клиринге пришла другая, в гостинице предварительный холд не совпал с окончательным чеком. Такая запись требует проверки допустимого отклонения, и если порог превышен, она попадает в очередь исключений [13].

Вторая группа исключений — клиринг без авторизации. Причина — *force post*, технический сбой или сценарий, когда авторизация прошла вне основного авторизационного потока. Каждую такую запись нужно объяснить: это либо допустимый сценарий, либо признак риска.

Обратная проблема — авторизация без клиринга, когда операция была разрешена, но в клиринг не попала из-за ошибки маршрутизации, сбоя у ТСП или истечения срока представления. Если не закрыть запись вовремя, держатель карты увидит только холд, а ТСП не получит выручку.

Ещё один сценарий — дубликаты в клиринговом файле. Если эквайер отправляет одну и ту же запись дважды из-за ошибки повторной передачи или сбоя пакетного обработчика, а сеть не отфильтровала дубль, эмитент получает два идентичных требования. Дубликат обнаруживает эмитент при сверке, когда видит два клиринга к одной авторизации. Visa и Mastercard отзывают клиринговую запись по-разному. У Visa BASE II эквайер заменяет код транзакции дублирующей записи кодом клирингового *reversal*, остальные данные не меняет и отправляет исправленный файл в следующий день передачи [13]. У Mastercard IPM отдельного MTI на отмену клиринга нет: используется тот же First Presentment/1240 с приватным подэлементом данных PDS 0025 (Message Reversal Indicator) со значением «R» и датой исходного сообщения; такая запись указывает получателю игнорировать оригинал [14]. Дубликат опаснее расхождения в сумме: каждая запись в отдельности выглядит корректной, и команда сверки может пропустить двойное списание.

В многошаговой правке новая запись ссылается на промежуточное сообщение. После исходной операции источник присылает её отмену, правку этой отмены и финансовое представление со ссылкой на последнюю правку. Внутреннюю последовательность определяет сам источник. Если он переназначает идентификатор промежуточной записи, меняет порядок записей или сводит две правки в одну, финальная запись ссылается на промежуточную запись из внутренней истории источника. Привязку к исходной операции восстанавливает устойчивый ключ: сетевой идентификатор транзакции (раздел 30.3); второй вариант — RRN исходной операции вместе с суммой и датой. Названия типов, которыми источник помечает записи, ненадёжны. «Корректировка» и «первичная операция» — ярлыки конкретного источника. В карточном процессинге правку несут отмена, частичная отмена, *reversal* и возврат, поэтому у разных источников одинаковые ярлыки значат разные процедуры.

Late presentment — транзакция дошла до сети позже применимого срока представления. У Mastercard это создаёт риск chargeback из-за истечения периода защиты от спора, а у Visa до 12 апреля 2024 года было закреплено отдельное основание спора Condition 12.1 (Late Presentment); с 13 апреля 2024 года Visa объединила его с Condition 11.3 «No Authorization» [13, 46]. Помимо бухгалтерской классификации команда сверки проверяет, нарушен ли срок представления и создаёт ли это основание для спора по правилам сети. Внутри России через ОПКЦ НСПК сроки представления и основания возвратов закреплены правилами ПС Мир; коды Visa и Mastercard здесь не применяются [75].

31.5 DCC и мультивалютный расчёт

Устройство DCC, распределение курсового риска и маршрутизация конвертации — в гл. 36. DCC меняет точку фиксации курса, и часть расхождений возникает из сочетания валюты транзакции, валюты расчёта сети, даты обработки и наценки DCC. Сверка отделяет курсовое отклонение от неверной проводки.

После марта 2022 года карты российских эмитентов Visa и Mastercard за рубежом не принимаются, поэтому DCC на стороне держателя российской карты за пределами РФ неприменима. DCC сохраняет смысл на стороне российских эквайеров, обслуживающих карты иностранных эмитентов в ТСП в России, и в сценариях кобейджа «Мир–UnionPay» и «Мир–JCB», где конверсию выполняет партнёрская сеть.

Мультивалютная сверка идёт по шагам: (1) зафиксировать валюту транзакции (в Mastercard IPM — DE 49), валюту расчёта (DE 50) и, если применимо, валюту

биллинга (DE 51); транзакция с DCC помечается DE 54 с типом суммы 58 [314]; (2) хранить дату и курс конвертации рядом с записью; (3) отделять наценку DCC от конвертации по правилам сети; (4) сверять расчётную позицию в валюте расчёта (валюта транзакции для этого шага не подходит). Если пропущен хотя бы один шаг, система показывает расхождения, объяснимые курсовой механикой.

31.6 Автоматизация сверки

Механизм сопоставления находит одну и ту же операцию в разных представлениях и работает проходами: строгий, мягкий, ручная очередь. Сначала задаётся общая ссылка `reference`; затем для строгого и мягкого проходов проверяются поля и допуски. Чем слабее критерии сопоставления, тем аккуратнее должна быть ручная проверка. Если на третий проход регулярно приходится больше 2–3 % записей, причина — в качестве входных данных или в пропущенном сценарии, а не в алгоритме. Таблица 45 показывает пример строки на каждом проходе с иллюстративными долями.

Таблица 45 — Проходы сверки: строгий, мягкий, ручная очередь

source	reference	amount	date	card
Pass 1: строгий, ARN+сумма+дата; matched, ≈85 %				
internal	ARN 72711493163001285828825	100,00 GBP	2023-06-12	4242 4242 4242 4242
external	ARN 72711493163001285828825	100,00 GBP	2023-06-12	4242 4242 4242 4242
Pass 2: мягкий, сумма+карта; soft, ≈12 %				
internal	RRN 316300273057	50,00 GBP	2023-06-12	5555 5555 5555 4444
external	ARN 32827643165001473829166	50,00 GBP	2023-06-14	5555 5555 5555 4444
Pass 3: ручная очередь; manual, ≈3 %				
internal	ARN 92831563163001473829166	95,00 GBP	2023-06-12	4242 4242 4242 4242
external	ARN 88142533164860392856103	75,00 GBP	2023-06-13	5555 5555 5555 4444

Общая ссылка записи `reference` — RRN на стороне авторизации, ARN или эквивалент в клиринге; для механизма сверки важно, чтобы строка была одинаково построена в обоих источниках. Строгий проход сравнивает одновременно поля: общую ссылку, сумму вместе с валютой и дату в допуске ± 1 день. Мягкий отменяет требование к `reference` (RRN авторизации и ARN клиринга могут не совпасть при *late presentment*), расширяет допуск до ± 2 дней и выбирает ближайшую по времени из доступных — поэтому находит позднее представление и смену идентификатора между авторизационным и клиринговым представлениями одной операции. Многошаговую правку механизм сопоставляет через исходную операцию. Записи, не сопоставленные ни одним проходом, попадают в `only_internal` или `only_external` — очереди исключений: продукт зафиксировал операцию, сеть её не подтвердила, либо сеть прислала запись, для которой у продукта нет авторизации.

```
from dataclasses import dataclass


@dataclass(frozen=True)
class Record:
  # RRN (DE 37) на стороне авторизации; ARN/Acquirer Reference (DE 31
  # в IPM, эквивалент в BASE II) на стороне клиринга. Реконсилиатору
  # достаточно того, что строка одинаково построена в обоих источниках.
  reference: str
  amount: int  # минорные единицы
  currency: str  # ISO 4217
  ts: float  # epoch seconds


@dataclass
class MatchResult:
  matched: list[tuple[Record, Record]]
  only_internal: list[Record]
  only_external: list[Record]


def reconcile(
  internal: list[Record],
  external: list[Record],
  strict_tolerance: float = 86_400,  # +-1 день
  soft_tolerance: float = 2 * 86_400,  # +-2 дня
) → MatchResult:
  int_taken = [False] * len(internal)
  ext_taken = [False] * len(external)
  pairs: list[tuple[Record, Record]] = []

  # Проход 1 (строгий): reference + currency + amount, дата в strict_tolerance.
  for i, irec in enumerate(internal):
    for j, erec in enumerate(external):
      if ext_taken[j]:
        continue
      if irec.reference ≠ erec.reference:
        continue
      if irec.amount ≠ erec.amount or irec.currency ≠ erec.currency:
        continue
      if abs(irec.ts - erec.ts) > strict_tolerance:
        continue
      pairs.append((irec, erec))
      int_taken[i] = True
      ext_taken[j] = True
      break

  # Проход 2 (мягкий): currency + amount, дата в soft_tolerance.
  # reference не сравниваем -- авторизационный RRN и клиринговый ARN
  # это разные идентификаторы, и при late presentment их связь теряется.
  # Из подходящих выбираем ближайшую по времени.
  for i, irec in enumerate(internal):
    if int_taken[i]:
      continue
    best_j: int | None = None
    best_delta: float = 0.0
    for j, erec in enumerate(external):
      if ext_taken[j]:
        continue
      if irec.amount ≠ erec.amount or irec.currency ≠ erec.currency:
        continue
      delta = abs(irec.ts - erec.ts)
      if delta > soft_tolerance:
        continue
      if best_j is None or delta < best_delta:
        best_j = j
        best_delta = delta
    if best_j is not None:
      pairs.append((irec, external[best_j]))
      int_taken[i] = True
      ext_taken[best_j] = True

  return MatchResult(
    matched=pairs,
    only_internal=[r for i, r in enumerate(internal) if not int_taken[i]],
    only_external=[r for j, r in enumerate(external) if not ext_taken[j]],
  )
```

Late presentment даёт ложные расхождения. Транзакция авторизована вчера, но клиринговая запись появляется через два-три дня. Если сверка закрывает день жёстко по календарной дате, такая запись останется несопоставленной до прихода клиринга, а потом потребует ручного сопоставления. Надёжнее выдерживать допустимый срок ожидания: несопоставленные авторизации ждут клиринга в течение разрешённого правилами сети срока представления и только после его истечения попадают в очередь исключений. После реформы Visa Authorization Framework от 13.04.2024 эти сроки таковы: 5 календарных дней для операций *card-present* и для всех *merchant-initiated transactions*; 10 дней для CNP-операций по инициативе держателя и для категорий аренды (*rental*) с предварительной авторизацией (*estimated authorization*: aircraft rental, bicycle rental, boat rental, clothing and costume rental, DVD and video rental, equipment rental, furniture rental, motor home rental, motorcycle rental, trailer parks); до 30 дней при предварительной авторизации у T&E-категорий cruise line, lodging, vehicle rental, а также для CNP по инициативе держателя при подключённом сервисе Extended Authorization Service (EAS) [13].

Состояние сверки показывают метрики: доля автоматически сопоставленных записей (*match rate*), средний возраст несопоставленной записи и размер очереди исключений на конец дня. Приемлемые пороги у каждого процессора свои и зависят от стабильности форматов клиринговых файлов, доли возвратов и качества клиентских реквизитов; универсальных эталонных значений этих метрик в открытых источниках нет, поэтому ориентир — собственный исторический ряд. Если доля сопоставления падает, причина — в изменении формата файла или в новом сценарии, который парсер не поддерживает. Если возраст несопоставленных записей растёт, очередь перегружена, и команда не справляется с ручным разбором.

Готовый сервис сверки имеет смысл там, где нет прямого доступа к сетям или объём транзакций не оправдывает собственной разработки. Свой механизм строят при сложном мультивалютном процессе, собственной ERP (Enterprise Resource Planning — учётная система предприятия) и нестандартных правилах нетто-расчёта.

ПРАКТИКА

Наиболее стойкие ложные расхождения в сверке связаны с датой отсечки. Расчёт сети привязан к времени закрытия расчётного дня, а не к календарной дате. Транзакция, прошедшая поздно вечером, может попасть в следующий расчётный день. Если система жёстко привязана к календарной дате, фиктивные расхождения будут появляться регулярно, особенно в конце недели и перед праздниками.

31.7 Клиринг и сверка ПС Мир через НСПК

Архитектура ОПКЦ НСПК и жизненный цикл внутрироссийской карточной операции — в гл. 16 (раздел 16.2).

Клиринговые файлы НСПК для сверки по картам «Мир» несут собственные коды причин и идентификаторы [75].[1] Эквайер и эмитент сверяют данные сразу на нескольких стыках: между собственным авторизационным журналом и клиринговой записью НСПК (типичный случай — пропущенный или поздно поступивший *reversal*), между клиринговой позицией ОПКЦ и расчётным отчётом (комиссии, плата за услуги ОПКЦ), между расчётным отчётом и движением по корсчёту в Банке России.

[1] Имена файлов, периодичность формирования и состав полей описаны в закрытой документации НСПК.

Карты кобейджа «Мир–UnionPay» (международная карточная платёжная система Китая; за пределами Китая представлена дочерней компанией UnionPay International) и «Мир–JCB» (Japan Credit Bureau, японская международная карточная платёжная система) добавляют параллельный процесс. Транзакции, прошедшие за рубежом через сеть партнёра, возвращаются в местный процессинг уже как зарубежная операция эмитента, со своим клиринговым форматом UnionPay International или JCB. Эмитенту программы кобейджа приходится поддерживать несколько процессов сверки одновременно.

31.8 Сверка платежей по СБП

C2B-операции (consumer-to-business — платежи физического лица в адрес бизнеса) по СБП (Система быстрых платежей; см. гл. 19, раздел 19.2) устроены иначе, чем карточные. У СБП нет двухтактной логики «авторизация и потом клиринг»: исполненный перевод окончателен и сразу учтён на корсчёте получателя. Поэтому сверка по СБП проверяет связку между платёжной сессией ТСП и фактическим зачислением на расчётный счёт.

Источников данных у ТСП несколько: собственный журнал платёжных сессий и заказов; реестр операций от банка-эквайера или PSP, полученный по протоколу ОПКЦ СБП (раздел 19.7); банковская выписка по расчётному счёту ТСП. Сверка СБП сопоставляет эти потоки по идентификатору операции `trxId` (или его аналогу в API банка-партнёра), проверяет совпадение сумм и по необходимости выявляет частичные возвраты как отдельную последовательность операций.

Финальность перевода означает, что между «ожидает подтверждения» и «исполнен» нет отдельного клирингового шага. Расхождения, которые у карточных сетей сглаживаются клиринговым сроком представления, в СБП проявляются немедленно и требуют разбора до закрытия дня. Возврат проходит отдельным переводом и сопоставляется с исходным платежом. Идентификатор исходной операции задаёт связь: на уровне протокола ОПКЦ это `originalTrxId` [364]. Реестр сверки СБП хранит такой перевод как возвратную операцию (см. раздел 32.8).

B2C-выплаты (business-to-consumer — выплаты бизнеса в адрес физических лиц) по реестру требуют отдельного процесса. Сверку ведут по реестру в целом и по каждой строке отдельно: с проверкой идемпотентности строк, повторной отправкой только ошибочных позиций и отдельным контролем статуса каждого получателя.

ПРАКТИКА

Если ваш продукт принимает оплаты и через карты, и через СБП, держите две независимые системы сверки. Общим остаётся только формальный объект — продажа, с которой связан один или несколько расчётных потоков.

Главная метрика сверки — скорость локализации расхождения. У зрелого процессинга расхождение получает имя — сумма, дубль, *late presentment*, курсовая разница DCC — в течение того же дня, а не остаётся в общей очереди «непонятное». После марта 2022 года расхождения из начала главы проходят по разным циклам: внутренний российский трафик — через ОПКЦ НСПК, карты иностранных эмитентов и зарубежные операции дочерних структур российских банков — в международной редакции BASE II и IPM. Универсальной модели сверки не существует ни между сетями, ни между карточной логикой и логикой СБП; попытка заменить разные процессы усреднённым учётным потоком разрушает диагностическую ценность сверки.

32 Споры и chargeback

Когда держатель карты звонит в банк и говорит: «я этого не покупал», вчерашняя завершённая транзакция превращается в спор. Каждая стадия меняет денежную позицию сторон, бремя доказывания и срок ответа.

32.1 Стадии диспута

Получив жалобу, банк запускает регламентированный цикл; каждая стадия задаёт срок, набор документов и финансовые последствия [13, 38].

Первая стадия — предварительный запрос на сведения, в отрасли — *inquiry* или *retrieval request*: эмитент или его процессор проверяет, есть ли основания открывать формальный спор. Стадия не обязательна, но часть недоразумений разрешается ещё до chargeback. Если спор не урегулирован, начинается формальный chargeback без согласия продавца, *chargeback*. Эмитент обращается к сети, сеть дебетует эквайера, а эквайер переносит риск на ТСП. К спору прикладывается код основания спора, *reason code*: он задаёт предмет доказывания и показывает, какая сторона несёт основное бремя доказывания [13].

Следующая стадия — ответ ТСП на chargeback, в отраслевой речи повторное представление, *representment*. У Visa официальная терминология устроена иначе: «диспут / ответ на диспут / предарбитраж / арбитраж»; Mastercard сохраняет язык циклов chargeback и подачи дела.

Если ответ не убедил эмитента, наступает предарбитраж, *pre-arbitration*. Эмитент либо принимает ответ, либо переводит спор на более узкую и дорогую стадию. Если предарбитраж не закрывает спор, сеть выносит дело в арбитраж, *arbitration*, где решение становится обязательным, а проигравшая сторона платит по спорной операции и по процессуальным сборам [13, 38].

Логи, чеки, сведения о доставке и согласии клиента хранят дольше самого заказа: код основания спора, под который их потребуют, эмитент выберет позже, чем продавец закроет заказ.

32.2 Процедуры Visa и Mastercard

В 2018 году Visa перевела процесс споров на *Visa Claims Resolution* (VCR). Стороны подают доказательства раньше, а количество обменов между эмитентом и эквайером сокращено [13, 39].

Когда клиент не узнаёт списание и звонит в банк, эмитент сначала показывает ему дополнительные сведения о покупке. Понятное описание товара, адрес доставки или имя получателя предотвращают часть споров до формального chargeback. На этом построен Order Insight — сервис Visa (через сеть Verifi), передающий эмитенту расширенные данные о покупке, чтобы закрыть спор до перехода в дорогую процессуальную стадию [686].

У Mastercard задача та же, но язык правил другой. Официальное руководство оперирует циклами chargeback, вторым предъявлением (*second presentment*) и подачей дела в арбитраж [38]. За прояснение покупки до формального спора у Mastercard

Таблица 46 — Стадии разрешения спора у Visa и Mastercard

Стадия процесса	Visa (VCR)	Mastercard
Раннее урегулирование	Order Insight, CDRN, RDR (Verifi)	Ethoca Consumer Clarity, Alerts
Chargeback	Visa Resolve Online (VROL)	MasterCom (IPM 1442)
Ответ эквайера	representment	second presentment (IPM 1240, FC 205/282)
Срок ответа эквайера	30 дн	45 дн
Предарбитраж	pre-arbitration (через VROL)	pre-arbitration case filing (Mastercom)
Арбитраж	Arbitration and Compliance Committee	Dispute Resolution Management

отвечает семейство сервисов Ethoca для раннего обмена данными между эмитентом и ТСП, включая Consumer Clarity, который передаёт эмитенту обогащённое описание покупки в момент звонка держателя [687, 688].

Самое заметное процессуальное расхождение — сроки. С переходом на VCR Visa сократила срок ответа эквайера на диспут с 45 до 30 календарных дней [13, 39]. Эквайер оставляет часть этого срока себе: у Adyen с 21 июля 2025 года ТСП отвечает на диспут Visa за 9 дней по внутренним операциям США и Канады и за 18 дней в остальных регионах [689]. Mastercard сохраняет 45 дней на ответ эквайера в первом цикле chargeback [38]. У ТСП из-за этого складываются разные внутренние сроки на ответ (Service Level Agreement, SLA) под каждую сеть: спор по Visa требует ответа быстрее, чем аналогичный спор по Mastercard. Точный срок сверяйте с текущей редакцией правил и договором с эквайером.

Исторически 45 дней соответствовали повседневной работе 1970-х–1980-х годов. Международная почта с подтверждением доставки шла несколько недель, банковская обработка добавляла ещё несколько дней. Более длинные сроки для поздних стадий, предарбитража и арбитража, давали сторонам время собрать доказательства через несколько часовых поясов. Сокращение сроков у Visa и эквайеров отражает цифровизацию доказательств: логи, отметки курьерской службы, данные 3-D Secure (3DS, см. гл. 11) доступны немедленно.

Для раннего урегулирования спора у Mastercard есть отдельный сервис Ethoca Alerts: эмитент уведомляет ТСП о поданной жалобе, и продавец успевает провести возврат до формального chargeback [687].

Раннее урегулирование спора применимо только там, где спор возник из-за неузнавания покупки или недостатка сведений. При неполученном товаре, некачественной услуге или нарушенном условии договора спор всё равно придётся вести по полной схеме.

К Order Insight у Visa и к Ethoca Consumer Clarity у Mastercard ТСП подключается через своего эквайера или напрямую через одобренного партнёра сети — Verifi у Visa, Ethoca у Mastercard. Оба продукта не меняют авторизационный поток: данные отдаются эмитенту по отдельному API уже после авторизации, в момент, когда держатель карты интересуется покупкой или подаёт жалобу. У Visa запрос обслуживается через Visa Resolve Online (VROL), к которому подключена сеть Verifi; у Mastercard — через Mastercom и партнёрскую сеть Ethoca. Для ТСП интеграция сводится к CRM-коннектору, который по входящему запросу возвращает расширенное описание покупки — название позиции, адрес доставки, имя получателя, идентификатор заказа на стороне ТСП. Эмитент показывает эти данные держателю карты при звонке

в колл-центр или при просмотре деталей операции в мобильном или интернет-банке. Собственный лог звонков и возвратов ТСП доходит до эмитента только через подключение к Verifi или Ethoca.

32.3 Категории кодов основания спора Visa

Visa делит коды основания спора на большие категории: фрод (10.x), ошибки авторизации (11.x), ошибки обработки (12.x) и потребительские споры (13.x) [13]. Категория сразу определяет, кто несёт бремя доказывания и какие доказательства сеть готова рассматривать.

Категория 10.x — фрод (*fraud*). Для интернет-торговли определяющим остаётся код 10.4, *Other Fraud — Card-Absent Environment*: держатель карты утверждает, что не участвовал в интернет-покупке. Под код 10.4 у Visa и работает Compelling Evidence 3.0 (CE 3.0; см. раздел 32.5).

Категория 11.x — нарушение правил авторизации: операция без обязательного запроса авторизации, продолжение несмотря на отказ, проведение по устаревшему ответу авторизации.

Категория 12.x — ошибки обработки на стороне продавца или процессинга: сумма клиринга не совпала с авторизацией, одна и та же операция попала в клиринг дважды, транзакция дошла до сети слишком поздно или с искажёнными данными.

Категория 13.x описывает потребительские споры: товар не получен, услуга не оказана, подписка не отменена, возврат обещан, но не проведён. Для этой категории решают доказательства исполнения обязательства: доставка, акцепт условий, подтверждение пользования, дата отмены и момент начисления следующего биллингового цикла.

У Mastercard собственная нумерация кодов основания спора, но деление сходное: фрод, авторизация, ошибка обработки, спор держателя карты [38].

По коду 10.4 бремя доказывания фрода в дистанционном канале несёт ТСП. Поэтому его защита опирается на 3DS, профилирование устройств и признаки поведенческого совпадения. По кодам 13.x предмет доказывания смещается к исполнению обязательства: подтверждению доставки и раскрытию условий до транзакции.

У подписочных кодов доказательная база делится по существу спора. По коду 13.2 «Cancelled Recurring Transaction» Visa с октября 2024 года принимает как защиту ТСП доказательство того, что клиент пользовался услугой уже после даты отзыва разрешения на списание и до даты обработки диспута, либо документально подтверждённый возврат или зачёт списанной суммы [13]. Сценарий «отписался заранее, а деньги списали» проходит по 13.2: держатель отозвал согласие, а списание прошло позже. Сценарий «не знал о продлении подписки» — триал или промопериод без явного уведомления — проходит по коду 13.5 «Misrepresentation»: здесь Visa с 2020 года требует от ТСП подтверждения явного согласия клиента на будущие списания и напоминания не позднее чем за 7 дней до даты списания после пробного или промопериода (см. раздел 30.4) [13, 662]. У Mastercard для подписок с биллингом раз в полгода и реже действует своё правило: за 7–30 дней до следующего списания клиенту отправляется напоминание о предстоящем платеже [46]. Лог коммуникаций ТСП с датами отправок и подтверждениями доставки нужен в обоих сценариях наравне с подтверждением исполнения услуги.

32.4 Состав доказательств

Выражение «убедительные доказательства» (*compelling evidence*) в споре означает конкретный набор фактов под конкретный код основания спора [13]. Факты, достаточные для спора о фроде, не сработают в споре о неполученном товаре.

В споре о дистанционной покупке ТСП показывает привязку транзакции и к устройству, и к поведению клиента. Сюда относятся IP-адрес, идентификатор или отпечаток устройства, учётная запись, адрес доставки, адрес электронной почты, номер телефона, а при наличии 3-D Secure результат аутентификации. Один IP-адрес сам по себе слаб; убедительной становится совокупность признаков.

Для спора о неполучении товара или услуги требуется подтверждение исполнения: отметка курьерской службы о вручении, подпись получателя, технический лог активации цифрового товара, запись о первом входе в сервис, протокол оказания услуги. Для спора об отменённой подписке требуются дата отмены, условия договора и доказательство того, что клиент видел эти условия до списания.

Логи под спор нужно собирать заранее: к моменту chargeback часть технических следов уже может быть недоступна. Собирают IP-адрес, строку `User-Agent`, сведения об устройстве, результат проверки адреса (Address Verification System, AVS) и кода проверки карты (Card Verification Value, CVV), результат 3-D Secure, подтверждение доставки и связку между первой клиентской транзакцией (Customer-Initiated Transaction, CIT; см. гл. 30) и последующими списаниями.

Что не считается доказательством: SMS клиента

Держатель часто предъявляет как «доказательство» SMS-уведомление от банка-эмитента — «с карты списано 1500 рублей в ТСП X». Когда чек продавцу не достался или терминал остановился на печати, держатель карты ссылается на это сообщение как на подтверждение транзакции. В цикле спора оно аргументом не является: правила Visa и Mastercard не регламентируют SMS-информирование и не учитывают его в разрешении спора [13, 46]; публичные правила ПС Мир SMS-информирование также не регулируют [169].

Само обязательство SMS-информирования вытекает из части 4 статьи 9 161-ФЗ [1]: эмитент обязан уведомлять клиента о каждой операции с использованием его электронного средства платежа (ЭСП; см. гл. 25), способ уведомления согласуется в договоре, и с момента уведомления начинается отсчёт срока, в течение которого клиент вправе оспорить операцию у эмитента. Положение Банка России 821-П [205] регулирует защиту канала: подтверждение контактных данных клиента и правила обработки информации о переводах. Межбанковский и клиентский циклы спора по срокам пересекаются лишь частично.

SMS отправляет внутренний сервис эмитента по триггеру изменения доступного остатка, формируя текст из полей сообщения ISO 8583 (DE — Data Element; см. гл. 6): DE 41 (Terminal ID), DE 42 (Merchant ID) и DE 43 (Card Acceptor Name/Location) авторизационного сообщения. Триггер срабатывает на одобренной авторизации, но не подтверждает, что ответ хоста дошёл до терминала, был корректно разобран POS-терминалом (Point-of-Sale) и распечатался чек. Терминал мог отправить автоматический технический *reversal* по таймауту или по ошибке разбора криптограммы ответа авторизации (Authorization Response Cryptogram, ARPC; см. гл. 7) уже после отправки SMS держателю. Держатель карты видит «списание», продавец — отказ.

Сеть сверяет спор с тем, что прошло через авторизацию и клиринг: код ответа DE 39 (Response Code) и клиринговую запись с кодом авторизации (*auth code*);

чек терминала с тем же кодом ответа подтверждает эти данные со стороны держателя. Push-уведомления мобильного банка и отображение в истории операций до клиринга сеть не рассматривает.

32.5 Compelling Evidence 3.0 и NTID

С 15 апреля 2023 года Visa расширила правила доказывания и ввела Compelling Evidence 3.0 (CE 3.0) для защиты от спора о фроде в дистанционном канале при наличии двух предшествующих неоспоренных транзакций с тем же реквизитом и совпадающими ключевыми признаками клиента. Так Visa отвечает на дружественный фрод (*friendly fraud*; см. раздел 29.1) — ситуацию, когда легитимный держатель оспаривает собственную покупку как несанкционированную [13, 690]. Связку списаний на всём интервале обеспечивает *сетевой идентификатор транзакции* (Network Transaction ID, NTID) — присваиваемый сетью ключ, привязывающий последующие операции к первой клиентской.

Для защиты по CE 3.0 требуются две предыдущие транзакции того же ТСП, у которых нет ни зарегистрированного отчёта о фроде, ни открытого спора по фроду, и которые попадают в интервал 120–365 дней до даты спора. Между спорной и историческими транзакциями совпадают минимум два ключевых признака клиента, и одним из них должен быть IP-адрес либо идентификатор устройства [690].

CE 3.0 работает через Visa Resolve Online (VROL) — единую онлайн-платформу Visa для обмена данными споров между эмитентом и эквайером. По спору с кодом основания 10.4 «Other Fraud — Card-Absent Environment» доказательства CE 3.0 подаются на стадии *pre-dispute*, когда ТСП в реальном времени отвечает через Order Insight до создания диспута в VROL, и после открытия диспута, когда эквайер прикладывает те же сведения к предарбитражу. Условие: собирать идентификатор устройства и IP-адрес при каждой покупке и хранить историю неоспоренных транзакций минимум 365 дней [690].

Visa не требует NTID как отдельный критерий CE 3.0. Но в подписочном сценарии сохранённый NTID и аккуратная связка первой клиентской транзакции CIT с последующими списаниями дают ТСП исторический след клиента [662, 690].

Против того же явления, которое Mastercard называет *first-party chargeback*, работает First-Party Trust Program. ТСП может передавать расширенные данные либо в момент авторизации, либо на стадии спора; для защиты от chargeback программа требует комбинацию признаков из групп факторов устройства (*device factor*), факторов доставки (*delivery factor*) и дополнительных идентифицирующих признаков (*additional identity factors*) [645, 687].

CE 3.0 применима только к спорам о фроде в дистанционном канале; против неполученного товара, некачественной услуги или ошибочной отмены подписки она не работает.

32.6 Мониторинговые программы сетей

Устойчиво высокий уровень chargeback грозит попаданием в мониторинговые программы сетей. Названия и пороги у программ меняются, эскалация остаётся прежней: при слишком высокой доле споров или фрода сеть переходит от предупреждений к плану исправления, штрафам и к прекращению обслуживания [13, 38].

В публичных материалах Visa свела мониторинг споров и фрода на уровне эквайера в Visa Acquirer Monitoring Program (VAMP), а Mastercard по-прежнему описывает набор отдельных программ контроля, включая Business Risk Assessment and Mitigation (BRAM), Excessive Chargeback Program (MC ECP), Excessive Fraud Merchant (EFM) и Questionable Merchant Audit Program (QMAP) [45, 691].

VAMP отслеживает оба уровня — и портфель эквайера в целом, и отдельные ТСП, с разными порогами для каждого. Программа объединила прежние Visa Dispute Monitoring Program (VDMP) и Visa Fraud Monitoring Program (VFMP) в единый мониторинг. В публичном документе Visa, действовавшем с 1 июня 2025 года, для портфеля эквайера заданы уровни Above Standard (от 50 базисных пунктов) и Excessive (от 70), а для ТСП — только уровень Excessive. В регионах AP, Канада, ЕС и США его порог составил 220 базисных пунктов при не менее 1 500 событий фрода и диспутов в месяц, в LAC — 150 базисных пунктов, в CEMEA — 220 базисных пунктов при не менее 150 событий на сумму от 75 000 долларов США. Переходный период закончился 30 сентября 2025 года; для AP, Канады, ЕС и США Visa объявила снижение порога до 150 базисных пунктов с 1 апреля 2026 года [692]. Точный порог сверяйте с датой редакции программы.

У Mastercard программа мониторинга chargeback ТСП оформлена в MC ECP. Публичные Security Rules and Procedures выносят BRAM и MC ECP в разные программы, а для ТСП с превышением порогов по chargeback используют категории Excessive Chargeback Merchant (ECM) и High Excessive Chargeback Merchant (HECM) [47, 691]. За конкретными числовыми порогами Mastercard отсылает участников к руководству Data Integrity Monitoring Program. В публичных материалах MC ECP описывается как отдельная программа с эскалацией у эквайера, без привязки к фиксированному порогу BRAM. Эквайеры публикуют эти пороги в памятках для ТСП: для ECM количество chargeback ≥ 100 в месяц при доле chargeback (*chargeback ratio*) $\geq 1{,}5\,\%$; для HECM — ≥ 300 при доле $\geq 3{,}0\,\%$. Доля chargeback рассчитывается как количество chargeback за текущий месяц, делённое на количество транзакций продажи за предшествующий месяц [693].

В плане исправления сеть требует конкретных мер: улучшение дескриптора продавца (*merchant descriptor* — текстовая строка с названием и местоположением ТСП, которая попадает в выписку держателя карты), подключение к Order Insight или Ethoca, ужесточение проверки 3DS, пересмотр политики возвратов, ограничение проблемных категорий товаров. Без снижения показателей за 90–120 дней эскалация продолжается.

Пороги «CB ratio $> 0{,}9\,\%$» и штрафы \$25–100 за chargeback относятся к эпохе VDMP, а не к действующей редакции VAMP. Знаменатели у методик расчёта разные: VAMP считает в базисных пунктах по формуле $(\mathrm{TC}40 + \mathrm{TC}15)/\mathrm{TC}05_{\mathrm{CNP}}$, где TC — Transaction Code в клиринге Visa BASE II (TC 40 — отчёт о фроде, TC 15 — chargeback, TC 05 — продажа; см. раздел 31.2).

Сеть оценивает сочетание абсолютного объёма и относительной доли. Сезонность, скользящий период и сдвиг спора в соседний календарный месяц легко искажают показатель; ТСП надёжнее считать свои показатели отдельно по спорам, фроду и возвратам, чем смотреть на единый агрегированный показатель.

32.7 Диспуты в системе «Мир»

Карты «Мир» обрабатываются ОПКЦ НСПК (раздел 16.2). Правила платёжной системы «Мир» отсылают разрешение диспутов к Стандарту Системы «Руководство

по разрешению диспутов», доступному участникам; обмен ведётся на платформе «Диспут Плюс», Visa Resolve Online и Mastercom (единая платформа управления спорами Mastercard для обмена сообщениями и доказательствами между эмитентом и эквайером) здесь не применяются [169]. По устройству регламент НСПК повторяет общую модель карточного диспута: chargeback, повторное представление *representment*, претензия *pre-arbitration*, арбитраж. Различия проявляются в кодах оснований, сроках и тарифах. Тарифы ПС фиксируют в рублях плату за доступ к «Диспут Плюс», плату за обработку диспута со стороны, признавшей ответственность, и плату за окончательное разрешение диспута Системой со стороны, признанной ответственной [300].

Для продавца доказательная база и сроки ответа на chargeback по карте «Мир» из привычного руководства по спорам Visa/Mastercard заимствовать напрямую нельзя; состав обязательных доказательств и сроки ответа сверяйте с правилами «Мир» через эквайера и его процессор. Для эквайера мониторинговые программы НСПК (аналоги VAMP/MC ECP) действуют отдельно. Пороги доли chargeback и доли фрода, после которых ТСП попадает под повышенный контроль или санкции, устанавливает НСПК.

32.8 Диспуты в СБП

Держатель карты, недовольный покупкой, нажимает кнопку спора в банковском приложении, и карточный chargeback начинает свой цикл. Плательщик через СБП в типовом потоке такой кнопки не видит: у системы нет встроенного механизма принудительного оспаривания уже исполненной операции.

В СБП деньги зачисляются получателю мгновенно. При ошибочном переводе банк плательщика может запустить «Просьбу СБП», но автоматически вернуть деньги нельзя — банк обращается к получателю, потому что для возврата требуется его согласие, если только иной порядок не вытекает из закона, решения суда или договора с банком [444]. Для оплаты бизнеса доступен обычный возврат через банк продавца, в том числе частичный, и деньги при таком возврате поступают покупателю моментально [348].

Продавец не несёт классических штрафов по спорам и не проходит последовательность стадий от ответа на chargeback до предарбитража. Если товар не доставлен, покупатель защищает свои интересы через переговоры, претензионную работу, обычный гражданско-правовой спор или возврат, который должен оформить продавец.

В продукте, который принимает и карты, и СБП, эти два потока работают по разным правилам: карточный — с циклом chargeback и SLA сети, СБП — через гражданско-правовой возврат и «Просьбу».

33 Управление отказами

Покупатель на странице оплаты видит одно сообщение: платёж не прошёл. За ним стоят разные коды ответа: один допускает повтор после паузы, другой указывает на проблему маршрута при исправном счёте клиента, третий запрещает повтор с теми же реквизитами. Различить эти случаи нужно до того, как система начнёт повторять заведомо безнадёжные попытки.

33.1 Структура отказа

Деление кодов на «мягкие» и «жёсткие» — эвристика продавца. Visa группирует коды отказов (*decline response codes*) на категории «Issuer will never approve», «Issuer cannot approve at this time», «Data quality» и «Generic»; Mastercard отдельно запрещает дополнительные авторизационные запросы по CNP для части кодов отказов [13, 46]. Продавцу важно одно: какое действие разумно после конкретного кода.

Мягкий отказ (*soft decline*) означает, что транзакция отклонена по вре́менной или устранимой причине: временный лимит, поведенческий фильтр, недоступность сервиса. В рабочей классификации сюда попадают `51` Insufficient Funds, `61` Exceeds Withdrawal Amount Limit, `65` Exceeds Withdrawal Frequency Limit и часть общих (*generic*) кодов вроде `05`, если сеть вообще допускает повтор и ТСП остаётся в пределах лимитов повторов [13].

Жёсткий отказ (*hard decline*) означает, что ту же операцию с теми же данными повторять бессмысленно или прямо запрещено правилами. Базовые примеры — `04` Pick Up, `14` Invalid Account Number[2], `41` Lost Card и `43` Stolen Card. Они указывают либо на неверные реквизиты, либо на карту, с которой продолжать операцию нельзя, и поэтому требуют другого платёжного реквизита или ручной проверки [13, 46].

`54` Expired Card для Visa относится к категории Data quality, поскольку сеть прямо трактует его как случай, когда нужно перепроверить платёжную информацию. У Mastercard правило сформулировано иначе: для CNP ТСП не должен инициировать дополнительные авторизационные запросы по той же операции с тем же PAN и сроком действия — повтор возможен только с новыми реквизитами [13, 46].

Технические и маршрутные коды образуют отдельную категорию. `91` Issuer Unavailable и `96` System Malfunction указывают на доступность эмитента или маршрута, не на состояние счёта. Для них сеть допускает повторные попытки в пределах лимитов; сначала нужно проверить доступность маршрута и эмитента, а состояние карты разбирают после исключения технического отказа. `01` Refer to Card Issuer слепо повторять нельзя: код указывает на иной канал или дополнительное действие со стороны держателя либо эмитента [13].

Visa Core Rules делят коды на Category 1–4 ради лимитов повторов и санкций за их нарушение; Mastercard Transaction Processing Rules часть запретов привязывает к контексту операции — повторы по CNP после `54` запрещены отдельной нормой (в классификации Visa этот код относится к Data quality, у Mastercard тот же `54` попадает в Lifecycle Declines и сопровождается MAC 01 с указанием на Account Updater) [13, 46]. Продавцу поверх этих групп нужна собственная классификация: какой следующий шаг возможен после конкретного отказа. Тот же код в разных

[2] В актуальной редакции Visa Core Rules код `14` отнесён к категории 1 (Issuer will never approve); для продавца это жёсткий отказ — повтор с теми же реквизитами бессмысленен, нужен новый PAN.

потоках читается по-разному: 51 в подписке — повтор через 24–48 часов, в разовой покупке — немедленное предложение другого инструмента. Для продавца это сводится к первому рабочему вопросу (табл. 47): прекратить операцию, обновить данные или проверить доступность маршрута.

Таблица 47 — Рабочая классификация кодов ответа по следующему действию.

Не повторять ту же операцию	Нужны новые данные / пауза	Технический / другой путь
04 Pick Up прекратить; запросить другой реквизит **14 Invalid Account** проверить PAN **41 Lost Card** карта утеряна; прекратить **43 Stolen Card** карта украдена; прекратить	**54 Expired Card** обновить срок действия или PAN; в Mastercard CNP не повторять тот же PAN+expiry **51 Insufficient Funds** пауза; без цикла повторов **61 Exceeds Limit** проверить сумму и лимит **62 Restricted Card** смотреть контекст и правила сети **65 Freq. Limit** дождаться сброса лимита **05 Do Not Honor** общий отказ; только в пределах лимитов сети	**91 Issuer Unavailable** проблема доступности маршрута или эмитента **96 System Malfunction** технический сбой; сначала зафиксировать финальный статус **01 Refer** нужен иной канал или действие банка **таймаут** подтвердить финальный статус, затем контролируемый повтор

33.2 Значение кодов ответа

Код ответа эмитента сжимает причину отказа: за одним кодом стоят десятки причин, и истинную из них восстанавливают только по дополнительным данным.

05 Do Not Honor формально означает «не проводите операцию» без указания причины. За ним могут стоять антифрод, дневной лимит, несоответствие поведенческому профилю клиента, временная блокировка в приложении или внутренняя политика эмитента по конкретному MCC. Часть причин временная и исчезает сама, часть постоянная, поэтому 05 трактуют с осторожностью. У Visa общие коды отказов (*generic decline response codes*) сведены в отдельную Category 4 и должны использоваться только там, где не подходит более точное значение [13]. Эмитент скрывает причину намеренно: детальный код полезен атакующему. Если 51 точно означает нехватку средств, злоумышленник с набором украденных карт отбросит карты без доступного остатка и сосредоточится на картах с доступным лимитом. Возвращая 05, эмитент лишает атаку перебором краденых учётных данных (*credential stuffing*) сведений о состоянии счёта.

51 Insufficient Funds тоже не сводится к буквальному прочтению. Для дебетовых карт он часто означает нехватку средств на счёте, для кредитных — превышение лимита, а у некоторых эмитентов — универсальную форму мягкого отказа, за которой эмитент прячет точную причину.

54 Expired Card в таблице категорий кодов отказа Visa Core Rules относится к классу Data quality, а в Visa Token Service (VTS) PAN Lifecycle прямо предусмотрены обновление PAN, срока действия и обновления Visa Account Updater (VAU). В потоках с повторными списаниями и сохранёнными реквизитами карт после 54 проверяют не возможность повтора, а факт получения обновлённых реквизитов. У Mastercard

ту же задачу решает Automatic Billing Updater (ABU), который сеть публично описывает как способ поддерживать актуальность платёжных реквизитов и избегать отказов [13, 287].[1]

В Visa технические 91 и 96 попадают в классы, где повторы разрешены в пределах лимитов, заданных сетью. Если такие коды доминируют в статистике, проблема в сети, маршрутизации или доступности хоста [13].

Мягкие отказы, связанные с аутентификацией, образуют отдельную категорию. Код 65 в исходной семантике ISO 8583/Visa означает Exceeds Withdrawal Frequency Limit, когда нужно дождаться сброса лимита частоты; в Европе, где действует Strong Customer Authentication (SCA, усиленная аутентификация плательщика), Mastercard использует тот же 65 как мягкий отказ, по которому эмитент готов одобрить операцию после повторной аутентификации по протоколу 3-D Secure (3DS); см. гл. 11. Шлюз получает 65, распознаёт его как допускающий повтор с 3DS-аутентификацией (*retryable-with-3DS* — внутренний класс шлюза, а не тег сети), инициирует аутентификацию: сообщение Authentication Request (AReq) уходит от 3DS-сервера ТСП на Directory Server (DS) платёжной сети и далее на Access Control Server (ACS) эмитента. По результатам аутентификации шлюз получает Electronic Commerce Indicator (ECI, индикатор уровня аутентификации) и Cardholder Authentication Verification Value (CAVV, криптограмма подтверждения держателя) и повторяет авторизационный запрос с данными аутентификации. Эмитент видит тот же PAN, ту же сумму, но с подтверждением SCA, и одобряет. Слепой повтор того же запроса даст лишь цикл отказов; повтор с 3DS возвращает шанс на одобрение [46].

ПРАКТИКА

Мониторинг отказов делит коды ответа минимум на три-четыре группы: жёсткие, мягкие финансовые, мягкие поведенческие и технические. Сводная панель с одним числом доли отказов скрывает структуру. 15 % отказов, половина из которых приходится на технические коды, ставят другую задачу, чем те же 15 % при преобладании необратимых отказов.

Офлайновые коды POS-терминала: Z1, Z3, Y1, Y3

Не все коды ответа приходят от эмитента. Если терминал по правилам EMV или по настройкам конфигурации принимает решение о судьбе транзакции — одобрить или отклонить, не отправляя её в сеть, — он генерирует код собственного формата. Эти коды не входят в ISO 8583 и видны в чеке POS и в локальном журнале; об офлайн-отказе эмитент не узнаёт, а офлайн-одобрение увидит только в клиринге [32].

Терминал принимает решение, сопоставляя Terminal Verification Results (TVR) с Terminal Action Code (TAC) терминала и Issuer Action Code (IAC). IAC — это записанные на карте битовые маски реакций EMV-приложения на результаты Terminal Risk Management. IAC-Denial указывает, по каким сигналам приложение карты требует отклонить операцию офлайн, IAC-Online — по каким сигналам нужно перейти на авторизацию к эмитенту, а IAC-Default — какое решение принять, если онлайновая авторизация недоступна [31]:

- Z1 — отклонено офлайн (*offline declined*): терминал отклонил операцию самостоятельно, не пытаясь связаться с эмитентом. Типичные причины — срабатывание условий IAC-Denial, провал офлайн-аутентификации данных, превышение прикладного лимита.

[1] Детали сервисов обновления реквизитов: [36, 673, 694].

- Z3 — онлайн не состоялся, отклонено (*no online, declined*): терминал должен был перейти онлайн (требование IAC-Online), но связи не было, и по правилам IAC-Default операцию пришлось отклонить.
- Y1 — одобрено офлайн (*offline approved*): терминал одобрил операцию локально, не отправляя её на авторизацию. Возможно только если конфигурация терминала разрешает офлайн-одобрение и сумма не превысила *floor limit*.
- Y3 — онлайн не состоялся, одобрено (*no online, approved*): попытка перейти онлайн провалилась, но IAC-Default позволил одобрить операцию офлайн.

В российской рознице Z1 и Y1 встречаются редко: *floor limit* у большинства терминалов равен нулю, и любая операция отправляется эмитенту. Z3 и Y3, напротив, появляются при разборе инцидентов с падением канала связи и помогают локализовать проблему между терминалом, эквайером и сетью.

Оба кода сообщают, что онлайновая авторизация не прошла; разница — в последующем решении, а его причину устанавливают по логам TVR, IAC и терминала. В Z3 бит TVR совпал с установленным битом IAC-Default или TAC-Default, и локальное одобрение запрещено; в Y3 совпадений нет, и терминал одобрил операцию офлайн. При массовом Z3 разбор начинают с канала между терминалом и эквайером, затем проверяют IAC-конфигурацию EMV-приложения: если карта требует онлайн, настройки терминала локально операцию не одобрят. Массовый Y3, наоборот, означает, что терминал регулярно переходит в офлайн-резерв, и эквайер позже получит пакетную выгрузку (*batch upload*) с операциями, прошедшими без полной онлайновой авторизации. Этот поток сверяют с лимитами сети по офлайновым суммам и фиксируют в отчётности отдельно: офлайн-одобрение жёстко привязано к EMV-криптограмме, эмитент увидит такие операции лишь на стадии клиринга и уже не повлияет на исход авторизации — оспорить операцию он сможет только через диспут после расчёта, и при соблюдённом EMV-профиле его позиция в диспуте слабее.

33.3 Повторы после отказа: время, частота, каналы

На повторах расходятся интересы продавца и платёжной сети: продавцу нужна конверсия, сети — бережное расходование пропускной способности авторизации. При миллионах подписочных ТСП даже два лишних запроса в месяц на клиента создают значимую нагрузку, и сеть ставит лимиты повторов там, где их польза близка к нулю.

Правила сетей задают внешние условия повторов: какие коды вообще можно повторять, а какие нельзя. Visa Core Rules сводят коды отказов в таблицу категорий с разными лимитами повторов для ТСП; Mastercard для CNP отдельно запрещает дополнительные авторизационные запросы по той же транзакции после ряда кодов отказа, включая 04, 14, 41, 43 и 54 [13, 46].

Сети задают лимиты, а не конкретный интервал вида «повтори через 17 минут»; они требуют не строить слепой цикл повторов и не выходить за лимиты. Если отказ связан с нехваткой средств или лимитом, серия одинаковых запросов не создаёт деньги и не расширяет лимит. Если код технический, бессмысленная очередь повторов увеличивает шум в логах и повышает риск попадания под мониторинг сети.

Перед каждым повтором продавец отвечает на вопросы: допускает ли сеть повтор этого кода или повтор требует новых данных (срок действия, токен, 3DS), а если повтор допустим — какой интервал и какой потолок безопасны для конкретного

продавца, PSP и категории ТСП. Mastercard на публичных продуктовых страницах описывает ту же логику как *intelligent retry strategies* [694].

Отдельный фактор — состояние холда эмитента (*auth-hold*) после первой авторизации (см. раздел 5.1). Если первая попытка вернула мягкий отказ уже после того, как эмитент успел поставить холд (например, тайм-аут на стороне эквайера), повтор по тому же реквизиту может прийти эмитенту как дубль и быть отклонён, а суммарная блокировка средств у держателя — удвоиться до истечения периода действия холда по MCC. Корректная логика повторов проверяет состояние первой попытки и при необходимости снимает блокировку сообщением *reversal* перед отправкой второго авторизационного запроса.

Для решения о повторе коды ответа делят на классы:

- **жёсткий отказ** (`04`, `14`, `41`, `43`) — карта недействительна, изъята или украдена. Повтор запрещён, нужен новый платёжный инструмент.
- **мягкий финансовый** (`51`) — нехватка средств. Повтор допустим, но не ранее чем через 24–48 часов, когда баланс может измениться; цикл с интервалом в минуты бесполезен.
- **мягкий аутентификационный** (`65`, `1A`) — требуется SCA. Повтор идёт через 3DS; повтор того же запроса бесполезен.
- **технический** (`91`, `96`) — эмитент или маршрут недоступен. Повтор допустим через 15–60 минут; каскад через другого эквайера эффективен только если альтернативный маршрут ведёт к другому хосту эмитента.
- **непрозрачный** (`05`) — причина неизвестна. Один отложенный повтор допустим; серия идентичных запросов повышает риск попадания под мониторинг сети.

Visa и Mastercard описывают токенизацию и оптимизацию одобрений как способы дать эмитенту более качественные данные и убрать лишние шаги авторизации, поэтому повтор через сетевой токен или через более удачный маршрут не равен простому повтору запроса по PAN [36, 695].[1]

Логика повторов отсекает бессмысленные попытки, но долю отказов снижают другие инструменты: обновление реквизитов, выбор маршрута, аутентификация.

Платёжные сети влияют на логику повторов через мониторинговые программы и тарифы за повторы; эти механизмы санкций независимы друг от друга.

Мониторинговые программы по фроду и диспутам — VAMP у Visa, MC ECP (Excessive Chargeback Program) и EFM (Excessive Fraud Merchant) у Mastercard (см. раздел 32.6) — считают доли фрода и chargeback в портфеле. VAMP агрегирует TC40-сообщения и TC15-диспуты по CNP, ECP — долю chargeback, EFM — долю подтверждённого фрода. Серии повторов сами по себе в доли фрода и диспутов не попадают; в них попадают последствия неуместных повторов, когда держатель оспаривает уже состоявшееся списание. Попытки авторизации VAMP считает отдельной метрикой перебора (*enumeration*): доля авторизаций с признаком перебора, одобренных и отклонённых, среди всех авторизаций ТСП; порог доли — 2000 базисных пунктов, порог числа таких авторизаций — 300 000 за месяц [691, 692].

Тарифы за повторы — отдельная санкция. У Visa это System Integrity Fees: Never Approve Reattempt Fee — по 0,10 $ за любую попытку после Category 1 (`04`, `14`, `41`, `43` и др.; для межрегиональных операций с 25.04.2026 — 0,25 $), Excessive Decline Reattempt Fee — по той же ставке за попытки сверх допустимых 20 по кодам Category 2–4 за 30 суток [13, 698]. У Mastercard аналогичные тарифы входят в программу Transaction Processing Excellence: сбор за каждый повтор после MAC 03 (Do not try again) или MAC 21 (Payment cancelled) в CNP на тот же PAN и ту же

[1] Доказательная база сетей по токенизации и оптимизации: [696, 697].

сумму в течение 30 суток, а также сбор Excessive Authorization Attempts после 10 отклонённых попыток за 24 часа или 35 попыток за 30 суток на один PAN; ставка этого сбора повышалась ежегодно и с января 2025 года составляет 0,50 $ за отклонённую авторизацию [669, 671].

Эти механизмы разнесены по разным управлениям сети и срабатывают независимо. Доля одобрений после серий 04/14/ 41/43 формально регулируется именно тарифами повторов, а не VAMP или EFM. Полные числовые пороги сети публикуют не всегда, но общая логика одинакова: тариф за повтор делает серию бессмысленных попыток дорогой, а мониторинговые программы наказывают за то, что часть этих попыток в итоге превратилась в фрод или диспуты. Поэтому политику повторов настраивают с запасом ниже формально разрешённого: решение «повторять или нет» переносят на уровень PSP. PSP видит статистику отказов по многим ТСП и эмитентам и принимает решение по портфелю, а ТСП применяет выданную PSP политику к конкретному запросу.

33.4 Сетевой токен и PAN: сигналы сети для решения эмитента

Сетевой токен меняет данные, которые видит эмитент: вместо PAN в открытом виде приходит идентификатор с привязанными ограничениями. Visa Token Service описывает токен как отдельный цифровой идентификатор, с которым эмитент задаёт параметры токена (*token variables*), определяет авторизованных запросчиков токена (*token requestors*) и запрашивает атрибуты токена (*token details*), включая данные об устройстве и риске. Токен может быть ограничен конкретным мобильным устройством, ТСП категории *e-commerce* или количеством покупок [36, 174].

В публичных материалах Visa называет рост доли одобрений (*approval rate*) для токенизированных транзакций на 2,5 %; Mastercard на страницах для эквайеров и PSP пишет о 3–6 п. п. роста доли одобрений у токенизированных цифровых платежей [695, 696]. Цифры принадлежат самим сетям и каждому продавцу не гарантируются, но общий вывод устойчив: токен даёт эмитенту более ясную картину, чем обычный PAN.

Жизненный цикл реквизитов делает эффект токенизации заметным: Visa PAN Lifecycle обновляет PAN, срок действия и выполняет обновления VAU, Mastercard ABU решает ту же задачу для сохранённых реквизитов. В потоках с сохранёнными реквизитами карт 54 Expired Card чаще означает устаревший реквизит у продавца, а не у эмитента [36].[1]

Миграцию на токены откладывают, пока текущий поток работает; к ней возвращаются, когда доля отказов и оттока становится заметной. Многие продавцы не управляют токенами напрямую и зависят от темпа своего PSP.

Подробнее об архитектуре сетевых токенов см. раздел 9.3.

33.5 Маршрутизация через эквайера

Платежи доходят до эмитента по нескольким маршрутам, и выбор пути меняет исход авторизации. В правилах Mastercard есть отдельные разделы об *authorization routing* и *domestic transaction routing*, а в публичных материалах для сообщества приёма (*acceptance community*) маршрутизация и оптимизация платежей (*routing*,

[1] Сервисы обновления реквизитов: [673, 694].

payment optimization) вынесены в самостоятельное продуктовое направление [46].[1] Выбор одного PSP определяет лишь точку входа, не весь путь до эмитента.

У разных эквайеров различаются локальное покрытие, подключения, качество формирования сообщения и сервисы оптимизации. Сетевая оптимизация одобрений использует эти различия: подбирает удачный маршрут авторизации или дополняет сообщение недостающими данными [697].

Страна BIN и страна ТСП определяют, транзакция внутренняя (*domestic*) или международная (*cross-border*); внутренний маршрут через локального эквайера даёт эмитенту знакомый контекст и повышает шанс одобрения. MCC влияет на доступные программы *interchange* и на набор правил антифрода эмитента. Валюта транзакции и валюта расчёта важны, если платформа поддерживает DCC. Историческая доля одобрений на конкретном сочетании эквайер–BIN–MCC служит исходными данными для выбора маршрута в реальном времени.

Принцип выбора маршрута — функция ожидаемого дохода $P(\text{approve} \mid \text{route}) \times \text{amount} - \text{cost}(\text{route})$, где маршрут с более высокой комиссией оправдан только при достаточно высоком $P(\text{approve})$. В зрелых системах такую функцию реализует ML-модель, переобучаемая на исторических авторизациях, а в простых конфигурациях — скоринговая (*score*) таблица по BIN $\times$ MCC $\times$ страна.

Два шаблона маршрутизации — *cascade routing* (каскадный перебор эквайеров) и *intelligent routing* (выбор маршрута по предсказанной вероятности одобрения), корректная обработка задержавшегося ответа первого эквайера и ограничения каскада по типам отказов разобраны в разделе 34.3. Если все эквайеры в каскаде вернули отказ, транзакция завершается с последним полученным кодом, повторно прогонять её через тех же эквайеров запрещено правилами повторов сетей, а правильное действие — показать ошибку или предложить другой платёжный метод.

Правила сетей, локальной маршрутизации и interchange запрещают маскировать географию ТСП или искусственно подбирать маршрут под выгодную тарифную модель. Маршрутизацию используют для повышения доли одобрений и сокращения операционных потерь [13, 46].[2]

33.6 Доля одобрений по категориям ТСП

Одно и то же значение доли одобрений — например, 85 % — интерпретируется по-разному в зависимости от категории ТСП, географии, типа карты и модели оплаты.

Сетевые правила и мониторинги считают долю одобрений раздельно: Mastercard отслеживает её для CNP- и международных операций через Merchant Advice Code (MAC), Authorization Optimizer и связанные мониторинговые программы. Сравнивать все потоки одной агрегированной метрикой нельзя [46].

Опубликованные диапазоны доли одобрений быстро устаревают: они зависят от категории ТСП, страны, доли 3DS, качества токенизации, текущих волн фрода и даже календарного периода. Универсальные ориентиры «нормальной» доли одобрений по категориям ТСП бесполезны: опубликованные числа не учитывают разрезов конкретного продавца. Конкретные проценты для своего потока сверяют по данным PSP или эквайера. Просадки относительно собственной исторической нормы по категории ТСП указывают на конкретные сбои: неправильный повтор,

[1] Материалы сети по маршрутизации и оптимизации: [695, 697].

[2] Правила Mastercard в части маршрутизации и маршрутизации по фроду (*fraud routing*): [15].

отсутствие 3DS в ответ на мягкий отказ, невыверенный маршрут по BIN или устаревшие реквизиты в *card-on-file*.

Сравнивать розницу с сервисами путешествий, подписки с разовыми интернет-платежами, а внутренний поток с международным в одной колонке бессмысленно. В подписочных операциях (*recurring*) добавляется контекст сохранённого реквизита. Связь повторного списания с исходным согласием эмитент считывает, только когда она оформлена по правилам SCF; иначе он видит обычный запрос CNP [46, 662].

Классификация кодов, повторы, сетевые токены, маршрутизация и раздельное измерение доли одобрений действуют через разные механизмы, и их эффекты не складываются механически: токенизация и маршрутизация перекрываются по целевым сегментам, аутентификация работает только на подмножестве кодов, а раздельное измерение показывает, какие сегменты снижают долю одобрений — прирост даёт работа с этими сегментами. Дальнейшие главы Части V разбирают этот набор по компонентам: шлюз — маршрутизация и идемпотентность, процессинговый центр — токены, расчётный сервис — холды и возвраты после отказа.

ПРАКТИКА

Долю одобрений измеряйте раздельно по сегментам: новые и вернувшиеся клиенты, карты с 3DS и без неё, PAN и токен, внутренний рынок и международные операции.

Часть V

Архитектура

Платёжная система выглядит монолитом только со стороны бизнес-API. Изнутри она разделена на компоненты, у каждого из которых собственный жизненный цикл, собственное состояние и собственная команда эксплуатации. Главы не предлагают рецепта «как собрать платёжную платформу с нуля»: их задача — показать, какой компонент за что отвечает, какие интерфейсы между ними сложились в индустрии и почему ответственность распределена именно так.

Платёжный шлюз превращает HTTPS-запрос продавца в авторизационное сообщение ISO 8583. Запрос проходит через приём API, оценку риска, маршрутизацию между эквайерами, изолированное хранилище карточных данных и модуль авторизации; каждый следующий компонент получает более узкое представление транзакции, чем предыдущий, и из этого порядка следуют требования к PCI scope и ограничения на обработку отказов.

Внутренний реестр обязательств отвечает за состояние денег внутри продукта: что уже заработано, что зарезервировано, что можно выплатить продавцу. Реестр опирается на двойную запись и событийную модель (авторизация, подтверждение, возврат, спор); в маркетплейсе один внешний платёж порождает несколько проводок с разными сроками признания и разными правилами отмены, и выразить это статусом одной транзакции нельзя.

Мультивалютность — вопрос о том, кто фиксирует курс: эмитент, эквайер с DCC, платформа или внешний FX-провайдер. От ответа зависит, кто несёт валютный риск и как устроена сверка между валютами. Для российских платежей с 2022 года к этому добавились ограничения доступа к SWIFT, перестройка корреспондентских схем через банки дружественных стран и рост доли юаня.

Процессинговый центр связывает шлюз с карточной сетью: коммутатор авторизации с таблицей BIN, пул HSM, клиринговый и расчётный модули. Архитектурное решение проверяется тем, что произойдёт с задержкой и доступностью при отказе внешнего канала и включении *stand-in*, и тем, кто контролирует ключевой материал.

У одной компании платёжный шлюз и внутренний реестр находятся в одном сервисе, у другой — в нескольких системах разных команд. Распределение функций между шлюзом, реестром и процессингом зависит от объёма платежей, профиля рисков и организационного устройства, но сам список задач остаётся прежним: их кто-то всё равно решает.

После части V книгу замыкает эпилог о том, как поддерживать знания актуальными в индустрии, где документы и правила быстро устаревают.

34 Платёжный шлюз

Один запрос продавца — `POST` к `/v1/payment_intents` на оплату заказа. Снаружи это обычный JSON (JavaScript Object Notation) поверх HTTPS. Внутри запрос проходит через последовательность решений, и ошибка на любом шаге меняет риск, конверсию или PCI scope — область оценки соответствия PCI DSS (Payment Card Industry Data Security Standard) [70].

34.1 Устройство шлюза

Платёжный шлюз (*payment gateway*) превращает один запрос продавца в корректную, наблюдаемую авторизацию. Роли шлюза, процессора и оркестратора среди участников расчётов разобраны в разделе 2.2.

Шлюз состоит из модуля приёма запросов к программному интерфейсу (API, application programming interface), модуля оценки риска, модуля маршрутизации, изолированного хранилища карточных данных и токенов (vault) и модуля авторизации, отправляющего запрос банку-эквайеру или напрямую карточной сети. Порядок их вызова определяет и архитектурные свойства системы, и её PCI scope.

Продавец отправляет HTTPS-запрос на API шлюза, например, `POST` к `/v1/payment_intents` либо `/v1/charges` в более старой версии API, с JSON-телом, содержащим сумму, валюту, данные карты или токен и метаданные заказа. Модуль приёма валидирует сообщение, проверяет аутентификацию по API-ключу или токену протокола делегированной авторизации OAuth 2.0 [699], применяет идемпотентность (см. раздел 34.5) и затем передаёт нормализованное внутреннее представление транзакции модулю оценки риска.

Модуль оценки риска применяет к транзакции правила и модели: проверки частоты повторов (*velocity checks*), сопоставление геолокации, отпечаток устройства (*device fingerprint*, см. гл. 29), а в системах с достаточной историей — модель оценки вероятности фрода. Решений три: передать транзакцию на следующий этап, отправить её на дополнительную проверку по протоколу подтверждения держателя карты 3-D Secure или отклонить. Проверка риска выполняется *до* авторизации: подозрительную транзакцию дешевле остановить заранее, чем разбирать последующий *chargeback*.

Если транзакция прошла оценку риска, она передаётся в модуль маршрутизации, который определяет, через какого эквайера или процессор отправить авторизационный запрос (см. раздел 34.3).

Если продавец передал полный номер карты (PAN, Primary Account Number), шлюз заменяет его токеном из хранилища. PAN сохраняется в зашифрованном хранилище (vault), а затем внутренний конвейер и ответ продавцу работают только с токеном. Это сужает CDE (cardholder data environment) до одного компонента и сокращает PCI scope всей системы — механизм подробно разобран в разделе 12.3. Если продавец сразу прислал сетевой токен (DPAN, device PAN — токенизированный аналог реального PAN), хранилище может не участвовать, но шлюз всё равно проверяет ограничения домена токена и при необходимости запрашивает у провайдера сетевой токенизации (TSP, Token Service Provider) актуальную одноразовую криптограмму транзакции для конкретной операции [174] (см. также раздел 9.3).

Модуль авторизации формирует сообщение по международному стандарту карточных операций ISO 8583 (см. гл. 6) или его эквивалент в протоколах API эквайеров, отправляет запрос по защищённому каналу банку-эквайеру, получает ответ от эмитента через карточную сеть, преобразует код ответа в формат API шлюза и возвращает результат продавцу.

Открытый пример такой сборки в одной кодовой базе — Hyperswitch от Juspay [700] (Rust, Apache 2.0): унифицированные коннекторы к 120+ процессорам, модуль маршрутизации с правилами повтора, vault для токенов и карточных данных, соответствующий PCI DSS. Та же кодовая база работает у самого Juspay в промышленной эксплуатации.

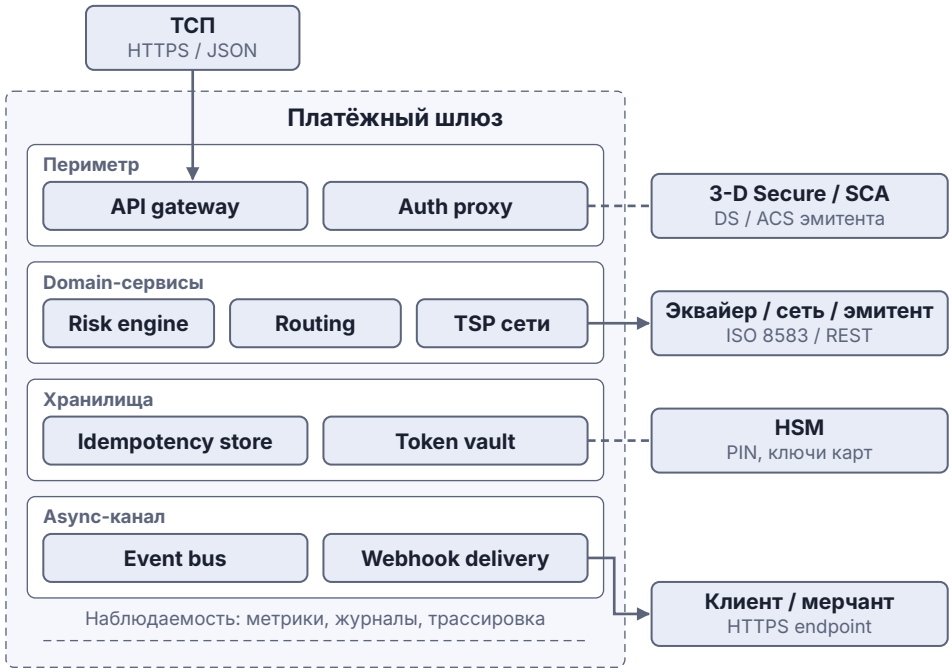


Рис. 64 — Компоненты платёжного шлюза.

34.2 Оркестрация поверх шлюза

Шлюз, процессор и оркестратор — разные архитектурные уровни. Разница влияет на продукт, когда ТСП подключает второго эквайера.

Шлюз — протокольная интеграция с одним эквайером или карточной сетью. Преобразует JSON-запрос в ISO 8583 (или REST-эквивалент в интерфейсе процессора), поддерживает соединение, токенизирует PAN и валидирует ответ.

Процессор обеспечивает сетевой обмен между шлюзом и эмитентом через карточную сеть: маршрутизирует сообщение в нужную сеть (Visa, Mastercard, Мир), при необходимости подменяет недоступного эмитента собственным ответом по правилам *stand-in processing* [75, 283]. У одного провайдера процессор и шлюз нередко совмещены в один узел.

Оркестратор — уровень над несколькими PSP и шлюзами. Продукт обращается к единому API, оркестратор распределяет вызовы по десяткам шлюзов: маршрутизирует транзакцию между провайдерами по правилам стоимости, доли одобрений и регионального профиля; реализует каскадный повтор при отказе одного из маршрутов; использует единый vault, унифицирует форму оплаты (*checkout*) поверх разных интеграций. Маршрутизация и оценка риска, описанные внутри одного шлюза, на уровне оркестратора повторяются между шлюзами.

Оркестратор окупается в нескольких сценариях:

- ТСП работает с двумя и более PSP одновременно — для устойчивости, арбитража стоимости или разнесения трафика по сетям;
- региональная экспансия, при которой каждому рынку нужен локальный эквайер с собственным договором и процессингом;
- маркетплейс, где продавцы хотят выбирать собственного PSP или подключать унаследованный договор эквайринга;
- снижение зависимости от одного вендора: переключение PSP нужно подготовить так, чтобы оно занимало считаные дни.

Primer [701] предлагает конфигурацию маршрутизации без программирования (*no-code*) поверх большого набора подключений; типичные сегменты — туризм, розница, игры, маркетплейсы. Spreedly [702] — коммерческая независимая от PSP (*PSP-agnostic*) платформа с 150+ интеграциями и универсальным vault уровня PCI Level 1. Gr4vy [703] — однопользовательская (*single-tenant*) платформа с облачной (*cloud-native*) архитектурой, устраняющая привязку к одному вендору (*vendor lock-in*). Hyperswitch [700] решает ту же задачу открытым кодом (см. раздел 34.1); Juspay на этой кодовой базе в FY25 обработал свыше 300 млн транзакций в сутки при годовом TPV около $1 трлн [704].

В 2025 году рынок оркестрации платежей (*payment orchestration*) оценивается в $3,5 млрд с прогнозом $18 млрд к 2034 году и CAGR около 20 % (отчёт Intel Market Research) [705].

Оркестратор нужен, когда у ТСП одновременно работают несколько шлюзов с разной экономикой; на архитектурной диаграмме он находится между приложением продавца и парком PSP.

34.3 Маршрутизация запросов

При нескольких эквайерах шлюз решает, куда отправить авторизационный запрос, балансируя стоимость, долю одобрений и время ответа.

Критерии оптимизации

Стоимость. Тарифы у эквайеров разные, а межбанковская комиссия (*interchange*) зависит от типа карты, четырёхзначного кода категории ТСП (MCC, Merchant Category Code), региона эмитента и десятков других параметров. Модуль маршрутизации выбирает эквайера с наименьшей стоимостью для конкретной комбинации условий — например, направляет внутрироссийскую транзакцию по карте Мир через эквайера с более выгодным тарифом Национальной системы платёжных карт (АО НСПК), а международную — через другого, у которого ниже валютная наценка.

Доля одобрений. На одних и тех же диапазонах BIN (Bank Identification Number, идентификатор банка-эмитента в составе PAN) эквайеры показывают разную долю

одобрений. Причины бывают техническими или коммерческими: качество подключения к сети, скорость ответа, репутация ТСП у конкретного эквайера, локальный или международный маршрут. Накопив статистику по BIN, стране и сумме, модуль маршрутизации направляет транзакцию туда, где вероятность одобрения выше. При крупных объёмах даже небольшая разница в качестве маршрута даёт заметный прирост выручки.

Латентность. Каждая лишняя секунда в сценарии оплаты снижает конверсию. Если один эквайер стабильно отвечает заметно быстрее другого, модуль маршрутизации при прочих равных предпочтёт первый.

Эти три критерия противоречат друг другу. У самого дешёвого эквайера доля одобрений может быть хуже, а самый быстрый — оказаться самым дорогим. Модуль маршрутизации ищет оптимум при ограничениях, заданных продавцом: «минимизировать стоимость при доле одобрений не ниже X% и p95 — 95-м процентиле распределения — латентности не более Y мс». Адаптивное распределение трафика между маршрутами моделируют как задачу о «многоруком бандите» (*multi-armed bandit*).

Каскадная маршрутизация

«Мягкий отказ» (*soft decline*) — это отказ, формально устранимый: повторная попытка по другому маршруту или после дополнительной аутентификации может завершиться одобрением. Если первый маршрут вернул такой отказ, шлюз отправляет транзакцию второму эквайеру. Сам термин у сетей имеет более узкий нормативный смысл. Mastercard, например, требует мягкий отказ в странах со строгой аутентификацией клиента (SCA, Strong Customer Authentication) только тогда, когда операции типа CNP (Card Not Present, операции без физического предъявления карты) требуется аутентификация, но она отсутствует; в каскаде этот термин лучше не использовать как общий ярлык любого отказа [46]. Каскад опирается на то, что второй эквайер может получить от того же эмитента иной ответ, особенно когда его авторизационный запрос отличается: другой BIN эквайера, другой MCC, другой идентификатор терминала (Terminal ID, TID; в паре с идентификатором ТСП, MID).

ВАЖНО

Каскад и обычный повтор решают разные задачи: каскад идёт к *другому* эквайеру, повтор — *тому же* спустя время. Путаница порождает дубли: эмитент видит два запроса и одобряет оба.

Каскад сам по себе не создаёт дубля на стороне первого эквайера, но несёт другой риск: задержавшийся ответ от первого маршрута может прийти после того, как второй успел получить одобрение. На опоздавшее одобрение первого маршрута шлюз немедленно отправляет *reversal*.

Каскад применим только к части отказов, которые эквайер или сеть считают устранимыми. Для явно неверных реквизитов каскад не применяется: код 14 Invalid Card Number Visa относит к отказам, после которых повтор с теми же реквизитами запрещён, а 54 Expired Card — к отказам, требующим сначала обновить реквизиты [13]. Сами сети ограничивают избыточные повторные попытки; конкретные лимиты зависят от сценария и правил конкретной сети [46]. Модуль маршрутизации обязан различать эти два класса отказов по коду ответа и включать каскад только для устранимых; рабочая классификация кодов на каскадные, допускающие повтор и финальные разобрана в разделе 33.2.

Различие между каскадом, повтором и финальным отказом становится явным, если выразить правило выбора чистой функцией. Вход — история попыток и список

доступных эквайеров; выход — одно из трёх решений. Таблицы кодов в примере ниже иллюстративны: в промышленной системе их задают правила сети и спецификация процессинга.

```
from dataclasses import dataclass
from enum import Enum


class Decision(Enum):
  RETRY_SAME = "retry"
  CASCADE = "cascade"
  FAIL = "fail"


# Каноничные имена DE 39 по ISO 8583:1987; по 2 на класс для иллюстрации.

# Реквизиты карты или статус -- повтор и каскад не помогут.
INVALID_CARD_NUMBER = "14"
EXPIRED_CARD = "54"
HARD_DECLINES = frozenset({INVALID_CARD_NUMBER, EXPIRED_CARD})

# Сбой канала или эмитента -- безопасно повторить тому же эквайеру.
ISSUER_INOPERATIVE = "91"
SYSTEM_MALFUNCTION = "96"
TRANSIENT = frozenset({ISSUER_INOPERATIVE, SYSTEM_MALFUNCTION})

# Иной маршрут (BIN эквайера, MCC, Terminal ID) может дать иной ответ.
DO_NOT_HONOR = "05"
INSUFFICIENT_FUNDS = "51"
SOFT_DECLINES = frozenset({DO_NOT_HONOR, INSUFFICIENT_FUNDS})


@dataclass(frozen=True)
class Attempt:
  acquirer: str
  response_code: str


def decide(
  history: list[Attempt],
  available_acquirers: list[str],
  max_retries: int = 1,
  max_cascade: int = 2,
) -> Decision:
  if not history:
    raise ValueError("history пуст: первая попытка делается без решения")

  last = history[-1]
  code = last.response_code

  if code in HARD_DECLINES:
    return Decision.FAIL

  if code in TRANSIENT:
    same = sum(1 for a in history if a.acquirer == last.acquirer)
    if same <= max_retries:
      return Decision.RETRY_SAME
    return Decision.FAIL

  if code in SOFT_DECLINES:
    tried = {a.acquirer for a in history}
    remaining = set(available_acquirers) - tried
    if remaining and len(tried) <= max_cascade:
      return Decision.CASCADE
    return Decision.FAIL

  # Незнакомый код -- безопаснее не повторять.
  return Decision.FAIL
```

34.4 Интеграционные модели

Способ подключения продавца к шлюзу определяет, как делится ответственность за карточные данные и каков PCI scope продавца.

Размещённая платёжная страница (перенаправление)

В модели размещённой платёжной страницы (hosted payment page, HPP) продавец инициирует платёжную сессию через API шлюза и получает URL, на который перенаправляет покупателя. Покупатель вводит данные карты на странице шлюза, шлюз обрабатывает транзакцию и возвращает покупателя на сайт продавца с результатом. Параллельно шлюз отправляет продавцу асинхронное уведомление с финальным статусом.

HPP сводит PCI scope к минимуму. Карточные данные не проходят через серверы продавца, поэтому базовый HPP-сценарий соответствует SAQ A (Self-Assessment Questionnaire A, упрощённая анкета самооценки PCI DSS); более широкие сценарии, где элементы платёжной страницы частично исходят от самого продавца, к нему не применяются [242, 243]. Для небольших ТСП без выделенной команды безопасности это часто единственный реалистичный вариант.

Недостаток — потеря контроля над пользовательским сценарием. Перенаправление прерывает ход оплаты, страница шлюза может не совпадать с визуальным языком сайта, обратный переход после оплаты не всегда проходит гладко. При такой схеме сайт продавца остаётся в PCI scope: PCI SSC (PCI Security Standards Council) отдельно уточняет, что механизм перенаправления оставляет сайт продавца в области оценки [245].

Встроенная форма (iFrame / JavaScript SDK)

Продавец встраивает в свою страницу платёжную форму шлюза — встроенный HTML-фрейм (iFrame) или готовый JavaScript-компонент из набора инструментов разработчика (SDK, software development kit). Визуально форма выглядит как часть сайта продавца, но технически данные карты вводятся внутри iFrame, контролируемого шлюзом, и отправляются напрямую на серверы шлюза, минуя серверы продавца.

Продавец сохраняет контроль над интерфейсом: стилизует форму и ведёт оплату без перенаправления. В зависимости от реализации он заполняет SAQ A или SAQ A-EP; выбор определяется тем, проходят ли карточные данные через JavaScript продавца хотя бы транзитом [242, 243].

ВАЖНО

PCI DSS v4.0.1 задаёт для страниц оплаты отдельные требования — 6.4.3 и 11.6.1. В январе 2025 года PCI SSC обновил SAQ A: продавец подтверждает, что сайт не подвержен атакам через вредоносные скрипты (FAQ 1588 [70, 241]). Даже при вводе данных в iFrame шлюза вредоносный скрипт продавца может перехватить ввод через оверлей или клавиатурный шпион (*keylogger*) до того, как данные дойдут до iFrame, поэтому при встроенной форме продавцу нужно доказуемо контролировать скрипты на странице оплаты.

Прямая интеграция через API (server-to-server)

Продавец собирает данные карты на своей стороне через собственную форму и отправляет их на API шлюза в серверном запросе. Это даёт полный контроль

над интерфейсом и собственную предварительную логику: проверку адреса, предавторизацию, разделение платежа между несколькими получателями. Карточные данные проходят через серверы продавца, и сценарий не подпадает под модели SAQ A / A-EP [244],[1] существенно расширяя PCI scope.

Этот путь выбирают крупные ТСП и платёжные платформы, сертифицированные по PCI DSS Level 1, которым прямой контроль над данными нужен для собственного защищённого хранилища токенов и оптимизации логики повторов на уровне PAN.

ПРАКТИКА

Начинать разумно с iFrame или SDK — приемлемый пользовательский опыт при минимальном PCI scope. На server-to-server переходят, когда ограничения встроенной формы блокируют конкретный сценарий, например, *card-on-file* (CoF — сохранённые в продукте реквизиты карты для повторных списаний) с прозрачной для покупателя токенизацией или каскадную маршрутизацию на уровне PAN.

34.5 Надёжность и наблюдаемость

Надёжность шлюза определяется тем, как он справляется с неопределённостью: ответ запаздывает, внешний вызов теряется, продавец нажимает «повторить».

Идемпотентность

Повторный вызов с тем же набором параметров обязан давать тот же результат, что и первый, без побочных эффектов. Если продавец отправил запрос на авторизацию, не получил ответа из-за таймаута или сетевого сбоя и повторил его с тем же ключом идемпотентности (*idempotency key* — клиентский идентификатор операции, по которому шлюз дедуплицирует повторные запросы), шлюз возвращает результат первой попытки; вторая транзакция не создаётся [706, 707].

Для этого шлюз хранит сопоставление между `idempotency_key` и `transaction_id` в хранилище со строгой консистентностью — обычно в реляционной базе с уникальным индексом по ключу. Срок жизни ключа должен покрывать весь период, когда ещё возможны безопасные повторы одной и той же операции, — от сетевого сбоя сразу после ответа до позднего повторного запроса клиента.[2]

ВАЖНО

Идемпотентность нужна на обоих уровнях: шлюз дедуплицирует свои попытки, а эквайер должен узнавать повтор той же авторизации по сетевым идентификаторам. Если шлюз отправил авторизацию, не получил ответа и отправил повторно, эквайер может обработать оба запроса. Шлюз либо использует поля данных ISO 8583 (data elements, DE) DE 11 (STAN, System Trace Audit Number — внутренний номер транзакции в коротком интервале) и DE 37 (RRN, Retrieval Reference Number — идентификатор для последующих обращений к транзакции) для дедупликации эквайером, либо реализует сценарий *authorize-then-check* («авторизуй-затем-проверь») — при таймауте отправляет не повтор, а запрос статуса (*status inquiry*) у эквайера, когда такой механизм предусмотрен протоколом, и только при статусе «не найдено» повторяет авторизацию.

[1] [242, 243].

[2] Защита от двойной обработки, встроенная в саму архитектуру записи и не реализуемая в каждом обработчике отдельно, описана как сквозной принцип в инженерном обзоре собственного реестра Stripe [708]: каждое исправление оформляется новой проводкой со ссылкой на исходную, а разовые проверки «существует ли уже» не используются.

Обработка таймаута

Таймаут опасен тем, что отсутствие ответа — это *не* отказ. Если шлюз отправил авторизационный запрос эквайеру и не получил ответа до истечения таймаута, возможны исходы: (а) запрос не дошёл; (б) запрос дошёл, эмитент одобрил транзакцию, но ответ потерялся на обратном пути; (в) запрос дошёл, эмитент отказал, ответ тоже потерялся. В момент таймаута шлюз не различает эти случаи.

Наихудший исход — (б): деньги заблокированы на карте держателя, эмитент считает транзакцию одобренной, продавец не знает об этом и может повторить платёж, создав двойное списание. Карточные правила устраняют эту неопределённость сообщением *reversal*: Visa требует его на одобрение, пришедшее после таймаута [13]. Mastercard требует автоматический *reversal* (*automatic reversal*), если ответ на запрос авторизации не пришёл [46]. После таймаута шлюз сначала устраняет неопределённость и только затем выбирает ответ продавцу.

Сбой шлюза между приёмом ответа и записью

Ответ пришёл, эмитент одобрил транзакцию, но шлюз упал до того, как сохранил результат. Состояние транзакции рассинхронизируется между шлюзом и эмитентом: эмитент удерживает деньги на карте держателя, а шлюз после перезапуска находит запись в статусе `sent_to_acquirer` без сведений об исходе.

Если шлюз просто повторит авторизацию, эмитент получит два удержания на одну сумму — двойное списание. Если шлюз вернёт продавцу ошибку, деньги останутся заблокированными без товара. Шлюз использует двухстатусный жизненный цикл записи (`pending` → `final`), который иногда по аналогии называют «двухфазной фиксацией»; с распределённым двухфазным коммитом (2PC) из теории СУБД его роднит только идея двух стадий — координации между несколькими узлами здесь нет. До отправки запроса эквайеру шлюз создаёт запись `pending` с ключом идемпотентности и STAN. После перезапуска фоновый процесс выбирает все `pending`-записи, по которым прошёл заданный интервал ожидания ответа эквайера, и выполняет запрос статуса (*status inquiry*) к эквайеру по STAN и RRN. Порог здесь задаёт не сетевой таймаут авторизации, у Visa не короче 15 секунд (см. ниже), а интервал, после которого ответ по исходному каналу уже не ожидается. Если эквайер подтверждает одобрение, шлюз переводит запись в `approved` и помещает вебхук (*webhook*) в очередь. Если эквайер не знает о транзакции, шлюз записывает `failed` и разрешает повторную попытку. Когда запрос статуса недоступен (не все эквайеры его реализуют), шлюз отправляет *reversal*, чтобы снять холд, и возвращает продавцу ошибку с рекомендацией повторить [46].

Без этого механизма после каждого перезапуска шлюза остаются зависшие холды: держатели карт принимают их за списания, продавцы — за потерянные заказы. При тысячах транзакций в минуту даже секундный сбой создаёт десятки расхождений, разбор которых вручную через эквайера занимает дни.

Дедупликация

Дедупликация — защита от двойной обработки одной и той же транзакции — работает на нескольких уровнях. На уровне API она опирается на ключ идемпотентности. На уровне внутреннего конвейера — на уникальность комбинации STAN + RRN + amount + timestamp, которая отлавливает дубли, проскочившие мимо идемпотентности: например, при каскадной маршрутизации, когда два эквайера получают запрос с разными STAN, но за одну и ту же покупку. На уровне денежных состояний

дедупликацию обеспечивает внутренний реестр обязательств из гл. 35, а на уровне внешних файлов и банковской выписки — сверка из гл. 31.

Вебхуки и гарантия доставки

Обработка платежа редко заканчивается в момент синхронного ответа API. Результат транзакции возвращается продавцу синхронно, в ответе на запрос, и асинхронно, вебхуком на указанный URL. Синхронный ответ может не дойти; кроме того, после первого ответа появляются новые внешние события: завершился сценарий 3DS *challenge*, пришло подтверждение, сработал возврат, поступило позднее обновление статуса от процессора.

Платёжные сервис-провайдеры (PSP, payment service provider) — Stripe, Adyen, ЮKassa, CloudPayments, Т-Бизнес и Сбер для бизнеса — доставляют вебхуки по принципу «как минимум один раз». Эндпоинт должен быть доступен по HTTPS. Шлюз ждёт ответ 2xx, при неуспехе повторяет доставку. Продавец проверяет подпись события, прежде чем доверять содержимому запроса. У Stripe подпись передаётся в HTTP-заголовке `Stripe-Signature: t=...,v1=...`, где `t` — timestamp подписи, а `v1` — HMAC-SHA256 (Hash-based Message Authentication Code на базе SHA-256 [709]) от конкатенации timestamp, точки и тела запроса с использованием секрета подписи вебхуков [710].[1]

ПРАКТИКА

Обработчик вебхуков на стороне продавца обязан быть идемпотентным: до изменения состояния заказа нужно проверить, не обработан ли уже этот `event_id`.

Наблюдаемость

При тысячах транзакций в минуту метрики обязаны фиксировать деградацию до того, как она станет массовой.

Доля одобрений — процент одобренных транзакций от общего числа попыток, с разбивкой по эквайеру, диапазону BIN, стране эмитента, MCC и сумме. Падение доли одобрений за короткий интервал — повод к немедленному расследованию: причиной бывает как сбой у эквайера, так и массовая атака скомпрометированными картами.

Шлюз отслеживает время ответа по p50, p95 и p99 — 50-й, 95-й и 99-й процентили распределения времени обработки запроса, измеренного от получения HTTPS-запроса продавца до отправки ответа. Неожиданный рост p99 указывает на сбои аппаратного криптомодуля (HSM, hardware security module, см. гл. 10), медленный ответ эквайера или перегрузку собственного модуля маршрутизации.

Доля системных ошибок включает транзакции, завершившиеся таймаутом, сетевой или внутренней ошибкой сервера; бизнес-ответы `approved` и `declined` в эту метрику не входят. Рост этой доли на фоне обычного трафика — инцидент.

Качество доставки вебхуков измеряет доля уведомлений, дошедших с первой попытки; падение этой доли указывает либо на проблемы продавцов, либо на перегрузку собственной очереди доставки.

[1] Правила подписи и формат вебхуков у разных PSP различаются. У одних подпись HMAC-SHA256 в HTTP-заголовке, у других — токен JWT (JSON Web Token [711]) или собственная схема; список повторов и таймаутов тоже разный. Перед интеграцией с конкретным PSP сверяйтесь с его документацией; перенос ожиданий от Stripe на любую другую интеграцию ведёт к ошибкам.

34.6 REST API и ISO 8583

Для разработчика транзакция выглядит как JSON-объект с полями `amount`, `currency`, `payment_method` и `description`, а для банка-эквайера и карточной сети та же операция становится сообщением ISO 8583. В публичных API PSP — Stripe, Adyen, ЮKassa, CloudPayments, Т-Бизнес, Сбер для бизнеса — это JSON поверх HTTPS с чётко описанным поведением запроса и ответа [712].[1] Шлюз транслирует одно представление в другое; о самом стандарте см. гл. 6.

У ТСП в России есть ещё один маршрут, не имеющий аналога в карточных API международных PSP, — оплата через СБП по динамическому QR. На уровне продукта это тот же вызов API вида `POST /payments` с указанием способа оплаты СБП; затем PSP создаёт платёжную сессию у банка-партнёра и QR-код в формате СБП, а шлюз возвращает продавцу ссылку или содержимое QR-кода (*payload*) для отображения. Внутри маршрут идёт в OpenAPI ОПКЦ СБП (см. раздел 19.7), минуя ISO 8583. Поэтому шлюз нужно проектировать как оркестратор методов оплаты (компонент, координирующий несколько методов оплаты в едином сценарии), для которого ISO 8583 — лишь один из исходящих протоколов наряду с OpenAPI ОПКЦ СБП и собственными API эквайеров.

Конвейер обработки одного `POST /charges` внутри шлюза устроен так:

- **приём и валидация** — HTTP-компонент проверяет ключ API, парсит JSON, валидирует обязательные поля (`amount` > 0, `currency` по ISO 4217, наличие `payment_method`). Если передан `idempotency-key`, шлюз ищет сохранённый ответ и при совпадении возвращает его без повторной обработки.
- **проверка риска** — шлюз вычисляет оценку риска фрода сам или запрашивает её у внешнего сервиса. Если оценка выше порога отказа, шлюз отклоняет транзакцию до контакта с эквайером и экономит на стоимости авторизационного запроса.
- **маршрутизация** — модуль маршрутизации выбирает эквайера по диапазону BIN, валюте, MCC и текущей доле одобрений каждого канала. Если основной канал деградировал, каскадное правило переключает трафик на резервный маршрут.
- **извлечение PAN** — если `payment_method` ссылается на сохранённый токен, шлюз обращается к vault за FPAN (Funding PAN — реальный номер карты, в отличие от DPAN, токенизированного) или непосредственно за DPAN. Хранилище возвращает карточные данные в оперативную память процесса; на диск они не попадают.
- **сборка ISO 8583** — шлюз формирует сообщение с индикатором типа MTI 0100 (Message Type Indicator), заполняет битовую карту присутствия полей (bitmap) и поля данных (data elements, DE) согласно интерфейсной спецификации (IFS, Interface Specification) выбранного эквайера. Сопоставление полей описано ниже.
- **отправка эквайеру** — сериализованное сообщение отправляется по соединению TCP/TLS из пула. Шлюз запускает таймер ожидания ответа, длину которого согласует с эквайером в соглашении об уровне обслуживания (SLA, Service-Level

[1] Названия эндпоинтов и набор полей у разных PSP свои. У Stripe это `POST /v1/payment_intents` и `POST /v1/charges`, у ЮKassa — `POST /v3/payments` [713], у CloudPayments — `/payments/cards/charge` для одностадийного платежа или `/payments/cards/auth` для двухстадийного, с поддержкой JSON и form-encoded [714]. Иллюстрация ниже намеренно использует обобщённый `POST /charges` как нейтральный пример; дословным эндпоинтом конкретного PSP она не является.

Agreement) в пределах правил платёжной системы. Правила Visa запрещают эквайеру и ТСП прерывать ожидание ответа по POS-транзакции раньше 15 секунд (в Европейском регионе правило не действует) [13]. Правила платёжной системы «Мир» нормируют обработку авторизационных сообщений Операционным центром: не дольше 2 секунд [75].

- **парсинг ответа** — ответ MTI 0110 парсится, DE 39 (Response Code) транслируется в статус JSON. Шлюз сохраняет результат и обновляет запись транзакции.
- **событие реестра** — шлюз публикует событие `authorization.created` во внутреннюю шину. Модуль реестра обязательств фиксирует pending debit/credit (см. раздел 35.5).
- **вебхук** — шлюз помещает событие в очередь доставки продавцу, подписывает ключом HMAC эндпоинта и отправляет на URL обратного вызова с повтором при неуспехе.
- **синхронный ответ** — HTTP-компонент возвращает JSON продавцу с полями `status`, `id`, `decline_code` (при отказе) и `timestamp`.

Конкретные значения p50/p95 латентности конвейера зависят от расположения шлюза, эквайера и эмитента, протокола сети, нагрузки HSM и политики повторов. Публичных агрегированных бенчмарков по российскому рынку нет, поэтому числа в книге не приводятся; ориентир для собственного измерения — разделение полного времени ответа на сегменты: внутренняя обработка шлюза, ожидание эквайера, ожидание сети и эмитента.

Сборка ISO 8583 на шаге 5 превращает короткий API-запрос в сообщение из десятков обязательных полей. Продавец отправляет запрос с суммой `1500`, валютой `RUB`, номером карты и сроком действия. Шлюз транслирует это в MTI 0100 (Authorization Request), заполняя:

- `amount` 1500 → DE 4 Amount, Transaction — 12-символьное числовое поле, выровненное нулями, `000000150000` в минорных единицах, копейках;
- `currency` `RUB` → DE 49 Currency Code, Transaction — `643`, числовой код рубля по ISO 4217 [84];
- `card.number` → DE 2 Primary Account Number — PAN, до 19 цифр;
- `card.exp_month`, `card.exp_year` → DE 14 Date, Expiration — `YYMM`;
- внутренний ID терминала ТСП → DE 41 Card Acceptor Terminal Identification — 8-символьный код;
- MCC ТСП → DE 18 Merchant Type — 4-значный код.

Шлюз также генерирует поля, которых нет в запросе API продавца, но которые требует протокол — DE 11 (STAN), уникальный в коротком интервале, обычно сутки или смена, 6-значный номер транзакции, DE 7 (Transmission Date and Time), DE 12 (Time, Local Transaction), DE 22 (Point of Service Entry Mode) — способ ввода данных карты и канал предъявления, — и DE 25 (Point of Service Condition Code, условия предъявления карты в точке обслуживания); DE 22 кодирует, *как* были введены данные карты (магнитная полоса, чип, бесконтакт, ручной ввод), а DE 25 — в *каких* условиях это произошло (например, операция без присутствия держателя).

Если продавец использует сетевой токен вместо PAN, шлюз заполняет DE 2 токенизированным PAN (DPAN), а криптограмму от TSP передаёт в EMV data — данные транзакции по стандарту EMV, обычно размещаемые в DE 55, — или в специфичном для сети поле, зависящем от конкретного протокола маршрута [174].

Ответ эмитента проходит обратный путь. DE 39 (Response Code), двухсимвольный код, шлюз транслирует в JSON-поле `status` со значениями `succeeded`, `declined`, `requires_action` и дополняет текстовым описанием. Шлюз *теряет* часть информации: ISO 8583 различает десятки причин отказа (`05` Do Not Honor, `51` Insufficient

Funds, 61 Exceeds Withdrawal Limit), тогда как API шлюза группирует их в несколько категорий. Чтобы отличить «недостаточно средств» от «карта заблокирована», разработчику нужно проверять поле `decline_code` или его аналог в дополнение к `status`; подробнее об интерпретации кодов ответа см. [46].

ПРАКТИКА

Многие шлюзы предоставляют подробный протокольный лог транзакции (*raw response*) со значениями полей данных DE 39, DE 44 (Additional Response Data) и DE 55 (EMV data). Если шлюз этого не показывает и эквайер возвращает непонятный отказ, запрашивайте у эквайера подробную запись обмена ISO-сообщениями (*trace log*) по STAN и RRN — это единственный способ понять, что именно произошло на уровне протокола.

Описанная трансляция охватывает только авторизацию. Возврат, отмена (*void*) и подтверждение не сводятся к одному универсальному набору сообщений для всех шлюзов и эквайеров: конкретное соответствие зависит от стадии операции и протокола маршрута. На уровне API это несколько продуктовых действий, а на уровне карточного обмена — последовательность авторизаций, сообщений *reversal*, финансовых сообщений (*financial messages*, обычно MTI 0200/0220) и клиринговых обновлений (*clearing updates*), которые затем попадают во внутренний реестр обязательств и в сверку.

Авторизация укладывается в одну пару MTI 0100/0110 (см. раздел 6.2); различия *reversal*, *void* и *refund* разобраны в разделе 5.5. Сообщение *reversal* отправляется эквайеру до клиринга — MTI 0400 в интерфейсах с синхронным ответом эмитента, MTI 0420 в интерфейсах с односторонним уведомлением. Если эквайер не отправил *reversal* в пределах срока, заданного правилами сети (у Mastercard — период защиты от *chargeback* по коду 4808: семь суток для *final authorization* покупки и тридцать для *pre-auth*), эмитент обязан снять холд не позднее истечения этого срока, а единственным способом вернуть деньги после клиринга остаётся отдельный *refund* [46]. После клиринга возврат в сети с одним сообщением (*single-message*) идёт сообщением MTI 0200 с кодом обработки (*processing code*) 20 (*refund*), в сети с раздельными сообщениями (*dual-message*) — отдельным финансовым представлением через клиринг: IPM 1240 First Presentment у Mastercard, клиринговая запись эквайера у Visa (при приёме через Visa Acceptance эквайер строит её по файлу захвата TC 33.A) [14, 280]. В реестре обязательств *refund* появляется самостоятельной проводкой со ссылкой на исходную авторизацию, а не её зеркалом. Финансовое представление (*capture*) по двухстадийной авторизации закрывает холд и переводит сумму в клиринг — MTI 0220 у одних протоколов, финансовое представление через клиринговый файл у других, отдельный REST-эндпоинт эквайера [14, 280].

35 Реестр обязательств и события

Шлюз отвечает продавцу за сотни миллисекунд, но этот ответ не определяет денежное состояние операции. К этому моменту неизвестно: состоится ли подтверждение (*capture* — вторая стадия двухстадийной авторизации, на которой ранее зарезервированная сумма списывается фактически; в сети оно уходит финансовым представлением) [715, 716], когда придёт расчёт (см. раздел 5.2), каким будет размер комиссии эквайера и не обернётся ли успешная продажа через месяц chargeback. Промежуток между шлюзом и сверкой заполняет внутренний реестр обязательств: продукт фиксирует в нём собственные денежные обязательства и привязывает их к событиям платёжного потока [13, 46, 715].

35.1 Шлюз не заменяет учёт

Шлюз отвечает на вопрос «что произошло на входе в систему»: пришёл запрос, сработала проверка риска, эквайер вернул одобрение или отказ, продавцу отправлен вебхук. Для интеграции этого достаточно, для финансового учёта — нет.

Во-первых, статус шлюза не равен денежному результату операции. Авторизация со статусом «approved» означает лишь, что эмитент зарезервировал сумму или одобрил её к дальнейшей обработке. Подтверждение, клиринг (*clearing* — обмен данными о транзакциях между банками-участниками), расчёт (*settlement* — фактическое перемещение денежных средств между ними), отмены и корректировки в правилах карточных сетей оформляются как отдельные стадии [283]. К выплате готова только сумма, перешедшая в доступный остаток (*payout* — перевод доступного остатка с внутреннего баланса продавца на банковский счёт [717]) [13, 46, 715, 718].

Во-вторых, за одним внешним статусом скрывается несколько денежных последствий. Успешная транзакция в маркетплейсе порождает отдельные обязательства перед ТСП, платформой и эквайером. Свернуть их в одну строку `payment.status = succeeded` — значит потерять связь между движением денег и жизненным циклом операции.

Покупатель платит одну сумму, а из неё возникают выплата продавцу, комиссия платформы и удержание на доставку, если она есть. Если платформа гарантирует возврат, добавляется резерв под возвраты. Для шлюза это строка `payment = 5000`; для реестра — проводки с разными сроками признания и разными правилами отмены.

Шлюз из раздела 34.1 отвечает за приём и маршрутизацию. Реестр отвечает за состояние денег внутри продукта: что уже заработано, что зарезервировано, что доступно к выплате продавцу.

35.2 Двойная запись: минимум для платёжного продукта

Счёт — именованный накопитель денежных значений: `cardholder_receivable`, `merchant_pending`, `platform_fee_earned`. **Проводка** (бухгалтерская запись) — пара «дебет счёта A, кредит счёта B на одну и ту же сумму». Один счёт увеличивается, другой уменьшается, в зависимости от типа. **Двойная запись** (*double-entry bookkeeping*) фиксирует каждое денежное событие как минимум одной парной

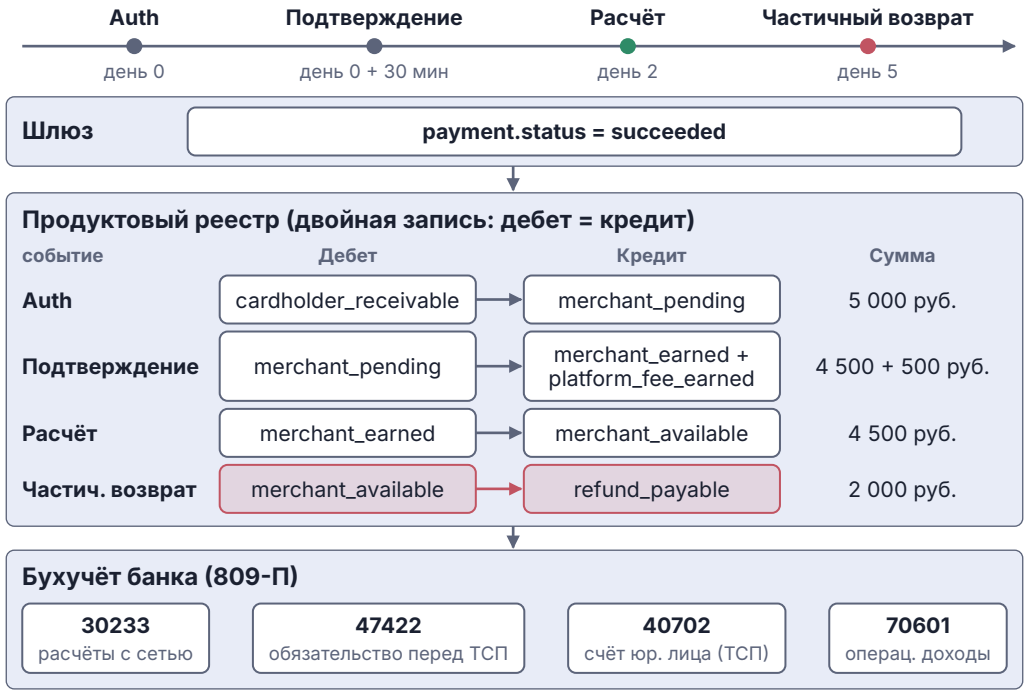


Рис. 65 — Шлюз и реестр обязательств: один платёж, четыре проводки.

проводкой: сумма дебетов равна сумме кредитов. Расхождение сумм означает ошибку в журнале: инвариант равенства встроен в саму схему учёта.

Двойная запись отличает реестр обязательств от обычного журнала. Журнал событий фиксирует «покупатель оплатил заказ»; реестр выводит из этого парные проводки.

Двойная запись делает аудиторский след проверяемым: любая потеря денег оставляет видимое расхождение. Обязательства и фактические остатки учитываются раздельно (`pending` отдельно от `available`, см. раздел 35.6). Банковская выписка устроена по той же двойной записи со стороны банка, поэтому сопоставление двух согласованных представлений надёжнее сравнения журнала с одной агрегированной цифрой.

35.3 Продуктовый реестр обязательств и бухгалтерский учёт банка

Внутренний реестр платёжного продукта и бухгалтерский учёт кредитной организации — разные системы, даже когда продукт встроен в банк.

Продукт — платёжный сервис, который видят покупатель и продавец: эквайринговый продукт банка, PSP, агрегатор, маркетплейс, кошелёк. Это уровень бизнес-логики (авторизация, подтверждение, выплата ТСП, chargeback, комиссия платформы). **Банк** — кредитная организация, на счетах которой проходят фактические движения денег: у банковского продукта это сам банк-оператор, у PSP или платформы — банк-эквайер или банк-партнёр. Эти два учётных уровня либо совпадают

(продукт работает внутри банка), либо разделены (продукт работает поверх партнёрского банка). Реестр обязательств — инструмент продукта, бухгалтерские счета — банка.

Продуктовый реестр обязательств — внутренний инструмент платёжного продукта. Он хранится в базах данных продукта, использует произвольную нотацию счетов (`merchant_pending`, `platform_fee_earned`, `refund_payable`), считает балансы партнёров — продавцов, плательщиков, платформ — и отвечает на вопросы продукта: сколько мы должны ТСП, сколько уже признано комиссией, какой резерв удержан под возвраты. Внешним бухгалтерским отчётом он не является.

Бухгалтерский учёт банка по РСБУ кредитная организация ведёт по Плану счетов кредитных организаций, утверждённого Положением Банка России от 24.11.2022 № 809-П «О Плане счетов бухгалтерского учёта для кредитных организаций» [6].[1] План счетов задаёт фиксированную нумерацию, где «30102» обозначает корреспондентские счета кредитных организаций в Банке России, «40817» — счета физических лиц, «40702» — счета коммерческих организаций, а «47422» — «Обязательства по прочим операциям», на котором, в частности, учитываются суммы клиентских платежей в пути. Банк обязан отражать платёжные операции на этих счетах: данные включаются в обязательную отчётность Банку России и проходят аудит.

Продуктовый реестр показывает жизненный цикл одной операции внутри продукта. Бухгалтерский учёт показывает общий срез по банковским счетам и обязательным группировкам. Запись продуктового реестра порождает на счетах 809-П одну, несколько или ни одной бухгалтерской проводки (холд на 809-П не отражается), а обратное верно не всегда: бухгалтерия агрегирует продуктовые записи и хранит их в свёрнутом виде. Для платёжного продукта в банке соответствие между внутренними счетами продуктового реестра и счетами 809-П фиксируется явно. Сверка идёт по этому соответствию, без дублирования двойной записи в обеих системах и без пересборки бухгалтерии.

Если платёжный продукт работает вне банка (например, в составе небанковской платформы), эта связь меняется: бухгалтерия по РСБУ ведётся у банка-партнёра или нескольких партнёров; продуктовый реестр связан с ней через интерфейсные документы, реестры и банковские выписки. В обоих случаях соответствие между внутренним реестром и Планом счетов закладывают в архитектуру с первой версии — иначе остаются два независимых параллельных учёта, которые не сойдутся.

35.4 Классы реализации реестра

Двойную запись в реестре обязательств гарантирует прикладной код, сторонний сервис или сама СУБД. Выбор задаёт стоимость поддержки, потолок производительности и цену миграции на следующую систему.

Реестр как код поверх универсальной СУБД

Проводки хранятся в обычной реляционной или документной базе, а инвариант двойной записи обеспечивает прикладной код. Такую схему реализует листинг `posting.py` из раздела 35.5. База остаётся универсальной (PostgreSQL, MySQL, ClickHouse, MongoDB), учётная логика расположена в сервисах продукта. Гибкость высокая: команда меняет схему счетов, правила начисления комиссии и конечный

[1] В силе с 01.01.2023; заменило 579-П.

автомат переходов без смены хранилища. Инвариант держится только на дисциплине команды: ошибка в одной из ветвей кода способна оставить незакрытое расхождение, а автотесты ловят только явно описанные сценарии.

Реестр как сторонний сервис

Внешний API, который продукт вызывает для записи проводок и запроса балансов. Инварианты двойной записи контролирует сервис, продукт отправляет ему события без знания внутреннего устройства хранилища. Modern Treasury Ledgers [719] — облачный управляемый реестр (*managed*) с декларируемой неизменяемостью (*immutability*): запись, внесённая в журнал, не редактируется и не удаляется, а исправления оформляются встречными проводками.[1] Formance Ledger [721] — реестр с открытым исходным кодом (лицензия MIT) и собственным DSL *numscript*, на котором проводки описываются как программа, а не как набор инструкций ORM.[2] Blnk Finance [723] — модульный реестр с открытым исходным кодом в той же нише: двойная запись, неизменяемый журнал, встроенные сверка и проводки в полёте (*inflight*). Этот класс подходит продукту, который отказывается от собственной инфраструктуры реестра и платит за SLA либо сам эксплуатирует открытый сервис.

Реестр как сама база данных

TigerBeetle [724] — OLTP-СУБД со встроенной в схему данных моделью двойной записи: каждый `transfer` обязан содержать `debit_account_id` и `credit_account_id` с равной суммой, инвариант двойной записи проверяет сама БД, поэтому приложение не может записать несбалансированный `transfer`. Журнал работает только на дозапись (*append-only*): проводку нельзя удалить или переписать, обратные движения оформляются отдельными записями. Декларируемая пропускная способность — до 1 000 000 переводов в секунду на одиночном узле. За эту скорость и встроенную целостность платят узкой специализацией: TigerBeetle не годится для произвольных запросов, бизнес-логики поверх проводок или сложной аналитики. В архитектуре приложения он работает рядом с основной СУБД, а не вместо неё.

Выбор класса реестра — архитектурное решение того же порядка, что выбор основной СУБД: переход с одного класса на другой задним числом обходится в отдельный проект миграции данных и учётной политики.

35.5 События: авторизация, подтверждение, возврат, спор

В карточном потоке реестр обрабатывает события авторизации, подтверждения, возврата, chargeback и начисления комиссии. Каждое порождает собственный набор проводок и не сводится к общему статусу «платёж успешен» [38, 46, 716]. Реестр атомарно записывает событие в журнал и сразу порождает проводки, поэтому продуктовая система видит связанные представления одной операции: *что произошло* и *как это отразилось в деньгах*.

[1] В октябре 2021 года Modern Treasury закрыл первичный раунд Series C на $85 млн при оценке более $2 млрд, а в марте 2022 года — расширение того же раунда на $50 млн от SVB Capital и Salesforce Ventures; суммарный Series C составил $135 млн [720].

[2] Formance прошёл набор Summer 2021 Y Combinator и привлёк раунд *pre-seed* на $3,1 млн (Y Combinator, Hoxton Ventures, Frst) [722].

Авторизация на 5 000 руб. ещё не создаёт выручку ТСП, но фиксирует ожидаемое обязательство. Подтверждение переводит обязательство в признанный доход; к выплате эти средства станут доступны только после расчёта. Возврат запускает обратное движение уже после подтверждения; платёж, не дошедший до подтверждения, отменяют (возврат для него не применяется) [715, 716]. Chargeback инициирует банк-эмитент; это самостоятельное событие, которое подчиняется правилам платёжной системы и несёт собственные сроки и комиссии (см. раздел 32.1) [38, 716].

ПРАКТИКА

Кодируйте возврат и chargeback как отдельные типы операций. Для клиента результат похож, но для продукта это разные процессы: возврат инициирует продавец, а chargeback приходит извне и проходит цикл оспаривания.

Событие отвечает за причинность, проводка — за денежный смысл. Попытка восстановить одно из другого задним числом лишает продукт объяснимости[1].

Переходы образуют конечный автомат: авторизация переходит в подтверждение или в отмену (*void* — аннулирование авторизации до её подтверждения; финансовой проводки в сети не порождает [715, 716]), но не наоборот; подтверждение переходит в «рассчитанное» состояние, после чего возможны возврат или chargeback; отмена допустима только до подтверждения. Возврат после расчёта порождает обратное движение средств, причём частичный возврат уменьшает обязательство, не отменяя его. Chargeback инициируется извне и возможен после расчёта; он открывает отдельную последовательность шагов — повторное представление (*representment* — ответ ТСП с доказательствами легитимности операции; у Mastercard этот шаг называется *second presentment*), доарбитраж (*pre-arbitration* — спор после повторного представления) и арбитраж (*arbitration* — финальное разрешение спора платёжной системой) [13, 38].

Каждый переход порождает проводку. Сумма обязательства перед ТСП движется по трёхфазной модели `pending` → `earned` → `available`, где `pending` — зафиксированное, но ещё не признанное обязательство (после авторизации до подтверждения); `earned` — признанная выручка ТСП (после подтверждения, ещё до фактического расчёта); `available` — доступный к выплате остаток (после расчёта) [718, 725]. Авторизация создаёт `pending`, подтверждение переводит `pending` в `earned`, отмена обнуляет `pending`, расчёт переводит `earned` в `available`. Возврат дебетует `available` и кредитует `refund_payable`, а chargeback дебетует `available` или `reserve` и открывает отдельный учётный цикл спора.

ВАЖНО

Состояние `pending` в реестре и *холд на счёте держателя*, который ставит эмитент после авторизации (см. раздел 5.1), — два разных таймера. Реестровое `pending` управляется внутренней логикой продукта — моментами подтверждения, расчёта, отмены; холд эмитента на авторизации (*auth-hold*) снимается автоматически по истечении срока, установленного правилами платёжной системы для категории операции, даже если в реестре проводка остаётся. Их рассинхронизацию разбирает сценарий *orphan authorization* среди краевых случаев ниже.

Когда автомат не описан явно, команда кодирует переходы разрозненными условиями, и через год единого правила для возврата после частичного chargeback уже нет.

[1] Тот же подход — системы-источники как конечные автоматы, чьи переходы разворачиваются реестром в проводки — описан на уровне архитектуры в инженерном обзоре собственного реестра Stripe [708]: декларируется около 5 млрд событий реестра в сутки и объяснимость (*explainability*) движения денег выше 99,9999 %.

Продавец маркетплейса продаёт товар за 5 000 руб., комиссия платформы — 10 %.

Авторизация (день 0). Когда эмитент одобряет авторизацию, реестр создаёт проводку: дебет `cardholder_receivable` 5 000 руб. и кредит `merchant_pending` 5 000 руб. Средства ещё не поступили платформе, но обязательство зафиксировано.

Подтверждение (день 0, через 30 мин). Когда продавец подтверждает отгрузку, реестр переводит `pending` в `earned` проводками: дебет `merchant_pending` 5 000 руб., кредит `merchant_earned` 4 500 руб. и кредит `platform_fee_earned` 500 руб. С этого момента платформа признала свою комиссию.

Расчёт (день 2). Когда эквайер перечисляет средства, реестр переводит `earned` в `available` проводками: дебет `merchant_earned` 4 500 руб. и кредит `merchant_available` 4 500 руб. После этого продавец вправе запросить выплату.

Частичный возврат (день 5). Когда покупатель возвращает часть товара на 2 000 руб., реестр оформляет это как дебет `merchant_available` 2 000 руб. и кредит `refund_payable` 2 000 руб. Комиссия платформы не пересчитывается (политика маркетплейса); если бы пересчитывалась, отдельная проводка уменьшила бы `platform_fee_earned` на 200 руб.

Каждый переход оставляет аудиторский след: сумма дебетов равна сумме кредитов, а баланс любого счёта восстанавливается обходом журнала проводок.

Знак сальдо зависит от классификации счёта по РСБУ. Активный счёт (`cardholder_receivable` — требование к плательщику, «где деньги») накапливает дебет; `balance` в листинге ниже считает сальдо как кредит минус дебет, поэтому для активного счёта остаток отрицательный. Пассивные счета (обязательства перед продавцом и плательщиком, признанная выручка — «откуда деньги») накапливают кредит и дают положительный.

Проводка — неизменяемая запись `(дебет, кредит, сумма)`; реестр — журнал таких проводок и операция запроса сальдо; событие платёжного потока — функция, формирующая группу проводок.

Минимальный API реестра — три типа и четыре функции событий. `Leg` хранит одну проводку и в конструкторе отвергает нулевые и отрицательные суммы: пустая проводка в этой модели считается ошибкой кода, и конструктор отсекает её до записи в журнал, что проще восстановления инварианта по журналу постфактум. `Ledger.post` принимает переменное число проводок и записывает их одной операцией: событие `confirm` порождает две проводки сразу, и журнал не остаётся в полусобранном состоянии при сбое между ними. `balance` восстанавливает сальдо обходом журнала вместо хранения текущего остатка рядом с проводками. Это медленнее в эксплуатации, но инвариант «сумма дебетов равна сумме кредитов» проверяет тот же код, который выводит сальдо, без отдельной фоновой ребалансировки. В промышленной эксплуатации прямой обход журнала заменяют производными структурами: таблицей снимков текущего остатка по счёту, материализованным представлением `balance` с инкрементальным обновлением или триггером накопления при записи проводки. Сам журнал остаётся источником истины, производные структуры — кеш с явной процедурой пересборки из журнала.

```
from dataclasses import dataclass, field


@dataclass(frozen=True)
class Leg:
  debit: str
  credit: str
  amount: int  # в минорных единицах (копейках)

  def __post_init__(self) → None:
    if self.amount <= 0:
```

(продолжение)

```
      raise ValueError("сумма проводки должна быть положительной")


@dataclass
class Ledger:
  journal: list[Leg] = field(default_factory=list)

  def post(self, *legs: Leg) → None:
    self.journal.extend(legs)

  def balance(self, account: str) → int:
    total = 0
    for leg in self.journal:
      if leg.credit == account:
        total += leg.amount
      elif leg.debit == account:
        total -= leg.amount
    return total


# Применение событий этой главы: одна функция -- одна группа проводок.


def authorize(ledger: Ledger, amount: int) → None:
  ledger.post(Leg("cardholder_receivable", "merchant_pending", amount))


def confirm(ledger: Ledger, amount: int, fee: int) → None:
  ledger.post(
    Leg("merchant_pending", "merchant_earned", amount - fee),
    Leg("merchant_pending", "platform_fee_earned", fee),
  )


def settle(ledger: Ledger, amount: int) → None:
  ledger.post(Leg("merchant_earned", "merchant_available", amount))


def refund(ledger: Ledger, amount: int) → None:
  ledger.post(Leg("merchant_available", "refund_payable", amount))
```

Внутренние счета реестра не совпадают один к одному со счетами 809-П на стороне банка-эквайера (или банка-партнёра, если речь о небанковском продукте).

`merchant_pending` соответствует None: авторизация фиксирует обмен сообщениями в сети, и в 809-П авторизационный холд балансовой проводкой не оформляется. Продуктовый реестр различает это состояние; банковский учёт отражает его только после клиринга. Дебет `cardholder_receivable` в реестре не синхронен с холдом, который эмитент удерживает на счёте плательщика: холд снимается по истечении срока, установленного правилами сети для категории операции, а проводка реестра закрывается только событием клиринга или отмены.

После клиринга возникает бухгалтерская пара 30233 / 47422 (30233 — «Незавершённые расчёты с операторами услуг платёжной инфраструктуры и операторами по переводу денежных средств», активный счёт; 47422 — «Обязательства по прочим операциям», пассивный) [6]: банк фиксирует требование к оператору платёжной инфраструктуры и встречное обязательство перед ТСП. `merchant_earned` и `merchant_available` отображаются в один и тот же 47422 — аналитические срезы одного и того же обязательства до выплаты ТСП. `refund_payable` отражается там же, но с противоположным знаком движения. `platform_fee_earned` отображается на 70601 («Доходы» — операционные доходы кредитной организации [6]), если речь о банке-партнёре или эквайере; в небанковском продукте этой проводки на 809-П не возникает, доход отражается в учёте платформы. Конкретное соответствие утверждается учётной политикой кредитной организации и зависит от схемы расчётов.

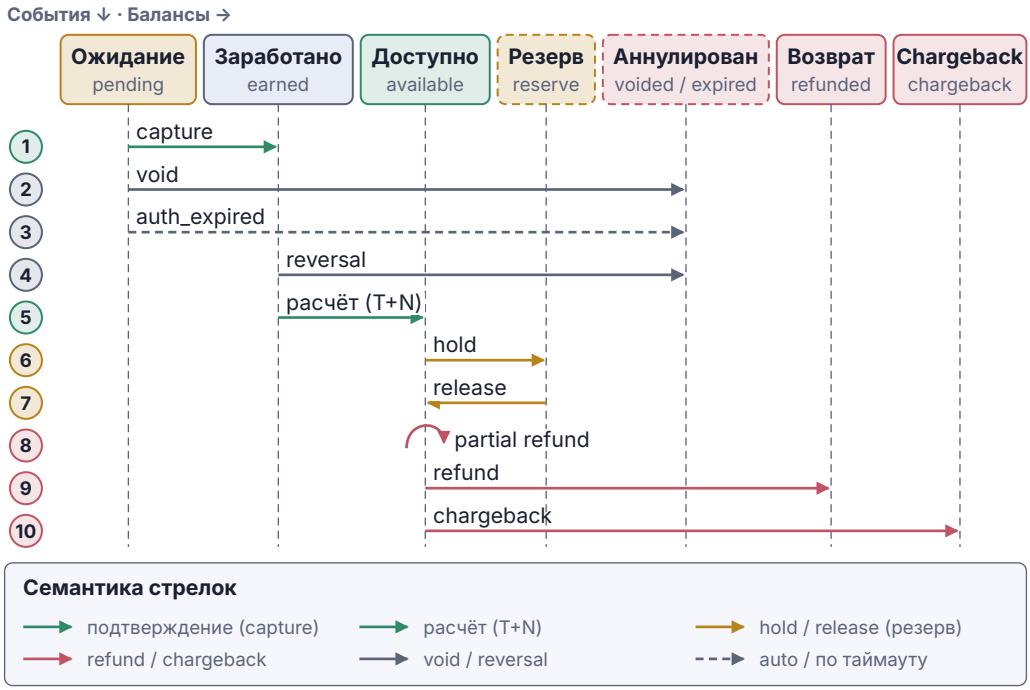


Рис. 66 — Балансы по горизонтали, события по вертикали.

35.6 Балансы, комиссии и правила перехода

Pending и **available** — состояния одного и того же основного баланса. Pending — сумма, недоступная к выплате: она зафиксирована между авторизацией и подтверждением, ожидает клиринга или удерживается до даты ближайшей выплаты. Available — та часть, которой платформа может распоряжаться: перечислить продавцу, зачесть в счёт комиссии или использовать для внутреннего неттинга (*netting* — взаимозачёт встречных требований до фактического перевода средств). Деньги переходят из `pending` в `available` по мере прохождения этапов жизненного цикла операции [718, 725].

Резерв (*reserve*) — отдельный балансовый механизм с собственными правилами пополнения, разморозки и закрытия. Резерв хранит сумму, изъятую из доступного остатка по правилу риска. Разновидности резерва:

- резерв под возвраты (*refund reserve*) — удержание под будущие возвраты, рассчитанное от объёма возвратов ТСП;
- минимальный остаток (*minimum balance*) — неснижаемая сумма на балансе ТСП для покрытия будущих споров и сборов;
- *holdback* — удержание фиксированной доли каждой транзакции до окончания согласованного срока под ожидаемые списания [718, 725, 726].

Без явного моделирования переходов `pending` → `earned` → `available` продукт перестаёт отличать «деньги есть» от «деньги когда-нибудь придут». Отсюда и расхождения между панелью продавца и банковской выпиской.

Комиссию платформы признают не в момент авторизации, а при подтверждении или расчёте, когда операция состоялась. Эквайерские сборы, сетевые комиссии,

валютная наценка и комиссии за chargeback появляются по собственным графикам, отличным от графика основной суммы. Реестр сначала признаёт ожидаемую комиссию, затем корректирует её по фактическому расчётному файлу [13, 46, 718].

Каждый резерв задаётся правилом перевода части `available` в отдельный баланс с собственным сроком разморозки.

Основной поток балансов и цикл оспаривания после chargeback показаны на рис. 66.

График выплат должен быть частью реестра: экспортёр банковских файлов только материализует уже рассчитанные правила перечисления. Ежедневные, еженедельные и ежемесячные циклы перечислений, ручные перечисления и задержки вида T+X — это правила перевода между внутренними балансами [717]. Правило, не выраженное в реестре, повторяется вручную в процедурах выплат и бэк-офиса, и единый источник истины теряется [725, 726].

35.7 Идемпотентность и передача в сверку

Идемпотентность на API шлюза разобрана в разделе 34.5. Шлюз присваивает операции стабильный внутренний идентификатор и связывает с ним все внешние сообщения через таблицу соответствия с STAN, RRN и другими идентификаторами процессинга [34]. Реестр принимает только нормализованные внутренние события с уникальным `event_id`. Повторная доставка того же события возвращает прежний результат, не порождая новых проводок [710]. Этот идентификатор распространяется и на многошаговые правки. Когда источник присылает отмену, правку этой отмены и подтверждение списания, реестр привязывает каждую запись к одному внутреннему идентификатору операции. Каждую правку реестр оформляет отдельной компенсирующей проводкой на тот же идентификатор; исходная проводка остаётся неизменной. Восстановление состояния опирается на внутренний идентификатор операции, потому что связь между записями непрозрачного источника ненадёжна (гл. 31, раздел 31.4).

Запись события в журнал и применение к балансам разделены: сначала фиксируется факт получения уведомления, затем событие атомарно меняет балансы. После сбоя между шагами повторный проход завершает запись проводок без дублей.

Сверка из гл. 31 сопоставляет внутреннее состояние продукта с внешними файлами и банковскими движениями. Сначала продукт фиксирует собственное состояние: шлюз записывает протокольный факт авторизации, реестр переводит этот факт в денежные движения, а сверка сопоставляет результат с TC33, IPM и банковской выпиской [13, 46, 283].

Без такого реестра сверка напрямую сопоставляет внешние файлы со статусами шлюза, а бэк-офис получает неполную картину: «операция одобрена, но непонятно, это доход, ожидаемая выплата или авторизационная блокировка».

Краевые случаи: orphan authorization и гонка возврата с chargeback

Реестры, спроектированные под счастливый путь (*happy path*), дают сбой на незавершённой авторизации и на одновременном возврате со спором. Оба сценария требуют явной обработки в коде реестра, иначе расхождения копятся незаметно.

Orphan authorization. Когда авторизация одобрена и реестр создал `merchant_pending`, а подтверждение не пришло (продавец отменил заказ, не получил вебхук или забыл подтвердить), правила платёжной системы задают предельный срок

от авторизации до клиринга для категории операции; по его истечении эквайер не вправе подтверждать транзакцию, а эмитент снимает соответствующий холд на счёте держателя по своей политике [13].[1] Без механизма экспирации запись `merchant_pending` остаётся в реестре бессрочно. Решение — фоновый процесс, который сканирует проводки в ожидании (*pending*) старше порога (максимальный срок холда по категории плюс буфер) и автоматически порождает событие `auth_expired`: дебет `merchant_pending` и кредит `cardholder_receivable` обнуляют обязательство. Без этого баланс `pending` растёт, искажая отчётность и блокируя сверку.

Гонка возврата и chargeback. Когда продавец инициирует возврат на 5 000 руб. в тот же день, когда эмитент открывает chargeback на ту же сумму, оба события дебетуют `merchant_available`; без защиты у продавца спишется 10 000 руб. вместо 5 000. Защита — блокировка на уровне транзакции: перед записью возврата реестр проверяет, нет ли открытого спора, а перед записью chargeback — нет ли уже проведённого возврата. Если возврат уже исполнен, chargeback переходит в статус `already_refunded`, а платформа отправляет повторное представление с доказательством возврата [38]; если же chargeback пришёл первым, возврат блокируется, и оператор разрешает конфликт вручную. Итоговый дебет с ТСП в обоих случаях не превышает исходную сумму транзакции.

ПРАКТИКА

Команде бэк-офиса нужна таблица соответствия внешних идентификаторов и внутренних счетов: авторизация, процессинг, заказ, выплата, спор. Без неё даже корректный реестр трудно сверить с внешними документами.

Реестр обязательств держится на инвариантах. Двойная запись из раздела 35.2 удерживает равенство дебетов и кредитов; соответствие счетов реестра и 809-П из раздела 35.3 сводит продуктовый учёт с бухгалтерским по Плану счетов; идемпотентный приём событий из раздела 35.7 удерживает однократность применения. Когда хотя бы один из них проверяется вручную или задним числом, в журнале появляются проводки без известного источника, и расхождения с банком разбираются вручную через переписку бэк-офиса. Реестр обязательств закладывается с первой версии: встраивание задним числом обходится в миграцию данных, переписывание учётной политики и пересборку бэк-офиса. Chargeback и *orphan authorization*, не записанные в журнал явным событием, превращаются в ручные операции бэк-офиса.

[1] По редакции *Visa Authorization Framework* от 13.04.2024 объединённый срок от авторизации до клиринга (*authorization-to-clearing time frame*) составляет 5 дней для большинства операций с физическим присутствием карты (*card-present*) и операций по инициативе ТСП (*merchant-initiated transactions*), 10 дней для CNP-операций по инициативе держателя (*cardholder-initiated*) и 30 дней для гостиниц (*lodging*), круизных компаний (*cruise lines*) и проката автомобилей (*vehicle rental*) при наличии флага *Estimated Authorization Indicator*. Mastercard и НСПК задают собственные пределы; срок удержания холда у эмитента формально его внутренняя политика, на практике повторяющая сроки сети [15, 75].

36 Мультивалютность и международные платежи

Один международный платёж проходит через несколько валют: покупатель видит цену в одной, платит картой или счётом в другой, продавец получает выплату в третьей, а расчёт с эквайером приходит в четвёртой. Каждая сумма фиксируется в свой момент времени. Для российского читателя мультивалютность в 2022–2026 годах означает работу под санкциями: ряд банков отключён от SWIFT (Society for Worldwide Interbank Financial Telecommunication — международная сеть финансовых сообщений) [9], корреспондентские отношения перестраиваются вокруг китайских, белорусских, казахстанских банков-посредников, растёт доля расчётов в юанях и других валютах дружественных юрисдикций. Часть этих юрисдикций входит в BRICS (акроним по странам-учредителям: Бразилия, Россия, Индия, Китай, ЮАР; на 2026 год объединение включает 11 стран, к учредителям присоединились Египет, Эфиопия, Иран, ОАЭ, Саудовская Аравия и Индонезия) [727]. Корреспондентские счета и международная логика карточных сетей разобраны в предыдущих частях; здесь — архитектура мультивалютного продукта и валютное регулирование после 2022 года.

36.1 Источники курса

В мультивалютном продукте курс фиксирует конкретная сторона; она же отвечает перед поддержкой и казначейством (*treasury* — внутренней службой компании, отвечающей за управление денежной позицией, ликвидностью и валютным риском; в отличие от государственного казначейства, упомянутого в гл. 24).

В первом варианте курс задаёт эмитент по правилам карточной сети. Так устроен стандартный карточный сценарий, когда продавец выставляет цену в одной валюте, а сумму в валюте карты эмитент определяет по правилам сети о валюте списания и конверсии [13, 314]. Для продавца схема проста, но итоговую сумму списания в валюте карты и продавец, и платформа узнают только после авторизации.

Во втором варианте курс контролирует эквайер или провайдер динамической конвертации валюты (Dynamic Currency Conversion, DCC), который показывает держателю карты итоговую сумму в домашней валюте ещё до авторизации. Цена становится предсказуемой для покупателя, но право задать курс и удержать маржу переходит к стороне, которая управляет DCC [13, 314].

В третьем варианте курс задаёт сама платформа. Так устроен кошелёк, сервис путешествий или маркетплейс с собственным валютным модулем, где интерфейс показывает курс, платформа берёт на себя риск его устаревания за короткий интервал, а затем хеджирует (страхует валютный риск встречным инструментом) или неттирует (взаимозачёт встречных требований до фактического перевода — «неттинг») фактические потоки на этапе расчёта.

В четвёртом варианте курс предоставляет внешний **FX-провайдер** (foreign exchange — операции на валютном рынке; источник зависит от валютной пары и канала — биржевая площадка, межбанковский рынок или уполномоченный банк), а платёжный продукт привязывает платёж к уже рассчитанной сделке. Так работают B2B-сервисы (business-to-business, расчёты между юридическими лицами) и платформы выплат, где цена перевода действует дольше одной сессии

Таблица 48 — Модели владения курсом в мультивалютном продукте

Владелец курса	Модель	TTL курса	Сумма держателю	Источник курса
Эмитент	стандартный карточный	фиксация при клиринге	постфактум	правила сети; диапазоны наценок в правилах сетей публично не закреплены
Эквайер / DCC-провайдер	DCC	момент авторизации	до авторизации	провайдер DCC
Платформа	собственный курс	короткий (сессия)	в момент выбора	валютный модуль
FX-провайдер	B2B / форвард	дольше одной сессии	B2B / пакетно	FX-провайдер

оплаты. Валютный риск несёт казначейство корпоративного клиента и закрывает его отдельной сделкой, например форвардным контрактом.

Платформа показывает клиенту курс в момент выбора, подтверждение приходит через час, и за это время курс изменился. Разница между показанным и фактическим курсом — убыток той стороны, которая зафиксировала обязательство. Курс действует в пределах TTL (time-to-live — срок действия котировки), и при позднем подтверждении платформа либо пересчитывает по актуальному курсу, либо принимает риск на себя. Значения TTL и допустимый диапазон волатильности для основных валютных пар оператор подбирает по собственным данным; короткий TTL увеличивает долю истёкших сессий, длинный — валютный риск. Без явного TTL потери на устаревшем курсе обнаруживаются только при ежемесячной сверке казначейства.

Подписка с ежемесячным списанием в EUR при выплате продавцу в USD проходит через конверсию 12 раз в год, и при каждой конверсии курс другой; совокупная дельта влияет на маржу платформы. Курс хранится как отдельный объект с явным источником, значением, моментом фиксации, TTL и стороной, несущей риск.

Минимальный реестр котировок принимает котировки от разных источников, отбрасывает устаревшие (по TTL) и слишком широкие по спреду (выше заданного порога в базисных пунктах, basis points, bps — сотых долях процентного пункта), и возвращает последнюю по времени из оставшихся. Источник времени вынесен в параметр `now`, чтобы тест не зависел от системного таймера:

ПРАКТИКА

Если продукт обещает клиенту «ваш курс», у этого курса должны быть явный источник и срок действия.

```
from collections.abc import Callable
from dataclasses import dataclass, field

# 1 pip = 1/10000 единицы quote-валюты. Хранение в pip-точности
# (целые), а не float, исключает накопление погрешности при цепочках
# конверсий.


@dataclass(frozen=True)
class Quote:
  source: str  # ECB, INTERNAL_TREASURY, REUTERS, ...
```

(продолжение)

```
    base: str  # ISO 4217: "EUR"
    quote: str  # "USD"
    bid_pips: int  # цена покупки base за quote, в pip
    ask_pips: int  # ask >= bid; spread = ask - bid
    ts: float  # epoch seconds, момент фиксации источника


  @dataclass
  class QuoteBook:
    now: Callable[[], float]
    ttl_seconds: float
    max_spread_bps: int  # basis points: 100 bps = 1%
    _quotes: list[Quote] = field(default_factory=list)

    def add(self, quote: Quote) → None:
      self._quotes.append(quote)

    def applicable(self, base: str, quote: str) → Quote | None:
      cutoff = self.now() - self.ttl_seconds
      best: Quote | None = None
      for q in self._quotes:
        if q.base ≠ base or q.quote ≠ quote:
          continue
        if q.ts < cutoff:
          continue
        mid_pips = (q.bid_pips + q.ask_pips) // 2
        if mid_pips <= 0:
          continue
        spread_bps = (q.ask_pips - q.bid_pips) * 10_000 // mid_pips
        if spread_bps > self.max_spread_bps:
          continue
        if best is None or q.ts > best.ts:
          best = q
      return best
```

36.2 Фиксация валюты расчёта

Валюта цены (transaction currency, в правилах карточных сетей также «валюта операции») — та, которую видит покупатель и которую продавец ожидает на странице оплаты. **Валюта списания** (billing currency, она же «валюта карты») — та, в которой эмитент дебетует держателя карты. **Валюта расчёта** (settlement currency) — та, в которой сеть или эквайер фактически рассчитывается с продавцом или платформой [13, 15]. Трёхбуквенные коды валют (RUB, USD, EUR, CNY, KZT и др.) даются по стандарту ISO 4217 [84].

Держатель карты работает в своей валюте, расчётная инфраструктура сети — в валюте расчёта, эквайер — в валюте своей юрисдикции. Для международных коридоров в Visa и Mastercard валютой расчёта по умолчанию выступают USD или EUR; в платёжной системе «Мир» внутрироссийский расчёт проходит в рублях через платёжную систему Банка России.

При **единой валюте расчёта** внутренний реестр обязательств и выплаты ведутся в одной базовой валюте, поэтому учёт упрощается до одного казначейского баланса, одной логики комиссий и меньшего числа сценариев для сверки. Плата за это — постоянная конверсия на входе или выходе из системы и зависимость от валютной наценки внешнего провайдера.

При **нескольких валютах расчёта** система хранит обязательства и расчёты в нескольких валютах. Реестр обязательств и логика выплат сложнее, но лишней конверсии нет, а фактические валютные позиции не смешиваются в одну синтетическую сумму.

Один и тот же EUR в разных частях системы — это валюта цены, валюта списания, валюта расчёта или валюта хранения обязательства; роли могут не совпадать.

Продавец из России продаёт цифровой продукт покупателю из Казахстана; цена выставлена в рублях, покупатель оплачивает **картой UnionPay казахстанского банка** в тенге, российский эквайер UnionPay рассчитывается с продавцом в рублях. Валюта цены — RUB, валюта списания — KZT (валюта карты), валюта расчёта — RUB. После марта 2022 года это *единственный массовый карточный канал* для иностранного держателя карты в российский ТСП (торгово-сервисное предприятие): международные сети Visa и Mastercard в РФ закрыты для иностранных карт [5, 75], а по соглашениям НСПК с национальными сетями маршрутизируются только пары «Мир ↔ национальная ПС», не карты Visa или Mastercard. Из четырёх таких сетей-партнёров на дату издания устойчиво работает лишь БЕЛКАРТ (Беларусь): Uzcard (Узбекистан) прекратил приём «Мира» ещё в 2022 году, а АРКА (Армения) и Элкарт (Кыргызстан) свернули его в 2024 году вслед за внесением НСПК в список SDN [634]. Реестр обязательств должен хранить все точки фиксации — сумму в KZT на момент авторизации, применённый курс при клиринге и сумму в RUB на момент расчёта.

На рис. 67 у каждой фазы свой источник курса: EUR→USD конвертируется правилами сети при клиринге, USD→GBP — внешним FX-провайдером выплаты на момент перевода продавцу. Авторизация и клиринг занимают секунды и часы, расчёт и выплата — дни.

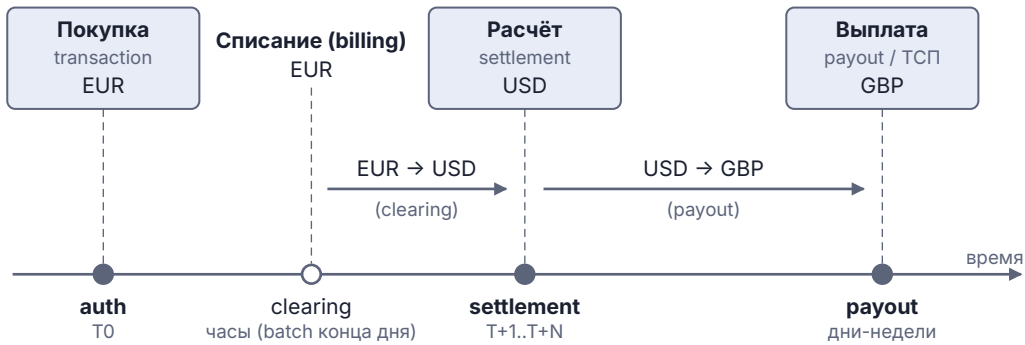


Рис. 67 — Жизненный цикл операции в нескольких валютах: transaction → billing → settlement → payout.

36.3 DCC и маршрутизация по валютным коридорам

Валютный коридор — пара «страна покупателя / страна ТСП» или «валюта источника / валюта получателя», для которой задан набор маршрутов, эквайеров и провайдеров. Коридор определяет, через какую сеть пойдёт авторизация и в какой валюте пройдёт расчёт.

С DCC расчёт идёт обычным маршрутом сети, а сумма списания для клиента считается отдельно [13, 46].

Продукт хранит исходную сумму, показанную сумму и применённый курс как отдельные значения, не выводя одно из другого задним числом. Только так платформа объясняет клиенту списание и сверяет удержанную маржу DCC [13, 46].

Маржа DCC возникает на спреде (разнице между ценой покупки и ценой продажи валюты), когда конверсия предлагается по курсу, менее выгодному для держателя карты, чем межбанковский (он же оптовый — курс, по которому платёжная сеть конвертирует на стороне расчёта). Разница в виде наценки (валютной маржи сверх

оптового курса) остаётся у эквайера или его провайдера DCC. Конкретное распределение определяется коммерческим договором между ними и в публичных правилах сетей не закреплено. Держатель карты видит сумму в знакомой валюте до операции, но платит за это наценкой, встроенной в курс. Сети требуют явного раскрытия наценки и согласия клиента до операции.

Покупатель платит 100 EUR картой американского банка в ТСП в Германии. Без DCC эквайер отправляет транзакцию на 100 EUR; сеть конвертирует её при клиринге по своему оптовому курсу с наценкой сети, и держатель карты видит итоговую сумму в своей домашней валюте (USD) только после списания. С DCC эквайер через провайдера DCC предлагает держателю карты фиксированную сумму в его домашней валюте сразу на терминале по курсу провайдера; разница между этим курсом и оптовым — плата за фиксацию суммы до операции. Значения наценок отличаются у разных провайдеров DCC и раскрываются клиенту перед операцией.

Если ТСП продаёт только в одной стране и получает выплаты в местной валюте, DCC не нужен: конверсию делает сеть при клиринге. Если ТСП предлагает DCC ради повышения маржи, нужен провайдер DCC, раскрытие наценки и согласие клиента; репутационный риск у этого варианта высокий. Если ТСП работает в нескольких странах и стремится снизить долю международных отказов, локальный эквайер в каждой стране повышает долю одобрений и убирает международную наценку, но требует юридического присутствия и отдельной расчётной модели в каждой юрисдикции [13, 46].

Политика маршрутизации по коридору, BIN, стране эквайера и типу ТСП задаёт допустимость DCC и источник курса.

Согласие клиента, раскрытая наценка и данные для последующей проверки фиксируются как поля события транзакции: по ним позже доказывают, что конверсия была предложена корректно [13, 46].

Платформа, работающая с несколькими странами, эквайерами и схемами выплат, маршрутизирует платежи по коридорам: для каждой пары «страна покупателя / страна ТСП» выбираются эквайер, валютная схема и способ выплаты.

Выбор коридора зависит от стоимости авторизации и расчёта, доли одобрений для нужного диапазона BIN, валюты выплаты продавцу и стороны, которая несёт валютный риск. Параметры обоих маршрутов по этим факторам показаны в табл. 49; состав параметров согласован с публичными правилами Visa и таблицами Visa USA IRF [13, 21].

Дорогой маршрут через эквайера страны держателя карты повышает $P(\text{approve})$, но увеличивает комиссию. Дешёвый маршрут через эквайера страны ТСП снижает комиссию, но и $P(\text{approve})$ на международных картах становится ниже. При высоком среднем чеке потеря на отказанной транзакции дороже разницы в комиссии, и выбор смещается к дорогому маршруту; при низком чеке выгоднее обратное.

При **выплате в домашней валюте продавца** платформа сама консолидирует и конвертирует все входящие потоки. Для продавца модель проще, для казначейства платформы — сложнее.

При **выплате в валюте исходного потока** платформа ведёт **раздельные валютные балансы продавца** (отдельный баланс на каждую валюту) и платит продавцу в той валюте, в которой пришёл поток. Конверсий меньше, но у продавца появляется несколько валютных балансов и отдельный график выплат по каждому.

Таблица 49 — Маршрутизация по коридору: сравнение стратегий для одного платежа

Параметр	Маршрут A: UK-эквайер для всех транзакций	Маршрут B: US-эквайер для US-карт, UK для прочих
Тип транзакции	международная	внутренняя для US-карт
Доля одобрений	ниже (эмитент видит как международную)	выше (эмитент видит как внутреннюю)
Межбанковская комиссия	международный тариф Visa USA	US Domestic IRF
Комиссии сети	+ International Service Assessment	стандарт + комиссии эквайера
Валюта расчёта	GBP	USD + GBP (раздельные балансы)
Подключение	минимальный	юрлицо в США, договор с US-эквайером
Когда выигрывает	**низкий объём US-карт**	**значимый объём US-карт**

ТСП с продажами в Великобритании, держатель Visa USA, средний чек 50 GBP.

ПРАКТИКА

Если внутри принимаются потоки в нескольких валютах, а продавцу обещан один баланс, у валютной позиции (чистой величины обязательств в данной валюте — длинной или короткой), лимитов и источников курса должен быть явный владелец.

Доля одобрений, комиссия, валюта выплаты и сторона валютного риска конкурируют между собой: маршрут, лучший по одному из этих параметров, редко остаётся лучшим по остальным, и единого показателя для выбора коридора нет. Платформа закрепляет за каждой парой «страна покупателя / страна ТСП» одну рабочую конфигурацию и поддерживает заранее подготовленные резервные, чтобы при падении доли одобрений или при отзыве BIN-диапазона переключение занимало минуты. Платформа считает фактическую стоимость каждой конфигурации по среднему чеку, и цифры берутся из собственной статистики, потому что публичные таблицы interchange покрывают только комиссионную часть; поведение конкретного BIN на конкретном эквайере наблюдает только оператор.

36.4 Сверка по валютам

Расхождения в мультивалютном продукте появляются после авторизации, когда одна и та же операция существует сразу в нескольких видах: на странице оплаты — в валюте цены, в журнале авторизации — одной суммой, в клиринге — с другой валютой расчёта, в отчёте о выплате — после удержания комиссии и валютного спреда. Валютная сверка остаётся отдельным процессом: карточные правила прямо требуют сверять данные сети с внутренними записями, а в Mastercard это сформулировано как ежедневная обязанность сверять итоги и транзакции с внутренним учётом [15].

Внутренний реестр обязательств хранит исходную валютную пару полностью — исходную сумму, сумму после конверсии, источник курса и момент его фиксации.

Комиссия и конверсия считаются отдельно. Если курсовая разница смешана с комиссией эквайера, казначейство не увидит, какая часть маржи ушла в курс, а какая — в комиссию.

Выплаты сверяются по раздельным валютным балансам; общий итог используют после проверки каждой валюты. Совпавший общий итог скрывает недостачу в отдельной валюте, когда одна валюта компенсирует другую.

Покупка за 100 EUR: расчёт по курсу 1,08 = 108 USD, комиссия эквайера 2,5 % = 2,70 USD, interchange 1,5 % = 1,62 USD, комиссия платформы 3 % = 3,24 USD, выплата продавцу = 108 − 2,70 − 1,62 − 3,24 = 100,44 USD. Если продавец получает выплату в GBP по курсу 0,79, итого 79,35 GBP. Одна и та же покупка существует в пяти представлениях — 100 EUR на странице оплаты, 100 EUR в авторизации, 108 USD в расчёте, 100,44 USD в нетто-выплате, 79,35 GBP на счёте продавца.

Типовая ошибка сверки — смешение валютной дельты и комиссий. Если 7,56 USD удержаний (2,70 + 1,62 + 3,24) учтены как курсовой убыток вместо раздельных комиссий, казначейство получает завышенную курсовую дельту. Каждое удержание имеет свой тип: interchange, assessment, комиссия платформы, валютная наценка — и сверяется отдельно; агрегированная сумма скрывает эту структуру. На рис. 68 удержания между расчётом и нетто-выплатой расписаны построчно с итогом −7,56 USD; валюта списания держателя карты (billing) на схеме отдельной точкой не показана.

Рис. 68 — Валютные представления одной транзакции.

36.5 Валютное регулирование после 2022 года

Валютные операции в России регулирует Федеральный закон от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле» [728]. Он определяет понятия резидента и нерезидента, перечень разрешённых валютных операций между ними и порядок валютного контроля. Подзаконные акты Банка России конкретизируют процедуры контроля. **Представление документов валютного контроля** — передача в уполномоченный банк контракта, счетов, актов и прочих подтверждающих документов по операциям с нерезидентами. **Постановка контракта на учёт** — присвоение контракту уникального номера в уполномоченном банке; обязательна для контрактов с нерезидентами выше пороговой суммы, закреплённой Инструкцией Банка России от 16.08.2017 № 181-И «О представлении документов валютного

контроля» [729].[1] **Репатриация валютной выручки** — обязанность резидента-экспортёра обеспечить поступление валютной выручки на счета в уполномоченных банках, а резидента-импортёра — возврат авансов по неисполненным импортным контрактам в срок, установленный контрактом. В платёжном продукте с международными операциями с участием российской стороны 173-ФЗ и подзаконные акты учитываются при открытии валютных счетов, идентификации клиента, направлении валютной операции в банк и формировании отчётности.

После марта 2022 года международные валютные расчёты для российских банков перестроились: ряд крупнейших банков был отключён от SWIFT по решению Совета ЕС, оформленному Регламентом Совета (EU) 2022/345 [615, 634]. SWIFT работает для значительной части российских банков и для большинства корреспондентских отношений с банками дружественных стран, но отключённым банкам пришлось перенести финансовые сообщения на альтернативные каналы.

СПФС (Система передачи финансовых сообщений Банка России; см. раздел 1.3) для отключённых от SWIFT банков превратилась из локальной альтернативы в основной канал финансовых сообщений с банками-партнёрами в ЕАЭС, СНГ и BRICS [12].

Расчёты в юанях стали отдельным каналом для экспорта и импорта после 2022 года. Расчёты в CNY между российскими и китайскими банками проходят через систему CIPS (Cross-Border Interbank Payment System) — китайскую инфраструктуру межбанковских расчётов в юанях. Оператор — Cross-border Interbank Payment System Co., Ltd., под надзором Народного банка Китая [730]. Российские банки подключаются к CIPS как прямые или непрямые участники либо проводят платежи через банки-посредники в Китае.

Корреспондентские счета через банки-посредники. Для отключённых от SWIFT российских банков корреспондентские отношения с зарубежными банками-партнёрами перестраиваются через банки-посредники в дружественных юрисдикциях — Китай, Индия, ОАЭ, Турция, страны Центральной Азии. Цепочка расчётов удлиняется, каждая операция проходит дополнительные проверки комплаенса и валютного контроля.

BRICS Pay и связанные инициативы. В BRICS обсуждаются проекты межоператорной интеграции национальных платёжных систем (BRICS Pay, BRICS Bridge) для прямых расчётов в национальных валютах без обращения к доллару [731].[2]

Отсюда следуют требования к архитектуре платёжного продукта в России. Во-первых, мультивалютная модель должна предусматривать несколько каналов расчёта: SWIFT (для неотключённых банков и зарубежных коридоров), СПФС (для внутрироссийских расчётов и ЕАЭС), CIPS (для расчётов в юанях), двусторонние и многосторонние соглашения. Во-вторых, после 2022 года выбор валют расчёта сместился к национальным валютам дружественных стран (CNY, AED, INR, KZT, BYN); USD и EUR остаются возможными, но требуют согласования с банком-партнёром по каждой операции и подпадают под санкционный контроль. В-третьих, валютный контроль по 173-ФЗ требует представления документов и постановки контрактов на учёт независимо от выбранного канала расчёта.

[1] Инструкция 181-И заменила Инструкцию 138-И.

[2] Отдельный проект межбанковского обмена цифровыми валютами центральных банков (CBDC, central bank digital currency) mBridge — многосторонняя платформа CBDC-расчётов — вёлся под BIS Innovation Hub (Банк международных расчётов, Bank for International Settlements) совместно с центральными банками Китая, ОАЭ, Гонконга и Таиланда; BIS вышел из проекта 31.10.2024, дальнейшее развитие продолжают участники без BIS; mBridge не является проектом BRICS.

ПРАКТИКА

Обещание «международный платёж в любой валюте» должно соответствовать фактическим валютным коридорам: набор работающих валют, банков-посредников и каналов зависит от санкционного статуса участников и меняется.

36.6 Корреспондентский банкинг и ISO 20022

Корреспондентские расчёты разобраны в разделе 1.2, миграция к ISO 20022 — в разделе 21.7.

Расчёт по международной операции проходит по более длинной цепочке, чем авторизация, и занимает больше времени [591, 732]: одобрение за секунду не означает выплату в тот же день. Расчётный банк, карточная сеть и валютный провайдер в модели продукта фиксируются как разные роли; продукт указывает ответственного за каждую стадию без отговорок вида «деньги идут через SWIFT».

Переход отрасли на ISO 20022 даёт структурированные поля, которые облегчают комплаенс-проверки и сверку, но сами по себе не отвечают на вопрос, кто несёт валютный риск и в какой валюте учитываются внутренние обязательства [10, 436, 733].

Структурированные поля ISO 20022 дают продукту явное представление участников перевода — но только когда внутренняя модель уже различает плательщика, конечного получателя, посредников и назначение перевода как отдельные сущности. Если в исходной модели платёж сводился к паре «отправитель — получатель» с произвольным текстом в поле описания, миграция к ISO 20022 на стороне сетевых сообщений не решит проблему: внутри продукт по-прежнему теряет цепочку. Поэтому переход начинается с инвентаризации внутренних полей; шлюзовая интеграция подключается, когда продукт уже хранит цепочку сущностей.

Корреспондентский банкинг в санкционных условиях добавляет требование: каждое дополнительное звено цепочки (банк-посредник в дружественной юрисдикции) добавляет комплаенс-проверки и риск возврата платежа на любой стадии. Продукт фиксирует, кто и какую информацию отправляет на каждом звене, и хранит копию переданных полей на своей стороне — иначе для разбора отказа придётся восстанавливать цепочку сообщений по логам трёх-четырёх банков с разными политиками хранения. ISO 20022 формализует синтаксис сообщений; собственный реестр стадий расчёта всё равно нужен для разбора отказов и сверки цепочки.

37 Процессинговый центр

Процессинговый центр связывает банк и карточную сеть: принимает сообщение ISO 8583, выбирает маршрут, выполняет криптографические проверки, ведёт журнал операций и позже превращает авторизацию в клиринговую и расчётную запись.

Процессинг существует в трёх конфигурациях. **Процессор эквайера** (*acquirer processor*) обслуживает эквайера: приём сообщений от терминалов и шлюзов, маршрутизация авторизаций в сеть, формирование исходящего клирингового файла, разбор входящих расчётных сообщений. **Процессор эмитента** (*issuer processor*) обслуживает эмитента: CMS, верификация ARQC и генерация ARPC, обработка входящих клиринговых записей по своему BIN, выпуск скриптов эмитента (*issuer scripting*), токенизация на стороне эмитента. **Совмещённый процессор** (*coupled processor*) объединяет обе стороны и обрабатывает операции *on-us* напрямую, минуя сеть.

По 161-ФЗ процессор отдельного банка остаётся его внутренней инфраструктурой [1]. Операционным и платёжным клиринговым центром (ОПКЦ) платёжной системы выступает выделенный оператор: НСПК — для ПС Мир и по поручению Банка России для СБП (оператор СБП — сам Банк России). Самостоятельный процессор-вендор, обслуживающий несколько участников, привлекается оператором платёжной системы как оператор услуг платёжной инфраструктуры (ОУПИ) и попадает в перечень ОУПИ, который ведёт этот оператор (см. раздел 37.4).

Внутри процессинг состоит из коммутатора авторизации, пула HSM, клирингового и расчётного модулей; каждый компонент задаёт свои требования к задержке, доступности и контролю над ключевым материалом. Распределение этих компонентов по трём конфигурациям сведено в табл. 50.

Таблица 50 — Распределение функций процессингового центра по конфигурациям: *acquirer*, *issuer*, *coupled*

Компонент	Acquirer processor	Issuer processor	Coupled processor
Коммутатор авторизации	приём от терминалов и шлюзов; маршрут запроса в сеть	запрос от сети к хосту; ответ обратно в сеть	on-us: напрямую, минуя сеть
Пул HSM	TAK, ZAK; PIN translation	IMK, ARQC verify, ARPC gen, key ceremony	объединённый пул: оба набора ключей
Клиринговый модуль	формирует исходящий: TC05/TC06 / IPM 1240 / НСПК	принимает входящий, матчит с авторизацией	on-us: сопоставление внутри одной системы
Расчётный модуль	своя нетто-позиция; проводки на корсчёт эквайера	своя нетто-позиция; проводки на корсчёт эмитента	on-us: внутренние взаимозачёты, без сети

37.1 Компоненты процессингового центра

Коммутатор авторизации

Коммутатор авторизации принимает каждое входящее сообщение ISO 8583 от эквайеров или от шлюзов, действующих от их имени, выбирает маршрут к эмитенту или в карточную сеть и возвращает ответ. Он работает в реальном времени, по одному сообщению: допустимая задержка измеряется десятками миллисекунд. [13, 46]

Таблица BIN задаёт маршрут внутри коммутатора: для каждого диапазона BIN в ней указан канал отправки запроса — VisaNet, Banknet, ОПКЦ НСПК или прямое подключение к эмитенту. Карточные сети регулярно публикуют изменения к таблице BIN, и процессинг обязан применять их в установленные сроки. Иначе часть транзакций будет отправлена по неверному маршруту и получит отказ не по вине клиента, ТСП или эквайера. [13, 15]

Коммутатор извлекает BIN (первые 6–8 цифр PAN из DE 2) и ищет совпадение в таблице BIN, определяя карточную сеть — Visa, Mastercard или Мир. Затем коммутатор проверяет, принадлежит ли BIN тому же банку, в котором работает процессинг. Такой случай называется *on-us*: сообщение маршрутизируется напрямую к авторизационному хосту эмитента, минуя сеть, а interchange не начисляется. Для *off-us* коммутатор выбирает исходящий канал (VisaNet, Banknet или ОПКЦ), форматирует сообщение по спецификации интерфейса (*Interface Specification*, IFS) конкретной сети и отправляет запрос. Различия между сетями проявляются в DE 25, DE 48 и в структуре подэлементов (*subelement layout*).

Во время маршрутизации коммутатор проверяет обязательные поля, формат MTI и корректность bitmap, дополняет запрос данными, требуемыми сетью, и ведёт журнал транзакций. Запись с точностью до миллисекунд используют для отладки и последующей сверки с клиринговыми файлами.

Когда внешний маршрут недоступен, включается резервная авторизация *stand-in* (механизм описан в разделе 5.1). Помимо сетевого *stand-in*, процессор эмитента может реализовать локальный *stand-in* по поручению эмитента, опираясь на собственные правила: лимит суммы, диапазон BIN, историю операций по карте. *Stand-in* ограничивают малыми суммами и заранее определёнными категориями транзакций, потому что одобрение проходит без онлайн-проверки баланса и лимитов. [13, 15]

Кредитный риск по операциям *stand-in* несёт эмитент при любом исполнителе. Visa возлагает на эмитента ответственность за все операции, одобренные или отклонённые STIP, Mastercard — за все операции, одобренные Stand-In Processing Service; параметры *stand-in* (лимиты суммы, списки BIN, ограничения MCC) эмитент задаёт не ниже значений сети по умолчанию [13, 46]. Если *stand-in* выполнял локальный процессор эмитента по его поручению, эмитент так же отвечает перед платёжной системой и держателем карты, а договор между эмитентом и процессором может предусматривать операционную ответственность процессора за превышение согласованных параметров *stand-in*. Параметры *stand-in* (максимальная сумма, разрешённые MCC, диапазоны BIN) задают предел этой операционной ответственности.

Пул HSM

Устройство HSM, иерархия ключей, церемония ключа (*key ceremony*) и базовые операции (проверка ARQC (*Authorization Request Cryptogram*), генерация ARPC (*Authorization Response Cryptogram*), перешифрование PIN-блока) разобраны в гл. 10.

Криптографические операции нельзя распределять по узлам так же свободно, как сервисы без состояния (*stateless*): ключевой материал загружается через регламентированные процедуры, и каждое новое устройство требует отдельной церемонии ключа. Процессинговые центры строят пул HSM с балансировкой нагрузки и заранее планируют его ёмкость. Производительность (число перешифрований PIN-блока, подписей RSA и проверок ARQC в секунду) зависит от модели, версии HSM и лицензированных функций. Её сверяют по документации производителя [200, 201, 734]. На российском рынке кроме зарубежных моделей Thales payShield, Utimaco и Atalla есть отдельный класс сертифицированных ФСБ России средств криптографической защиты информации (СКЗИ): от КриптоПро HSM до решений Аладдин Р.Д. и ИнфоТеКС [735]. Криптографию по ГОСТ выполняют только такие сертифицированные СКЗИ. HSM вносит в задержку единицы миллисекунд (см. бюджет ниже), но ёмкость пула наращивается медленнее, чем у коммутатора и сети.

ВАЖНО

Горизонтальное масштабирование пула HSM ограничено физически: ввод каждого нового устройства требует церемонии ключа (см. раздел 10.8). Планирование ёмкости учитывает текущую нагрузку и часы, необходимые на ввод устройства в эксплуатацию.

Сверка KCV (*Key Check Value*) между устройствами подтверждает, что все HSM пула работают с одним и тем же ключом, не раскрывая самого ключа. При отказе одного HSM ключевой материал сохраняется: он загружен во все устройства пула в одной церемонии ключа.

Клиринговый модуль

Клиринговый модуль, в отличие от авторизации, обрабатывает пакеты.

На стороне процессора эквайера модуль запускается по расписанию, собирает авторизованные транзакции за период и добавляет данные, появляющиеся только после авторизации: финальную сумму после добавления чаевых, результат адресной проверки, параметры конверсии DCC. Затем формирует исходящий клиринговый файл в формате сети: записи TC05 и TC06 (*transaction code*, Sales Draft и Credit — финансовое представление Visa в BASE II) для Visa, IPM (*Integrated Product Messages*, клиринговый формат Mastercard на MTI 1240) для Mastercard или профиль ISO 8583 с расширениями НСПК для внутрироссийских операций (доставка через систему электронного документооборота НСПК; см. раздел 31.7). [13, 46, 75, 736]

На стороне процессора эмитента модуль принимает входящие клиринговые файлы от сети и сопоставляет каждую запись с ранее одобренной авторизацией по коду авторизации, сетевому идентификатору транзакции (у Visa — Transaction Identifier), сумме и дате [13]. Совмещённый процессор видит обе стороны и сопоставляет свой исходящий клиринг со своим входящим внутри одной системы.

В любой конфигурации сопоставление вскрывает расхождения: *orphan authorization* (авторизация без клиринга), *late presentment* (поздний клиринг), *force post* (клиринг без авторизации), частичное подтверждение и *tip adjustment* — корректировка клиринговой суммы на величину чаевых, добавленных после авторизации. Любое такое расхождение создаёт риск прямых денежных потерь; клиринговый модуль

формирует отчёт об исключениях, который команда сопровождения разбирает по правилам сверки (см. раздел 31.1).

Расчётный модуль

Нетто-позиции считает оператор сети (VisaNet Settlement Service у Visa, GCMS и расчётная система S.A.M. у Mastercard, ОПКЦ НСПК для внутрироссийских операций) и рассылает каждому банку расчётные сообщения с его нетто-позицией и детализацией для сверки: interchange, комиссии сети, корректировки (chargeback, повторные представления, сборы).

Расчётный модуль процессора принимает эти сообщения и формирует по ним проводки во внутренней банковской системе. Для внутрироссийских транзакций расчёт проходит через НСПК и платёжную систему Банка России (см. раздел 1.3), для международных операций — через расчётные механизмы, предусмотренные правилами соответствующей сети. [5, 13, 14, 283] На расчётном этапе деньги уже движутся между банками, и любая ошибка в проводках превращается в прямой финансовый убыток.

37.2 Производительность и отказоустойчивость

Требования к задержке и доступности процессингового центра задаёт внешний контракт сети. Visa публикует предельное время ответа на авторизационный запрос и связывает просрочку ответа со включением *stand-in*; Mastercard в Transaction Processing Rules задаёт нормативы доли отказов авторизации по вине эмитента, включая таймауты. [13, 46]

Бюджет задержки

Карточные сети задают внешний предел времени ответа; универсальной внутренней таблицы «сколько миллисекунд должен занимать каждый сервис» они не дают. Внутренний бюджет сервисов процессор рассчитывает сам, оставляя запас на сетевой путь, обработку у эмитента и возврат ответа. Пример внутреннего бюджета: парсинг и валидация сообщения 1–3 мс, обращение к HSM (ARQC или перешифрование PIN-блока) 3–7 мс, поиск по BIN и маршрутизация 1 мс, логирование 1–2 мс, сериализация ответа 1 мс. Внутренняя обработка укладывается в 7–14 мс; остальной бюджет остаётся на сетевой путь до эмитента и обратно.

Резервирование площадок

Несколько минут недоступности процессингового центра превращаются в тысячи отклонённых транзакций и штрафы от карточных сетей. Схему резервирования (*active-active*, *active-standby* или гибридную) правила сетей оставляют на выбор оператора; в любом варианте он обязан выдерживать отказ площадки без потери управления трафиком.

Active-active предпочтительнее *active-standby* из-за времени запуска пассивной площадки. При переключении она переходит от холодного состояния к полной нагрузке: HSM загружает ключи, таблицы BIN синхронизируются, очереди восстанавливаются. Каждая секунда запуска — это новые отклонённые транзакции. В *active-active* оба узла работают под реальной нагрузкой, и при отказе одного трафик

перераспределяется без отдельного запуска резервной площадки. Взамен появляется риск *split-brain* при разрыве репликации. Авторизация не хранит состояния между запросами, и последствия кратковременного *split-brain* для неё ограничены. Клирингу и расчёту нужна более жёсткая гарантия согласованности: авторизационный след досверяется по внешним журналам сети, а потеря клиринговой или расчётной записи прямо отражается на движении денег.

Главная сложность — синхронизация состояния между центрами обработки данных (ЦОД). Журнал транзакций, таблицы BIN, лимиты для *stand-in* и ключи HSM должны оставаться согласованными в обоих центрах.

ПРАКТИКА

Шардинг по диапазонам BIN — простая и распространённая стратегия горизонтального масштабирования коммутатора авторизации. BIN однозначно определяет эмитента и карточную сеть, а значит, маршрут и набор ключей; транзакции с разными BIN не зависят друг от друга и могут обрабатываться разными экземплярами коммутатора без координации. При необходимости шард переносится на другой сервер или в другой ЦОД без влияния на остальные диапазоны BIN.

Аварийное восстановление

Георезервирование (размещение ЦОД в разных географических точках) защищает от региональных катастроф: пожара, наводнения, отключения электричества в районе. Чем дальше площадки друг от друга, тем лучше защита от локальных событий, но тем выше задержка синхронной репликации. Расстояние выбирают по сочетанию регионального риска, качества каналов связи и цены синхронной репликации.

RTO (*Recovery Time Objective*) — время восстановления после полного отказа ЦОД. Переключение трафика обязано происходить достаточно быстро, чтобы локальный сбой не превратился в массовый поток отказов. Парный показатель — RPO (*Recovery Point Objective*) — задаёт допустимую потерю данных: сколько последних транзакций может не оказаться на резервной площадке после переключения. Для авторизации, чей след досверяется по журналам сети, допустим больший RPO; для клиринговой и расчётной записи он стремится к нулю. Значения RTO и RPO задают архитектура и обязательства оператора.

37.3 Подключение к платёжным системам

VisaNet

Подключение к VisaNet, глобальной сети Visa, регулируют правила Visa и региональные эксплуатационные регламенты. В публичных документах Visa отдельно описаны использование VisaNet, требования к сетевым сертификатам и правила обработки транзакций. VisaNet разделяет онлайн-авторизацию в V.I.P. System (компонент BASE I) и пакетный клиринг в BASE II. [13]

Подключение включает канал связи и сертификацию под конкретный интерфейс сети. Публичные правила Visa оговаривают, что часть деталей, относящихся к безопасности сети и проприетарной внутренней обработке, исключена из публичной редакции. [13]

Banknet

Mastercard использует собственную сеть Banknet. Публичные материалы Mastercard описывают её как самостоятельную систему авторизации, клиринга и расчёта; Transaction Processing Rules задают сообщения *Authorization Request*/0100, *Financial Transaction Request*/0200, *First Presentment*/1240 и форматы IPM. [46, 283]

Mastercard поддерживает *single-* и *dual-message* сценарии; клиринговая часть опирается на IPM и GCMS (*Global Clearing Management System* — клиринговая система Mastercard). [46, 283]

ОПКЦ НСПК

Все внутрироссийские карточные транзакции проходят через НСПК — независимо от того, относится ли карта к ПС Мир или к международной сети, работающей внутри страны через локальную инфраструктуру. Банк России указывает, что внутрироссийская обработка операций международных платёжных систем ведётся через НСПК; сама НСПК публично описывает себя как оператора ПС Мир и ОПКЦ. [5, 17]

Чтобы работать во внутренней карточной инфраструктуре, банк подключается к ОПКЦ НСПК и соблюдает правила ПС Мир и связанные технические документы НСПК. [75]

СБП

СБП устроена иначе, чем карточный процессинг: это сервис платёжной системы Банка России с отдельным порядком подключения кредитных организаций, который публикует Банк России. НСПК выпускает материалы по сценариям оплаты по QR, кнопке и NFC (*Near Field Communication* — бесконтактная радиосвязь ближнего радиуса), а также по возвратам. [347, 348, 359]

Процессинг, который поддерживает и карты, и СБП, совмещает в одной инфраструктуре два разных протокола обмена. Карточная операция передаётся через ISO 8583: в *dual-message* сценарии авторизация выполняется в реальном времени, клиринг собирается отдельным пакетом, а сеть рассчитывает нетто-позиции; в *single-message* сценарии финансовое сообщение совмещает авторизацию и клиринг. СБП — одношаговый перевод средств между счетами в Банке России: одно сообщение в формате ISO 20022, валовый расчёт каждой операции на счетах в Банке России, без отдельного клирингового цикла. Одна платформа обработки поэтому поддерживает два набора форматов сообщений, таймаутов, схем сверки и расчётных моделей. [347, 359]

Перегрузка и управляемая деградация

Когда карточная сеть не отвечает, процессинговый центр ограничивает ожидание, иначе тысячи новых авторизаций быстро переполнят очередь. Защиту строят на таймаутах внешних вызовов и автоматическом размыкании канала при массовых сбоях; пороги зависят от реализации процессинга и обязательств перед сетями.

37.4 Лицензирование и сертификация

Требования Банка России

161-ФЗ разделяет роли операционного центра (ОЦ), платёжного клирингового центра (ПКЦ), расчётного центра (РЦ) и других операторов услуг платёжной инфраструктуры (ОУПИ); через эти роли описывается юридический статус процессингового центра. Банк России ведёт реестр операторов платёжных систем; перечень привлечённых ОУПИ ведёт оператор платёжной системы и указывает его в заявлении на регистрацию [1, 737].

Для самостоятельного ОУПИ базовый набор требований составляют 821-П, ГОСТ Р 57580.1-2017 с методикой оценки по ГОСТ Р 57580.2-2018 и Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» в части локализации персональных данных [63, 181, 205, 249]. Для процессингового центра в составе кредитной организации к ним добавляются 850-П с требованиями к операционной надёжности [531] и 851-П: оно задаёт требования к противодействию переводам без согласия клиента на стороне банка-эмитента [206]. Разбор приведён в разделе 25.2. Для платёжной системы Банка России, включая ОПКЦ СБП и ССНП (сервисы срочного и несрочного перевода платёжной системы Банка России), действует Положение Банка России от 25.07.2022 № 802-П «О защите информации в платёжной системе Банка России» [738].

Для участия в платёжной системе «Мир» процессинговый центр проходит сертификацию у НСПК как оператора ПС Мир [75]. Для участия в СБП требуется интеграция с ОПКЦ СБП на стороне НСПК [368]. Эти процедуры дополняют требования Банка России: сертификация даёт допуск к сети, регуляторные требования действуют независимо от неё.

Сертификация у карточных сетей

Каждая карточная сеть проводит собственную программу сертификации для процессинговых центров, подключающихся к её инфраструктуре. Публичные документы Visa и Mastercard задают условия участия в сети: правила использования VisaNet, требования к обработке транзакций, составу данных, клирингу и расчёту. [13, 15, 46]

Сертификация охватывает корректность форматов и обязательных элементов данных, криптографические процедуры и устойчивость к операционным сбоям. Ни Visa, ни Mastercard в открытых редакциях не раскрывают полную матрицу тестов, связанных с безопасностью. Приёмочные сценарии хранятся в закрытых руководствах и открываются участнику на этапе подключения. [13, 15]

PCI DSS

Процессинговый центр обрабатывает PAN и PIN-блок; процессор эмитента дополнительно проверяет ARQC и генерирует ARPC. Процессинг целиком попадает в среду данных держателя карты — CDE (*cardholder data environment*). PCI SSC (*Payment Card Industry Security Standards Council*) разделяет данные держателя карты (*cardholder data*) и чувствительные данные аутентификации — SAD (*sensitive authentication data*). Для PIN, PIN-блока и связанных процедур управления ключами действует самостоятельный стандарт PCI PIN Security. [64, 200, 238]

Требования к подтверждению соответствия зависят от роли и категории поставщика услуг в программе конкретного бренда; одной принадлежности к Level 1 недостаточно для выбора процедуры. Visa для поставщиков услуг Level 1 и процессоров с прямым подключением к VisaNet требует ROC (*Report on Compliance* — отчёт о соответствии), подготовленный QSA (*Qualified Security Assessor* — аккредитованный аудитор PCI DSS). Mastercard для регистрируемых поставщиков услуг требует ежегодного подтверждения соответствия PCI DSS, а для применимых категорий — ежеквартальных сканов ASV (*Approved Scanning Vendor* — одобренный поставщик внешнего сканирования уязвимостей). [739—741]

В CDE процессингового центра попадают коммутатор авторизации, пул HSM, клиринговый модуль, журнал транзакций и резервные копии — через них проходят PAN и SAD. Сетевая сегментация, токенизация PAN на входе шлюза и суррогатные идентификаторы в аналитических витринах сокращают число систем в аудите, но перечисленные компоненты остаются в CDE при любой сегментации. Разбор сегментации и состава аудита (*scoping*) — в разделе 12.2.

PCI PIN Security требует обмена ключами PIN-обработки в формате ключевого блока (*key block*: ANSI X9.143, исторически TR-31), запрещает обработку PIN в открытом виде вне HSM и задаёт церемонию ключа (см. раздел 10.8) [200]. Процессинговый центр в терминологии PCI DSS — поставщик услуг (*service provider*); Mastercard относит всех сторонних процессоров (*Third Party Processor*, TPP) к Level 1 безусловно, Visa — любого, кто хранит, обрабатывает или передаёт более 300 000 транзакций в год, а также всех процессоров с прямым подключением к VisaNet. Процессинг с таким объёмом или категорией валидируется как Level 1 через ROC. Анкета SAQ D *for Service Providers* доступна только провайдерам ниже порога объёма, не подпадающим под автоматическое отнесение к Level 1 по категории [244, 248, 739, 740].

Для российской финансовой организации PCI DSS действует параллельно с ГОСТ Р 57580.1: оба свода обязательны одновременно и оцениваются независимыми циклами (см. раздел 12.7).

Эпилог. Как отслеживать изменения

Устаревшее знание вредит: правильно спроектированная система, опираясь на прошлогодний пересказ бюллетеня, принимает решения, которые в текущей редакции правил уже неверны. Пока команда работает по такому пересказу, малое отклонение в источнике остаётся скрытым и оборачивается крупным сбоем в эксплуатации.

Очевидные причины ошибки: не нашли нужный документ или не отследили его обновление. Коварнее другая: команда нашла *пересказ* нужного документа на корпоративной вики и приняла его за сам документ. Отсюда задачи: быстро выйти на основной источник, отделить устойчивое от устаревающего и выстроить ритуал проверки изменений.

Где меняется

Когда в один и тот же месяц приходят бюллетень карточной сети, разъяснение PCI SSC и письмо регулятора, их легко сложить в одну папку с пометкой «изучить». Это ошибка: у изменений из разных областей разная цена пропуска. Пропустить одно — замечание на сертификации; пропустить другое — штраф сети и срочная переделка под фиксированный срок.

Правила участия вводят новые обязанности банков, пороги мониторинговых программ, ограничения на повторы, пересматривают логику диспутов. Протокол меняется новыми полями, новой версией 3DS, изменённым соответствием полей в сообщениях, требованиями к токенам или к ядру терминала. Комплаенс добавляет контрольные меры, даты прекращения прежних редакций требований, уточняет область применения. Регулирование определяет допустимость продукта: вступает в силу закон, положение или разъяснение регулятора.

Признак области изменения — то, как оно проявится, если его пропустить. Протокольная правка проявляется как падение доли одобрений или сбой приёма карт: быстро, заметно, наблюдаемо. Изменение в комплаенсе проявляется во время аудита: медленно, но с уже накопленным ущербом. Регуляторная перемена проявляется как вопрос о допустимости работы в таком виде: редко, но с последствиями, способными остановить бизнес целиком.

Что читать заранее

У главных документов платёжной отрасли обязательность редко появляется внезапно: зрелый процесс публикации даёт участникам время на адаптацию.

Банк России ведёт основной раздел платёжной системы — `cbr.ru/PSystem/` — где сгруппированы нормативные акты, методические рекомендации и информационные письма по НСПК, СБП, цифровому рублю и доступу оператора [5]. Проекты нормативных актов выходят в отдельном разделе публичного обсуждения с указанными сроками для замечаний ещё до принятия документа [742].

НСПК публикует основной текст правил «Платёжная система „Мир“» (на момент издания книги — редакция 4.3 от 02.12.2025) с указанной датой вступления в силу [75, 169]; рядом, на `nspk.ru/banks/guides/`, — тарифные документы, методические руководства для банков и стандарты ПС Мир (в частности, требования к системе

управления рисками информационной безопасности). Для СБП на том же портале выложены «Правила оказания операционных услуг и услуг платёжного клиринга в СБП», опубликованные оператором — ОПКЦ НСПК; публичная часть OpenAPI ОПКЦ СБП доступна на `sbp.nspk.ru/api` [359, 364]. Интерфейсные спецификации (полная семантика полей ISO 8583 в редакции НСПК, коды расширений, процедуры подключения, сертификационные материалы) остаются закрытой частью документации, выдаваемой ОПКЦ через портал поддержки участникам и банкам-кандидатам.

PCI SSC и EMVCo полезны там, где вопрос касается мер контроля PCI или поведения чипа, токена и 3DS: новые версии стандартов выходят с заранее указанной датой обязательности и отдельными бюллетенями [70, 188, 217, 743].

У каждой организации рядом с открытым текстом правил и стандартов есть закрытая интеграционная документация (детальные спецификации, сертификационные материалы, бюллетени для участников — например, Mastercard Chip Information Center на портале Connect) [744]; пересказ подменяет первоисточник именно в этой закрытой части.

Регулярное чтение бюллетеней занимает немного времени и перехватывает дорогое изменение до того, как оно превратится в инцидент.

Самая неприятная ситуация — когда публичный материал только обозначает изменение, а полный текст требования закрыт. Достраивать реализацию по пересказам — ошибка, которая оплачивается переделкой на внедрении или сертификации. Сначала — факт изменения и дата вступления в силу; затем — основной документ через участника системы, эквайера или процессингового партнёра; после этого — проектирование решения.

Как превращать новое правило в задачу

Новый документ становится полезен, когда команда превратила его в задачу, ответив на вопросы:

- К какой области относится изменение: правила участия, протокол, комплаенс или регулирование?
- Какие роли и системы оно затрагивает: эмитента, эквайера, шлюз, службу управления рисками, сверку, юристов?
- Нужна ли правка кода, процесса, документации или пока достаточно мониторинга?
- Каков крайний срок внедрения и чем грозит его пропуск?
- Кто из команды несёт последствия пропуска — тот же, кто отвечает за внедрение, или другой человек?

Последний вопрос — ключевой и чаще всего пропускаемый. Если последствия пропуска несёт одна команда, а внедрение поручено другой, исполнитель не отвечает за последствия, и задача регулярно отступает перед более громкими. Бюллетень читает тот, кто платит штраф; иначе вся схема становится театром ответственности.

ПРАКТИКА

Полезен короткий формат разбора изменения: источник, основной документ, дата вступления в силу, затронутые системы, требуемое действие, ответственный с последствиями и ссылка на внутреннюю задачу. Такая запись переживает почту и чаты лучше длинного конспекта.

Что оставлять в книге, а что сверять заново

Книга не должна претендовать на вечную актуальность там, где отрасль обновляется короткими циклами. По сроку жизни материал делится на длинный и короткий.

Длинный — это инварианты: архитектурные связи, роли участников, логика протоколов, причины существования клиринга в его текущей форме. Чем дольше эти вещи прожили без изменений, тем дольше проживут ещё. Их место — в книге.

Короткий — это пороги, даты, тарифы, версии, доли: каждое такое значение заменяет следующая публикация. Сюда относятся, например:

- актуальные пороги мониторинговых программ карточных сетей;
- ограничения на повторы и даты вступления требований в силу;
- актуальные доли методов оплаты и сравнительные таблицы;
- тарифы, пороги и даты, зависящие от конкретного выпуска правил;
- полные таблицы кодов ответа (*response codes*) и кодов причин (*reason codes*).

Решение — разнесение по краям: на одном конце максимально устойчивые инварианты в книге, на другом — максимально живые таблицы и бюллетени по прямой ссылке. Середина — «полу-актуальная вики, которую обновляли в прошлом квартале» — хуже обоих концов: она содержит ошибки и создаёт иллюзию точности. От середины лучше отказываться открыто, а не пытаться «поддерживать актуальность» героическими усилиями.

Расписание сверок

Отслеживание изменений работает как ритуал; авральная реакция на инцидент даёт худший результат. Команда, привыкшая к мелким регулярным сверкам, проходит большое изменение спокойно; команда, ждущая «когда надо будет, тогда и разберёмся», ломается на первом серьёзном.

Раз в неделю полезно просматривать входящие бюллетени, регуляторные новости и обновления PCI SSC и EMVCo. Ежемесячно — разбирать новые документы по схеме из этой главы и обновлять карту рисков. Ежеквартально — пересматривать справочные таблицы и решать, что в книге устарело, что следует убрать или переписать в следующей редакции и какие места стоит жёстче привязать к первоисточнику. Перед крупным релизом — перечитывать основные документы по тем областям, которых релиз касается.

Карта первоисточников

Когда в платёжной команде звучит фраза «надо проверить в правилах», спор часто разгорается вокруг источника истины. Один человек открывает свод правил сети, другой ищет ответ в технической спецификации, третий пересказывает заметку поставщика. Одну и ту же тему описывают публичные правила для участников, технические спецификации и закрытые оперативные уведомления.

Отсюда первая задача навигации: прежде чем читать, понять, какой документ в этой теме главный, а какой — только комментарий, пересказ или вспомогательный портал интеграции.

EMVCo

EMVCo нужен там, где спор идёт не о договорных обязанностях, а о поведении платёжной техники. Если вопрос звучит как «что именно должны сделать терминал, карта, токен или мобильный кошелёк», ответ ищут здесь.

Если речь идёт о контактной транзакции EMV, точкой входа остаются EMV Chip Specifications, Books 1–4 [86] (см. гл. 7). Для бесконтактной оплаты нужен корпус EMV Contactless Specifications [160], в котором описаны NFC и логика бесконтактного ядра (см. гл. 8). Токенизацию описывает EMV Payment Tokenisation Specification [35]: роли TSP, ограничения домена токена и его жизненный цикл (см. гл. 9). Для 3DS основной документ — EMV 3-D Secure Protocol and Core Functions Specification [659]: сообщения AReq/ARes, сценарий *challenge* и общая логика протокола (см. гл. 11).

EMVCo тяжелее всего читать подряд. Здесь выгоднее идти от вопроса к разделу. Если нужно понять жизненный цикл контактной операции, полезнее всего Book 3. Если важно поведение терминала, кассира и интерфейса приёма, открывают Book 4. Если вопрос относится к бесконтактному входу в транзакцию, нужен соответствующий том Contactless.

PCI SSC

Стандарты PCI нужны, когда команда спорит о периметре PCI и наборе обязательных контролей. Как уложиться в SAQ A, как контролировать JavaScript на странице оплаты, как защищать PIN block и где размещать точку дешифрования: на все эти вопросы отвечают документы PCI.

По периметру PCI и базовому набору контролей нужен PCI DSS [70] (см. гл. 12). Для разных моделей интеграции существуют сокращённые типы оценки SAQ [244]. Работу с PIN и HSM регулирует PCI PIN Security Requirements [200]. Когда вопрос упирается в шифрование от терминала до точки дешифрования, открывают PCI P2PE [239].

Порядок чтения здесь такой: сначала определить периметр PCI, потом понять, какой путь оценки применим, и затем разбирать отдельные требования. Ошибка в определении периметра обычно обходится дороже, чем неверное чтение одного подпункта.

НСПК, Мир и СБП

НСПК нужна там, где вопрос касается правил, порядка работы или формата сообщения внутри РФ — для платёжной системы «Мир», СБП или внутрироссийского процессинга карт. Здесь полезно заранее определить, ищете вы правовое поле, продуктовую модель или конкретный формат сообщения.

Правила платёжной системы «Мир» задают роли и обязанности участников [75, 169]; на момент издания книги действует редакция 4.3, в силе с 03.12.2025. Вокруг них на портале для банков `nspk.ru/banks/guides/` опубликован набор документов: Стандарты ПС Мир доопределяют требования к системе управления рисками информационной безопасности и к использованию карт в нефинансовых сервисах; тарифная политика и методические руководства описывают регуляторные и операционные вопросы участия, а лист самооценки SAQ D-MIR опубликован рядом с правилами [75]. Спецификация бесконтактных платежей «Мир» описывает приём.

Документы по СБП опубликованы на том же портале и на `sbp.nspk.ru`. Правила оказания операционных услуг и услуг платёжного клиринга в СБП задают работу оператора — ОПКЦ НСПК (операционного и платёжного клирингового центра) [359]; публичная часть OpenAPI ОПКЦ СБП выложена на `sbp.nspk.ru/api` [364]; подключение регулируют документы Банка России [347].

ОПКЦ НСПК — функциональная роль внутри НСПК: маршрутизация и клиринг для «Мир» и для СБП, исторически также внутрироссийская обработка операций международных платёжных систем. ОПКЦ предоставляет участникам полные интерфейсные спецификации (форматы сообщений в редакции НСПК, коды расширений), процедуры подключения и сертификационные материалы через закрытый портал поддержки. Программное обеспечение НСПК (мобильные решения и терминальные технологии) описано в открытом разделе [37].

Если вопрос касается роли участника, продуктовой схемы или общей модели работы «Мир» либо СБП, обычно хватает публичных правил и стандартов. Если же спор упирается в формат сообщения, сертификацию или детали внутрироссийского процессинга, понадобится закрытая документация ОПКЦ, доступная через участника системы или процессингового партнёра.

Банк России

Документы Банка России нужны, когда требуется понять пределы допустимого поведения. Если вопрос звучит как «обязаны ли мы», «имеем ли мы право» или «какой статус нужен», переходить следует к нормативным актам ЦБ и федеральным законам.

Основной публичный раздел — `cbr.ru/PSystem/` — собирает вместе нормативные акты, методические рекомендации, информационные письма, реестры и справочные материалы по национальной платёжной системе: разделы «Платёжная система Банка России», «Основные документы», «Стандарт ISO 20022», «Система передачи финансовых сообщений», «Система быстрых платежей», «Надзор и наблюдение», «Доступ оператора платёжной системы» [5]. Проекты нормативных актов выходят в отдельном разделе публичного обсуждения `cbr.ru/project_na/` с указанными сроками для замечаний до принятия документа [742].

161-ФЗ задаёт базовые роли платёжного рынка [1]. 762-П описывает правила перевода денежных средств [532]. 821-П задаёт защиту информации при переводах денежных средств, 850-П — операционную надёжность кредитных организаций, 851-П — противодействие переводам без согласия клиента; все три отсылают

к 57580.1 в части состава мер и к 57580.2 в части оценки соответствия [205, 206, 531]. 266-П задаёт карточную специфику [538]; на смену готовится новый акт Банка России — проект Положения «О порядке предоставления электронных средств платежа и осуществления операций с их использованием» (последняя публичная редакция — от 28 октября 2024 года; на момент написания этих строк в силу не вступил). Для цифрового рубля отправная точка — 340-ФЗ [4]; 248-ФЗ [361] задаёт поэтапные обязанности банков и ТСП, а требования к защите информации для участников платформы установлены 833-П [500]. Для СБП и других специальных тем набор документов свой.

Помимо нормативных актов, ЦБ выпускает методические рекомендации (серии МР) и информационные письма — они не задают обязанности, но фиксируют позицию регулятора по спорным вопросам. В ежедневной работе их полезно отслеживать вместе с основными актами: интерпретация часто появляется раньше, чем формальное изменение акта.

Нормативные акты полезно читать связкой: закон задаёт роли и пределы модели, положение описывает порядок исполнения, письма и разъяснения показывают регуляторскую интерпретацию спорных мест. Для практической работы удобнее пользоваться правовыми системами, где доступны история изменений и перекрёстные ссылки.

ISO

ISO нужен, когда требуется обобщённый язык, более широкий, чем диалект конкретной сети. Для прикладной задачи читают сначала сетевой диалект, потом ISO как общую модель; для архитектурной или межсистемной (новый обмен) сразу берут ISO 20022 как исходную модель.

ISO 8583 остаётся базовым стандартом структуры финансовых сообщений [74]; его конкретизируют сетевые реализации. ISO 20022 [436] задаёт современную модель финансовых сообщений и особенно важен для международных систем, SWIFT MX и многих систем мгновенных платежей (см. раздел 36.6). ISO 4217 [84], ISO 3166-1 [322] и ISO 9564-1 [215] задают базовые коды валют, коды стран и форматы PIN block.

Глоссарий

A2A Account-to-Account, перевод со счёта на счёт без участия карточной сети; общий случай account-based-модели платежа в противоположность card-based-операциям карточных сетей

AAC Application Authentication Cryptogram, криптограмма отказа в EMV

ABA American Bankers Association, формат Track 2 магнитной полосы

ABU Automatic Billing Updater, сервис Mastercard автоматического обновления реквизитов карт у мерчантов; аналог Visa Account Updater (см. VAU)

AC Application Cryptogram, криптограмма EMV-операции (одна из ARQC, TC, AAC); синонимы: EMV-криптограмма

ACH Automated Clearing House, расчётная сеть пакетных межбанковских переводов в США

ACS Access Control Server, компонент эмитента в 3-D Secure, проводящий аутентификацию держателя; синонимы: сервер аутентификации эмитента

ADF Application Definition File, файл платёжного приложения на чипе карты (EMV); адресуется через AID

AES Advanced Encryption Standard, симметричный блочный шифр (FIPS 197)

AFL Application File Locator, описывает расположение записей EMV-приложения на чипе

AFT Account Funding Transaction, операция загрузки средств на счёт через карточную сеть (Visa Direct/Money Movement); синонимы: загрузка средств на счёт

AID Application Identifier, идентификатор платёжного приложения на чипе карты (EMV); синонимы: идентификатор приложения

AIP Application Interchange Profile, битовое поле, описывающее возможности EMV-приложения

AIS Account Information Security, программа Visa, предшественница PCI DSS

AISP Account Information Service Provider, поставщик услуг информирования о счёте (PSD2)

AML Anti-Money Laundering; русский канон функции — финмониторинг

ANSI American National Standards Institute, американский институт национальных стандартов

AOC Attestation of Compliance, аттестат соответствия PCI DSS

AOV Average Order Value, средний чек заказа

APDU Application Protocol Data Unit, единица обмена данными между терминалом и чипом (ISO/IEC 7816-4)

API Application Programming Interface, программный интерфейс взаимодействия систем

APID Application Program Identifier, объект EMV (тег `0x9F5A`) в бесконтактных профилях Visa; кодирует регион программы и служит ключом выбора набора лимитов в DRL

Apple ECP Enhanced Contactless Polling, проприетарное расширение Apple над ISO/IEC 14443-A для считывателей NFC (используется в Apple Pay, Apple VAS, Apple Wallet Access)

ARC Authorisation Response Code, двухбайтовый код ответа эмитента в EMV; входит в MAC при расчёте ARPC

ARCA Armenian Card, армянская национальная платёжная система

ARN Acquirer Reference Number, эквайринговый идентификатор операции, используемый в клиринге и спорах

ARPC Authorisation Response Cryptogram, ответная криптограмма эмитента (EMV online auth); синонимы: Authorization Response Cryptogram

ARQC Authorisation Request Cryptogram, запросная криптограмма карты (EMV online auth); синонимы: Authorization Request Cryptogram

ASK Amplitude Shift Keying, амплитудно-манипулированная модуляция в ISO/IEC 14443 Type A; синонимы: Amplitude-Shift Keying, амплитудная манипуляция

ASPSP Account Servicing Payment Service Provider, банк, обслуживающий счёт клиента в открытом банкинге PSD2; синонимы: ПУ, поставщик услуг, банк обслуживающий счёт

ASV Approved Scanning Vendor, аккредитованный PCI SSC внешний сканировщик уязвимостей

ATC Application Transaction Counter, счётчик операций EMV-приложения

ATM Automated Teller Machine, банкомат

ATO Account Takeover, захват учётной записи

ATQA Answer To Request, Type A, ответ карты на WUPA/REQA в ISO/IEC 14443-3 Type A

ATS Answer To Select, ответ карты на RATS в ISO/IEC 14443-4 с параметрами кадра (FWI, FSCI и др.)

AUC Area Under Curve, площадь под ROC- или PR-кривой; метрика классификатора; синонимы: площадь под PR

AVS Address Verification Service, проверка адреса держателя у эмитента в операциях CNP; синонимы: Address Verification System, сверка адреса

BCB Banco Central do Brasil, Центральный банк Бразилии (регулятор PIX)
BCD Binary Coded Decimal, двоично-десятичное кодирование (ISO 8583, EMV)
BDK Base Derivation Key, базовый ключ деривации в DUKPT
BER Basic Encoding Rules, бинарная нотация ASN.1 (ITU-T X.690); основа кодирования BER-TLV в EMV
BIN Bank Identification Number, первые цифры PAN, идентифицирующие эмитента (см. также IIN); синонимы: Issuer Identification Number, банковский идентификационный номер
BIS Bank for International Settlements, Банк международных расчётов
BLE Bluetooth Low Energy, маломощный Bluetooth для платежей и смежных задач
BNPL Buy Now Pay Later, рассрочка/отложенная оплата как платёжный метод; синонимы: buy-now-pay-later
BRAM Business Risk Assessment and Mitigation, программа Mastercard по оценке рисков мерчанта
C2B Customer-to-Business, перевод от физлица в пользу бизнеса
C2C Customer-to-Customer, перевод между физическими лицами
CA Certificate Authority, удостоверяющий центр; в платежах — корень доверия сертификатов EMV карт и PKI для удалённой инъекции ключей; синонимы: Certification Authority
CAVV Cardholder Authentication Verification Value, криптографический результат 3-D Secure-аутентификации (Visa); синонимы: криптограмма 3DS Visa
CBC Cipher Block Chaining, режим сцепления блоков для блочных шифров; синонимы: сцепление блоков
CBDC Central Bank Digital Currency, цифровая валюта центрального банка (например, цифровой рубль); синонимы: цифровая валюта ЦБ
CBPII Card-Based Payment Instrument Issuer, регистрируемая роль эмитента карточного инструмента (PSD2)
CBPR Cross-Border Payments and Reporting Plus, миграционная программа SWIFT на ISO 20022
CDA Combined Dynamic Data Authentication / AC Generation, метод офлайн-аутентификации данных карты с динамической подписью операции (EMV)
CDCVM Consumer Device Cardholder Verification Method, верификация держателя средствами устройства (биометрия, PIN-код экрана); синонимы: Consumer Device CVM, верификация на устройстве
CDE Cardholder Data Environment, периметр окружения данных держателя по PCI DSS
CDOL1 Card Risk Management Data Object List 1, список тегов EMV, которые карта ожидает в первой команде GENERATE AC (CDOL2 — для второй)
CE Compelling Evidence, набор доказательств, позволяющий эквайеру отбить часть споров (Visa CE 3.0, MC compelling evidence)
CHD Cardholder Data, данные держателя карты в терминах PCI DSS
CIBA Client-Initiated Backchannel Authentication, протокол отделённой аутентификации (OpenID Foundation)
CID Cryptogram Information Data, тег EMV (`0x9F27`) с типом криптограммы (ARQC/TC/AAC) и решением карты
CIPS Cross-Border Interbank Payment System, китайская система международных межбанковских переводов в юанях
CISP Cardholder Information Security Program, программа Visa, предшественница PCI DSS
CIT Customer-Initiated Transaction, операция, инициированная держателем карты; синонимы: операция инициированная клиентом
CMAC Cipher-based Message Authentication Code, MAC на блочном шифре (NIST SP 800-38B)
CMS Card Management System, система управления жизненным циклом карт у эмитента; синонимы: система управления картой
CNP Card-Not-Present, операция без физического предъявления карты; синонимы: без предъявления карты, не предъявление карты, дистанционная операция, card-absent
CPM Customer-Presented Mode, QR-сценарий с предъявлением кода клиентом
CPS Custom Payment Service, программа квалификации операций Visa с льготным interchange (CPS/Retail и др.)
CUP China UnionPay, китайская карточная сеть
CVC1 Card Verification Code 1, статический код подлинности на магнитной полосе; синонимы: CVV, Card Verification Value
CVC3 Card Verification Code 3, динамический код Mastercard для contactless mag-stripe (PayPass M/Stripe); синонимы: dCVV, dynamic CVV, динамический CVV
CVM Cardholder Verification Method, метод верификации держателя (PIN, signature, CDCVM, no CVM)
CVR Card Verification Results, бит-маска внутри IAD с результатами проверок карты по операции
CVV/CVC Card Verification Value (Visa) / Card Verification Code (Mastercard), статический код подлинности карты на магнитной полосе

CVV2/-CVC2 Печатный код безопасности на оборотной стороне карты, используется в операциях CNP; синонимы: CVV2, CVC2

DCC Dynamic Currency Conversion, конверсия в валюту держателя на стороне эквайера/терминала; синонимы: динамическая конвертация валюты

DICT Diretório de Identificadores de Contas Transacionais, директория Banco Central do Brasil, сопоставляющая ключам Pix (телефон, e-mail, CPF, CNPJ, EVP) реквизиты счёта и участника

DDA Dynamic Data Authentication, метод офлайн-аутентификации с динамической подписью данных карты (EMV)

DE Data Element, поле сообщения ISO 8583; синонимы: элемент данных, data elements

DLT Distributed Ledger Technology, технология распределённых реестров; база данных с синхронизированными копиями у нескольких участников; синонимы: распределённый реестр

DMS Dual Message System, двухстадийная авторизация и клиринг отдельным сообщением (см. также SMS); синонимы: dual-message, двухсообщенный, двухстадийный клиринг, двухстадийная схема

DPAN Device Primary Account Number, токенизированный номер, привязанный к устройству (Apple Pay, Google Pay и др.); синонимы: Device PAN, токен устройства, device token, токен-номер

DRL Dynamic Reader Limit, механизм бесконтактных ридеров Visa и AmEx, позволяющий держать несколько наборов лимитов на один AID в зависимости от региональной принадлежности карты (см. APID); синонимы: Dynamic Reader Limits

DS Directory Server, маршрутизатор сообщений 3-D Secure от мерчанта к ACS эмитента; синонимы: сервер маршрутизации 3DS

DSRP Digital Secure Remote Payment, механизм Mastercard генерации криптограмм в CNP; синонимы: Digital Secure Remote Payments

DUKPT Derived Unique Key Per Transaction, схема производных одноразовых ключей для PIN/данных в POS

EAS Extended Authorization Service, продление окна авторизации Visa до представления операции к расчёту (до 30 дней); не путать с Estimated Authorization (авторизация на оценочную сумму)

EBA European Banking Authority, Европейская банковская администрация; синонимы: Европейская банковская служба

EBCDIC Extended Binary Coded Decimal Interchange Code, кодировка IBM, исторически используется в ISO 8583

ECC Elliptic Curve Cryptography, криптография на эллиптических кривых; синонимы: эллиптическая криптография

ECDSA Elliptic Curve Digital Signature Algorithm, алгоритм цифровой подписи на эллиптических кривых

ECI Electronic Commerce Indicator, индикатор результата 3-D Secure в авторизационном сообщении; синонимы: индикатор электронной коммерции, индикатор уровня аутентификации

ECM Excessive Chargeback Merchant, статус мониторинговой программы Mastercard для ТСП с повышенной долей chargeback

ECR Electronic Cash Register, кассовая программа, обменивающаяся данными с POS-терминалом по отдельному интерфейсному протоколу (nexo Retailer Protocol или проприетарный формат вендора)

EEA European Economic Area, Европейская экономическая зона

EFA EMV Final Advice, индустриальное название второй POS-to-host-сессии (ISO 8583 MTI 0220/0230), в которой терминал передаёт ПЦ результат обработки картой ARPC и финальную криптограмму; в спецификациях EMVCo тот же шаг обозначается как online completion / second GENERATE AC

EFM Excessive Fraud Merchant, статус мониторинговой программы Mastercard по фроду

EIRF Electronic Interchange Reimbursement Fee, штрафная категория interchange Visa для операций без полного набора данных

ELCARD Кыргызская национальная платёжная система (см. также ЭЛКАРТ)

EMV Europay/Mastercard/Visa, семейство спецификаций чиповых карт (EMVCo); синонимы: Europay/Mastercard/Visa, EMVCo спецификации, чиповый стандарт

EP E-commerce Page, тип SAQ A-EP в PCI DSS для платёжных страниц с прямой отправкой данных карты

FAPI Financial-grade API, профиль безопасности OpenID Foundation для финансовых API (см. также ФАПИ)

FATF Financial Action Task Force, межправительственная организация по борьбе с отмыванием денег и финансированием терроризма; синонимы: ФАТФ

FBO Fulfillment by Operator, маркетплейсная схема с логистикой на стороне оператора

FBS Fulfillment by Seller, маркетплейсная схема с логистикой на стороне продавца

FCA Financial Conduct Authority, регулятор финансовых услуг Великобритании

FCI File Control Information, ответ карты на SELECT (PPSE/PSE/ADF) с метаданными приложения; содержит, в частности, PDOL

FedNow Мгновенная розничная платёжная система Federal Reserve Banks, запущена 20 июля 2023 года; регулируется 12 CFR 210 Subpart C и Operating Circular 8, расчёт через master account участника в Reserve Bank; синонимы: Federal Reserve FedNow Service

FEP Front-End Processor, сетевой шлюз эквайера, принимающий сообщения от терминалов, разбирающий ISO 8583 и маршрутизирующий по BIN

FF1 Format-Preserving Encryption Algorithm 1, режим сохраняющего формат шифрования (NIST SP 800-38G)

FF3 Format-Preserving Encryption Algorithm 3, режим FPE (NIST SP 800-38G, 2016); исключён в черновике Rev. 1 вместе с вариантом FF3-1 из-за уязвимости в tweak schedule; действует только FF1

FIN SWIFT FIN, исторический сервис передачи MT-сообщений

FIPS Federal Information Processing Standards, серия стандартов NIST (FIPS 140-3, FIPS 197 и др.)

FIS Fidelity National Information Services, крупный американский процессор

Floor limit терминальный порог офлайн-одобрения по сумме операции; задаётся эквайером по правилам сети (EMV terminal risk management); синонимы: лимит офлайн-одобрения

FPAN Funding Primary Account Number, реальный номер карты, которому соответствует токен; синонимы: Funding PAN

FPE Format-Preserving Encryption, шифрование с сохранением формата (например, длины и алфавита PAN)

FWI Frame Waiting Integer, поле в ATS, из которого выводится максимальное FWT в ISO/IEC 14443-4

FWT Frame Waiting Time, максимальное время ожидания ответа карты в ISO/IEC 14443

GCMS Global Clearing Management System, клиринговая система Mastercard

GPO Get Processing Options, EMV-команда инициации транзакции

HCE Host Card Emulation, эмуляция карты в ОС устройства без аппаратного Secure Element; синонимы: программная эмуляция карты

HECM High Excessive Chargeback Merchant, повышенный уровень программы Mastercard по chargeback

HMAC Hash-based Message Authentication Code, MAC на хеш-функции (RFC 2104)

HPP Hosted Payment Page, размещённая платёжная страница на стороне PSP

HSM Hardware Security Module, аппаратный модуль для хранения ключей и криптоопераций; синонимы: аппаратный криптомодуль, криптомодуль, аппаратный модуль безопасности

HUMO Узбекская национальная платёжная система; синонимы: NIPC Узбекистан

IAC Issuer Action Codes, заданные эмитентом правила решения по EMV-операции; синонимы: коды действий эмитента

IAD Issuer Application Data, тег EMV (`0x9F10`) с данными эмитента (включает CVR и производные ключевые поля), передаётся картой в составе ответа на GENERATE AC

IANA Internet Assigned Numbers Authority, реестр идентификаторов Интернета (порты, MIME, JOSE-алгоритмы)

IATA International Air Transport Association, формат Track 1 магнитной полосы

ICC Integrated Circuit Card, чиповая карта (EMV)

iCVV Integrated Circuit Card Verification Value, статический код верификации в чипе; при расчёте используется сервисный код `999`; синонимы: Chip CVC

IFR Interchange Fee Regulation, регламент ЕС 2015/751 о межбанковских комиссиях; синонимы: регламент ЕС о межбанковских комиссиях

IFS Interface Specification, документ карточной сети, описывающий формат и семантику ISO 8583-сообщений конкретного интерфейса

IIN Issuer Identification Number, термин ISO, эквивалент BIN; синонимы: Bank Identification Number, банковский идентификационный номер

IK Initial Key, начальный ключ устройства в DUKPT

IKI Initial Key Identifier, идентификатор начального ключа DUKPT

IMK Issuer Master Key, мастер-ключ эмитента, из которого выводятся ключи EMV-приложения карты

IPC Interbank Processing Center, межбанковский процессинговый центр Кыргызстана

IPR Instant Payments Regulation, Regulation (EU) 2024/886 о мгновенных кредитовых переводах в евро; обязательность SCT Inst в еврозоне с 9 октября 2025 года; синонимы: Regulation 2024/886

IPK Issuer Public Key, открытый ключ эмитента в EMV PKI-иерархии (тег `0x90`), подписан корневым CA платёжной сети

IPM Integrated Product Messages, формат клиринговых сообщений Mastercard

IRF Interchange Reimbursement Fee, межбанковская комиссия (термин UnionPay); синонимы: interchange fee

ISO International Organization for Standardization, в книге встречается в обозначениях стандартов 4217, 7810, 7813, 7816, 8583, 20022; синонимы: Independent Sales Organization

JARM JWT Secured Authorization Response Mode, подписанный ответ авторизационного эндпоинта (FAPI)

JCB Japan Credit Bureau, японская карточная сеть

JSON JavaScript Object Notation, формат обмена данными в REST/HTTP-интерфейсах

JWE JSON Web Encryption (RFC 7516)

JWK JSON Web Key (RFC 7517)

JWS JSON Web Signature (RFC 7515)

JWT JSON Web Token (RFC 7519)

KCV Key Check Value, контрольная сумма ключа, по которой проверяют, что копии ключа на разных устройствах совпадают

KEK Key Encryption Key, ключ шифрования ключей; используется для защищённой передачи и хранения других ключей

KYB Know Your Business, идентификация юридических лиц при подключении; синонимы: идентификация юридического лица, идентификация ТСП

KYC Know Your Customer, идентификация и верификация клиента-физлица; синонимы: знай своего клиента, идентификация клиента

LLVAR Length-Length Variable, поле переменной длины с двухсимвольным префиксом длины (ISO 8583)

LMK Local Master Key, локальный мастер-ключ HSM; защищает производные ключи внутри устройства

MAC Message Authentication Code, код аутентичности сообщения; синонимы: код аутентификации сообщения

MC ECP Excessive Chargeback Program, программа Mastercard по мониторингу chargeback у эквайеров и ТСП

MCC Merchant Category Code, четырёхзначный код категории мерчанта (ISO 18245); синонимы: код категории ТСП, категория ТСП, категория мерчанта

MDB Mir Debit Business, продуктовый код дебетовой карты Мир для бизнеса

MDES Mastercard Digital Enablement Service, токенизационный сервис Mastercard

MDP Mir Debit Prepaid, продуктовый код предоплаченной карты Мир

MDR Merchant Discount Rate, торговая уступка мерчанта; синоним MSC; также: Merchant Service Charge, ставка торговой уступки

MDT Mir Debit, продуктовый код стандартной дебетовой карты Мир

MED Mecanismo Especial de Devolução, возврат по антифроду Pix; банк-отправитель инициирует через инфраструктуру схемы запрос на блокировку и возврат при подозрении на фрод

Me2Me Pull Сценарий протокола C2C, инициируемый банком-получателем: клиент «стягивает» средства со своего счёта в банке-отправителе, где и даёт согласие на списание; синонимы: Me2Me-Pull

Me2Me Push Сценарий протокола C2C: перевод самому себе по номеру телефона по инициативе отправителя — из приложения банка-отправителя на свой счёт в банке-получателе; синонимы: Me2Me-Push

MID Merchant ID, идентификатор ТСП у эквайера; синонимы: номер ТСП

MIP Mastercard Interface Processor, шлюз сети Mastercard на стороне эквайера или эмитента; терминирует авторизационный протокол к международному коммутатору

MIT Merchant-Initiated Transaction, операция, инициированная мерчантом без участия держателя в момент списания; синонимы: операция инициированная мерчантом

MPA MIR Payment Application, EMV-апплет карты системы Мир с поддержкой контактного и бесконтактного интерфейсов и криптографии ГОСТ

MPM Merchant-Presented Mode, QR-сценарий с предъявлением кода продавцом

MSC Merchant Service Charge, торговая уступка, комиссия мерчанта эквайеру; синонимы: MDR, Merchant Discount Rate, ставка торговой уступки

MT Message Type, формат текстовых сообщений SWIFT (MT103, MT202 и др.); синонимы: SWIFT MT, Message Type SWIFT

MTI Message Type Indicator, четырёхзначный идентификатор типа сообщения ISO 8583; синонимы: тип сообщения ISO 8583

NFC Near Field Communication, ближнепольная радиосвязь для бесконтактных платежей

NIST National Institute of Standards and Technology, американский институт стандартов и технологий

NNSS National Net Settlement Service, расчётный сервис Visa в США

NPCI National Payments Corporation of India, оператор UPI и RuPay в Индии

NRZ Non-Return-to-Zero, схема линейного кодирования (например, в ISO/IEC 14443 Type B); синонимы: без возврата к нулю

NTID Network Transaction ID, идентификатор операции сети Visa, используемый в цепочках MIT/CIT и CE 3.0

OCT Original Credit Transaction, обратный денежный перевод на карту через карточную сеть; синонимы: обратный перевод на карту

OFAC Office of Foreign Assets Control, санкционное подразделение Минфина США

OIDF OpenID Foundation, организация-разработчик OIDC и FAPI

OXXO Мексиканская сеть convenience-магазинов и одноимённый способ оплаты по штрихкоду; синонимы: OXXO Pay

P2PE Point-to-Point Encryption, шифрование данных карты от точки приёма до дешифрующего узла; PCI имеет одноимённый стандарт; синонимы: шифрование точка-точка

PAN Primary Account Number, основной номер карты (ISO/IEC 7812); синонимы: основной номер счёта

PAR Pushed Authorization Requests, режим OAuth с предварительной отправкой параметров (RFC 9126)

PCI Payment Card Industry, отрасль платёжных карт; в книге чаще обозначает PCI SSC и его стандарты

PDOL Processing Options Data Object List, список тегов EMV, которые терминал должен передать в команде GET PROCESSING OPTIONS; задаётся картой в FCI

PIN Personal Identification Number, секретный код держателя для верификации; синонимы: ПИН-код, ПИН, pin-код

PISP Payment Initiation Service Provider, поставщик услуг инициации платежа (PSD2)

PIX Бразильская система мгновенных платежей под управлением BCB

PKCE Proof Key for Code Exchange, защита OAuth-кода от перехвата (RFC 7636)

PKI Public Key Infrastructure, инфраструктура открытых ключей: удостоверяющие центры, сертификаты и правила доверия между ними

PoA Proof-of-Authority, алгоритм консенсуса с заранее утверждённым списком валидаторов; типичный выбор для приватных DLT и CBDC

POI Point of Interaction, обобщённый термин PCI для устройств приёма платежа; синонимы: point-of-interaction

POS Point of Sale, точка продажи; в узком смысле — POS-терминал; синонимы: Point-of-Sale, кассовый терминал

PoS Proof-of-Stake, алгоритм консенсуса, в котором право подписать блок получают участники, заблокировавшие залог криптовалюты; нарушители теряют залог (*slashing*). Применяется в Ethereum с 2022 г

PoW Proof-of-Work, алгоритм консенсуса, в котором валидаторы тратят вычислительную работу на подбор хеша; применяется в Bitcoin

PPSE Proximity Payment System Environment, бесконтактный аналог PSE (`2PAY.SYS.DDF01`); синонимы: бесконтактный каталог приложений

PSD2 Payment Services Directive 2, директива ЕС об открытом банкинге и SCA

PSE Payment System Environment, контактный каталог приложений на чипе (`1PAY.SYS.DDF01`)

PSP Payment Service Provider, провайдер платёжных услуг; синонимы: платёжный провайдер, поставщик платёжных услуг

PSU Payment Service User, клиент в терминологии PSD2

PTS PIN Transaction Security, стандарт PCI SSC для аппаратных модулей и POS-устройств

PWCB Purchase with Cashback, тип EMV-операции «покупка с выдачей наличных» (Mastercard); кодируется тегом `0x9C` = `0x09`; синонимы: Наличные на кассе

QMAP Questionable Merchant Audit Program, программа Visa по мониторингу подозрительных мерчантов

QR Quick Response (code), двумерный штрихкод как контейнер платёжных реквизитов; синонимы: QR-код, QR код

QSA Qualified Security Assessor, аккредитованный PCI SSC аудитор; синонимы: аккредитованный аудитор PCI

RATS Request for Answer To Select, команда PCD в ISO/IEC 14443-4 для перехода в режим обмена кадрами; ответ карты — ATS

RBA Risk-Based Authentication, риск-ориентированная аутентификация в 3-D Secure; синонимы: аутентификация на основе риска

RID Registered Application Provider Identifier, первая часть AID, идентифицирующая платёжную сеть (EMV); синонимы: идентификатор провайдера приложения

RKI Remote Key Injection, удалённая загрузка криптографических ключей в POS-терминал по защищённому каналу; синонимы: удалённая загрузка ключей, удалённая инъекция ключей

ROC Report on Compliance, итоговый отчёт QSA по PCI DSS; синонимы: отчёт о соответствии PCI

RRN Retrieval Reference Number, идентификатор, по которому участники находят операцию (DE 37 в ISO 8583); синонимы: сквозной ссылочный номер

RRP Relay-Resistant Protocol, защита от relay-атак в Mastercard M/Chip; синонимы: Distance bounding, привязка по расстоянию

RSA Rivest-Shamir-Adleman, асимметричный криптоалгоритм; синонимы: Rivest–Shamir–Adleman

RTGS Real-Time Gross Settlement, валовой расчёт в реальном времени; синонимы: режим срочного перевода

RTO Recovery Time Objective, целевое время восстановления сервиса после инцидента

RTS Regulatory Technical Standards, технические регламентирующие стандарты EBA по PSD2

SAD Sensitive Authentication Data, данные аутентификации, не подлежащие хранению по PCI DSS; синонимы: чувствительные аутентификационные данные, чувствительные данные аутентификации

SAK Select Acknowledge, ответ PICC в ISO/IEC 14443-3 на SELECT в ходе антиколлизии; указывает тип кадра

SAM Settlement Account Management, расчётная подсистема Mastercard: нетто-позиции участников после клиринга (Banknet/GCMS)

SAQ Self-Assessment Questionnaire, опросник самооценки PCI DSS; синонимы: PCI SAQ

SCA Strong Customer Authentication, строгая аутентификация клиента (PSD2); синонимы: усиленная аутентификация

SCF Stored Credential Framework, правила Visa и Mastercard для повторных списаний по сохранённым реквизитам

SCT Inst SEPA Instant Credit Transfer, мгновенный кредитовый перевод в евро по своду правил EPC; целевое сквозное время 10 секунд, 24/7/365

SDA Static Data Authentication, статическая офлайн-аутентификация данных карты (EMV)

SDK Software Development Kit, набор библиотек для интеграции в приложение; синонимы: комплект разработчика

SDN Specially Designated Nationals (and Blocked Persons), санкционный список OFAC; синонимы: SDN List

SDP Site Data Protection, программа Mastercard, предшественница PCI DSS

SE Secure Element, аппаратный защищённый элемент устройства

SEPA Single Euro Payments Area, единое пространство платежей в евро

SFI Short File Identifier, 5-битный идентификатор файла на чипе EMV/ISO 7816-4; адресует записи внутри AFL

SLA Service Level Agreement, соглашение об уровне обслуживания; синонимы: договор об уровне обслуживания

SMC Secure Messaging Confidentiality, ключ EMV для шифрования сценариев эмитента

SMI Secure Messaging Integrity, ключ EMV для целостности сценариев эмитента

SNA Systems Network Architecture, проприетарный сетевой стек IBM

SPI Sistema de Pagamentos Instantâneos, бразильская инфраструктура мгновенных расчётов, на которой работает PIX

SRED Secure Reading and Exchange of Data, модуль PCI PTS для шифрования данных карты внутри терминала

STAN System Trace Audit Number, локальный счётчик операций терминала/эквайера (DE 11 в ISO 8583); синонимы: Systems Trace Audit Number, номер трассировки

STIP Stand-In Processing, авторизация на стороне сети, когда эмитент недоступен; синонимы: стенд-ин

SWIFT Society for Worldwide Interbank Financial Telecommunication, межбанковская сеть передачи финансовых сообщений

TAC Terminal Action Codes, заданные сетью правила решения по EMV-операции на терминале; синонимы: коды действий терминала

TADG Visa Transaction Acceptance Device Guide, документация интерфейса Visa для эквайера; синонимы: Visa Terminal Acceptance Device Guide, Visa Technology Asset Documentation

TAVV Token Authentication Verification Value, криптограмма токена в CNP-операциях (Visa Token Service)

TC Transaction Certificate, криптограмма операции EMV, одобренной офлайн; синонимы: криптограмма офлайн-операции

TC33 Формат клирингового файла Visa BASE II; синонимы: TC 33, transaction code 33

TDEA Triple Data Encryption Algorithm, он же Triple DES (3DES); устаревший симметричный шифр; синонимы: тройной DES

TDOL Transaction Certificate Data Object List, список тегов EMV для криптограммы TC, задаваемый картой по умолчанию

TEE Trusted Execution Environment, изолированная среда исполнения внутри основного процессора устройства (в смартфонах — ARM TrustZone); используется мобильными кошельками для хранения ключей без отдельного чипа SE

TID Terminal ID, идентификатор терминала у эквайера; синонимы: номер терминала

TIPS TARGET Instant Payment Settlement, центробанковская платформа расчёта мгновенных платежей в евро под управлением Eurosystem; работает 24/7/365 в деньгах центрального банка

TLV Tag-Length-Value, формат кодирования данных EMV (BER-TLV)

TMK Terminal Master Key, мастер-ключ POS-терминала; под ним хранятся остальные ключи устройства

TMS Terminal Management System, система управления парком терминалов; синонимы: система управления терминалами

TPK Terminal PIN Key, ключ шифрования PIN внутри POS-терминала

TPP Third Party Provider, сторонний поставщик услуг в открытом банкинге PSD2; синонимы: СПУ

TPAP Third-Party Application Provider, небанковское приложение в UPI (PhonePe, Google Pay, Paytm), работающее через PSP-bank; для одного TPAP действует потолок 30 % объёма

TPR Transaction Processing Rules, документ Mastercard, описывающий правила формирования авторизационных сообщений

TPS Transactions Per Second, операций в секунду; целевая метрика производительности

TRA Transaction Risk Analysis, освобождение от SCA на основе риск-анализа эквайера (PSD2); синонимы: анализ риска операции

TRID Token Requestor ID, идентификатор запросчика токена в EMVCo

TSP Token Service Provider, провайдер токенизации; синонимы: провайдер услуг токенизации

TTQ Terminal Transaction Qualifiers, тег EMV (`0x9F66`) с возможностями и предпочтениями бесконтактного терминала (online-предпочтение, поддерживаемые CVM)

TVR Terminal Verification Results, результаты проверок терминала по операции EMV

UBO Ultimate Beneficial Owner, конечный бенефициарный владелец (KYB)

UDK Unique Derivation Key, ключ карты, выведенный из IMK эмитента по PAN; основа сессионных ключей AC

UN Unpredictable Number, случайное число терминала в EMV (тег `0x9F37`); входит в CDOL1 и служит nonce для криптограммы

UPI Unified Payments Interface, индийская A2A-система мгновенных платежей

UZCARD Узбекская национальная платёжная система

VAA Visa Advanced Authorization, риск-сервис Visa, оценивающий вероятность фрода в авторизации

VAMP Visa Acquirer Monitoring Program, программа Visa мониторинга эквайеров по фроду и chargeback

VAU Visa Account Updater, сервис автоматического обновления реквизитов карт у мерчантов; синонимы: Real-Time Account Updater

VOP Verification of Payee, обязательная по IPR проверка соответствия имени получателя и IBAN перед инициацией SCT/SCT Inst; схема EPC, обязательна с 9 октября 2025 года (свод правил EPC — с 5 октября); синонимы: проверка получателя

VPA Virtual Payment Address, идентификатор получателя в UPI вида `name@psp`, связывающий пользователя с банковским счётом без раскрытия реквизитов

VCAS Visa Consumer Authentication Service, ACS-как-сервис Visa для эмитентов в 3-D Secure

VCPS Visa Contactless Payment Specification, спецификация бесконтактных платежей Visa

VCR Visa Claim Resolution, регламент работы со спорами Visa

VDMP Visa Dispute Monitoring Program, программа Visa мониторинга мерчантов по доле споров

VEPS Visa Easy Payment Service, упрощённый бесконтактный сценарий с ограничением суммы и без CVM

VFMP Visa Fraud Monitoring Program, программа Visa мониторинга мерчантов по доле фрода

VROL Visa Resolve Online, инструмент Visa для работы со спорами и обмена доказательствами

VSDC Visa Smart Debit/Credit, бренд EMV-приложений Visa на чипе (контактный и бесконтактный профили, qVSDC — бесконтактный)

VT Virtual Terminal, ввод реквизитов оператором ТСП через защищённую страницу (PCI SAQ C-VT)

VTS Visa Token Service, токенизационный сервис Visa

WAF Web Application Firewall, межсетевой экран уровня приложений

WUPA Wake-Up Type A, команда PCD активации PICC в ISO/IEC 14443-3 Type A; ответ карты — ATQA

XS2A Access to Account, фреймворк доступа к счёту в PSD2/Berlin Group

ZMK Zone Master Key, мастер-ключ зоны; передаётся между организациями (банк, процессор, сеть) для защищённого обмена другими ключами

АСВ Агентство по страхованию вкладов

АФТ Ассоциация ФинТех, разработчик отраслевых стандартов открытых API в России; синонимы: Ассоциация развития финансовых технологий

БИК	Банковский идентификационный код, девятизначный код участника платёжной системы Банка России
БПА	Банковский платёжный агент (161-ФЗ)
БЭСП	Банковские электронные срочные платежи, исторический сервис ВРСС Банка России (выведен из эксплуатации в 2018 г.)
ГРБС	Главный распорядитель бюджетных средств; орган, определённый ст. 158 Бюджетного кодекса РФ, имеющий право распределять бюджетные ассигнования и лимиты обязательств между подведомственными получателями
ДБО	Дистанционное банковское обслуживание (мобильный банк, интернет-банк и др.)
ЕАГ	Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма
ЕБС	Единая биометрическая система
ЕЦБ	Европейский центральный банк; синонимы: ECB, European Central Bank
ЕЭЗ	Европейская экономическая зона
МБВ	Мир Бюджетные Выплаты, продуктовый стандарт карт Мир для бюджетных получателей
МВК	Межведомственная комиссия по противодействию финансированию терроризма
Наличные на кассе	Сервис ПС Мир «покупка с выдачей наличных» (аналог PWCB); для карт, эмитированных после 10.04.2023, лимит 5 000 рублей, обязательны онлайн-PIN или CDCVM; синонимы: Purchase with Cashback
НКО	Небанковская кредитная организация
НПС	Национальная платёжная система Российской Федерации (161-ФЗ)
НСПК	Национальная система платёжных карт, оператор карты Мир и СБП; синонимы: АО НСПК, АО НСПК
ОД	Отмывание доходов, полученных преступным путём; вместе с ФТ образует ПОД/ФТ
ОПКЦ	Операционный и платёжный клиринговый центр НСПК, обрабатывающий внутрироссийские транзакции международных сетей; синонимы: операционно-клиринговый центр
ОСР	Оператор сервиса рассрочки, статус по Федеральному закону от 31.07.2025 № 283-ФЗ
ОУД4	Оценочный уровень доверия 4 по ГОСТ Р ИСО/МЭК 15408 (аналог Common Criteria EAL4)
ОУПИ	Оператор услуг платёжной инфраструктуры (операционный, платёжный клиринговый, расчётный центры)
ОФД	Оператор фискальных данных, организация-посредник по 54-ФЗ, принимающая фискальные документы от касс и передающая их в ФНС
ОЦ	Операционный центр в архитектуре НПС (см. ОУПИ)
ПКС	Платформа коммерческих согласий Банка России
ПКЦ	Платёжный клиринговый центр в архитектуре НПС (см. ОУПИ)
ПОД	Противодействие отмыванию доходов; вместе с ФТ образует ПОД/ФТ; синонимы: противодействие легализации
ППС	Перспективные платёжные сервисы Банка России (преемник БЭСП)
ПС	Платёжная система
ПУ	Поставщик услуг в российском открытом банкинге (СТО БР ФАПИ.СЕК); аналог ASPSP
ПЭП	Политически значимое лицо (politically exposed person); синонимы: PEP, политически значимый клиент
РСБУ	Российские стандарты бухгалтерского учёта
РЦ	Расчётный центр в архитектуре НПС (см. ОУПИ)
СБП	Система быстрых платежей Банка России
СКЗИ	Средство криптографической защиты информации, сертифицированное ФСБ России
СПУ	Сторонний поставщик услуг в российском открытом банкинге; аналог TPP
СПФС	Система передачи финансовых сообщений Банка России
ССНП	Сервисы срочного и несрочного перевода в платёжной системе Банка России (Положение Банка России от 25.07.2022 № 802-П); синонимы: Сервис срочных и несрочных переводов, Сервис срочных переводов платёжной системы Банка России
СТО	Стандарт организации; в открытом банкинге – СТО БР (Банка России)
ТК	Технический комитет Росстандарта; ТК 26 разрабатывает криптографические стандарты
УФЭБС	Унифицированный формат электронных банковских сообщений Банка России; синонимы: унифицированные форматы электронных банковских сообщений
ФАПИ	Финансовые API; русское обозначение профиля FAPI в стандартах СТО БР; синонимы: Financial-grade API
ФАПИ.СЕК	Профиль безопасности открытых API Банка России (СТО БР ФАПИ.СЕК)
ФАС	Федеральная антимонопольная служба
ФД	Фискальный документ, элемент данных кассы по 54-ФЗ (чек, отчёт открытия/закрытия смены и др.)

Финмониторинг	Финансовый мониторинг — русский канон функции AML (мониторинг операций, формирование ФЭС, разбор сигналов); омоним: Росфинмониторинг (надзорный орган)
ФинЦЕРТ	Центр взаимодействия и реагирования Департамента информационной безопасности Банка России; синонимы: FinCERT
ФН	Фискальный накопитель, аппаратный модуль кассы по 54-ФЗ, хранящий фискальные документы и подписывающий их ФПД
ФНС	Федеральная налоговая служба
ФПД	Фискальный признак документа, криптографическая подпись фискального документа, вырабатываемая ФН
ФРОМУ	Финансирование распространения оружия массового уничтожения; вместе с ОД и ФТ образует ПОД/ФТ/ФРОМУ
ФТ	Финансирование терроризма; вместе с ОД образует ПОД/ФТ; синонимы: CFT, Combatting the Financing of Terrorism
ФЭС	Формализованное электронное сообщение (115-ФЗ; обмен с Росфинмониторингом)
ЦБ РФ	Центральный банк Российской Федерации (Банк России); синонимы: ЦБ, Центральный банк РФ, Центробанк
ЦНФС	Центр новых финансовых сервисов, дочернее общество Сбербанка; синонимы: Плати частями
ЭДС	Электронные денежные средства (161-ФЗ)
ЭЛКАРТ	Кыргызская национальная платёжная система; см. также ELCARD
ЭСП	Электронное средство платежа (161-ФЗ)

Список источников

[1] *Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платёжной системе»*.

[2] *Федеральный закон от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации»*.

[3] *Федеральный закон от 23.12.2003 № 177-ФЗ «О страховании вкладов»*.

[4] *Федеральный закон от 24.07.2023 № 340-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (закон о цифровом рубле)*.

[5] Банк России. *Платёжная система Банка России*. 2026.

[6] Банк России. *Положение от 24.11.2022 № 809-П «О Плане счетов бухгалтерского учёта»*. 2022.

[7] Банк России. *Положение Банка России от 03.12.2025 № 876-П «О платёжной системе Банка России»*. 2025.

[8] Банк России. *Ответы на вопросы по Указанию Банка России от 30.11.2014 № 3462-У*. 2014.

[9] SWIFT. *About SWIFT: Society for Worldwide Interbank Financial Telecommunication*. 2024.

[10] SWIFT. *Global financial community completes switch to ISO 20022, paving the way for new levels of cross-border payment speed and innovation around the world*. 2025.

[11] SWIFT. *ISO 20022: MT to ISO 20022 Conversion*. 2026.

[12] Банк России. *Система передачи финансовых сообщений (СПФС)*. 2024.

[13] Visa. *Visa Core Rules and Visa Product and Service Rules*. 2025.

[14] Mastercard. *Global Clearing Management System Reference Manual*. 2021.

[15] Mastercard. *Mastercard Rules*. 2025.

[16] ISO. *ISO 18245:2023 «Merchant category codes»*. 2023.

[17] НСПК. *О компании АО «НСПК»*. 2025.

[18] Visa. *Inside Visa's engine of global commerce*. 2025.

[19] Futurum. *The Main Scoop, Episode 09: How Mastercard Empowers Sustainable Digital Economies*. 2023.

[20] European Parliament and Council. *Regulation (EU) 2015/751 on interchange fees for card-based payment transactions*. 2015.

[21] Visa. *Credit Card Processing Fees & Interchange Rates*. 2026.

[22] Mastercard. *Merchant Rates, Incentives, and Interchange*. 2026.

[23] American Express. *American Express Network*. 2026.

[24] American Express. *Form 10-K Annual Report 2014: Global Network & Merchant Services*. 2015.

[25] Банк Русский Стандарт. *Банк Русский Стандарт и American Express подписали 10-летний контракт*. 2017.

[26] Ведомости. *American Express не смогла договориться со Сбербанком*. 2015.

[27] Lenta.ru. *Сбербанк откажется от American Express*. 2016.

[28] Discover Financial Services. *Merger of Discover Financial Services and Pulse EFT Association Closes Following Pulse Member Approval*. 2005.

[29] JCB. *JCB Corporate Profile*. 2025.

[30] EMVCo. *EMV Book 2 «Security and Key Management»*. Вер. 4.4. 2022.

[31] EMVCo. *EMV Book 3 «Application Specification»*. Вер. 4.4. 2022.

[32] EMVCo. *EMV Book 4 «Cardholder, Attendant, and Acquirer Interface Requirements»*. Вер. 4.3. 2011.

[33] Amazon Web Services. *AWS Payment Cryptography: Industry Terminology*. 2026.

[34] FIS. *ISO 8583 Reference Guide V2.46*. 2023.

[35] EMVCo. *EMV Payment Tokenisation Specification «Technical Framework»*. 2024.

[36] Visa. *Visa Token Service Provisioning and Credential Management*. 2026.

[37] НСПК. *Программное обеспечение НСПК: мобильные решения, терминальные технологии (раздел Mir HCE SDK)*. 2026.

[38] Mastercard. *Chargeback Guide Merchant Edition*. 2026.

[39] Visa. *Visa Claims Resolution: Efficient Dispute Processing for Merchants*. 2017.

[40] BIS CPMI. *A glossary of terms used in payments and settlement systems*. 2016.

[41] Банк России. *Письмо от 30.06.2005 № 92-Т «Об организации управления правовым риском и риском потери деловой репутации»*. 2005.

[42] Visa. *Visa Third Party Agent Registration Program Frequently Asked Questions*. 2016.

[43] Visa. *Visa Merchant Data Standards Manual*. 2025.

[44] Банк России (ФинЦЕРТ). *Обзоры о несанкционированных операциях по картам и в национальной платёжной системе*. 2026.

[45] Visa. *Introducing the Visa Acquirer Monitoring Program*. 2024.

[46] Mastercard. *Transaction Processing Rules*. 2025.

[47] Mastercard. *Security Rules and Procedures — Merchant Edition*. 2025.

[48] Visa. *Visa Merchant Screening Service*. 2026.

[49] НСПК. *Программа безопасности ПС Мир*. 2024.

[50] Visa. *Beyond the Acquirer: Additional Visa Acceptance Entities*. 2024.

[51] Visa. *Payment Facilitator and Marketplace Risk Guide: How to Identify and Manage Risk in Today's Payment Ecosystem*. 2021.

[52] Банк России. *Указание от 06.04.2020 № 5429-У «О ведении перечня БПА-агрегаторов»*. 2020.

[53] *Федеральный закон от 20.02.2026 № 44-ФЗ «Об ограничении идентификации физических лиц банковскими платёжными агентами»*.

[54] ISO. *Bank card numbers are getting longer*. 2016.

[55] Visa. *Transaction Acceptance Device Guide (TADG), Version 3.3*. 2025.

[56] American National Standards Institute. *Issuer Identification Number (IIN) Registration Program*. 2026.

[57] ISO/IEC. *ISO/IEC 7812-1:2017 «Numbering system»*. 2017.

[58] ISO/IEC. *ISO/IEC 7812-2:2017 «Application and registration procedures»*. 2017.

[59] Google Patents. *US2950048A — Computer for Verifying Numbers*. 1960.

[60] Росстандарт. *ГОСТ Р ИСО/МЭК 7811-6–2017 «Карты идентификационные. Способ записи. Магнитная полоса большой коэрцитивной силы»*. 2017.

[61] ISO/IEC. *ISO/IEC 7811-2:2018 «Magnetic stripe recording»*. 2018.

[62] ISO/IEC. *ISO/IEC 7813:2006 «Financial transaction cards»*. 2006.

[63] *Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»*.

[64] PCI Security Standards Council. *Does PCI DSS apply to bank account data?* 2023.

[65] Mastercard. *MasterCard Security Rules and Procedures*. 2016.

[66] Visa. *Visa Smart Debit/Credit and Visa payWave Contact/Contactless U.S. Acquirer Implementation Guide*. 2020.

[67] Amazon Web Services. *AWS Payment Cryptography: Card Verification Functions (CVV, CVV2, iCVV)*. 2025.

[68] Visa. *Mitigating Fraud Risk Through Card Data Verification*. 2015.

[69] Mastercard. *MasterCard Contactless Security Fact Sheet*. 2015.

[70] PCI Security Standards Council. *PCI DSS v4.0.1*. 2024.

[71] PCI Security Standards Council. *Does cardholder name, expiration date, etc. need to be rendered unreadable if stored in conjunction with the PAN?* 2025.

[72] PCI Security Standards Council. *Can card verification codes be stored for card-on-file or recurring transactions?* 2025.

[73] PCI Security Standards Council. *How can an entity meet PCI DSS requirements for PAN masking and truncation if it has migrated to 8-digit BINs?* 2024.

[74] ISO. *ISO 8583:2023 «Financial-transaction-card-originated messages — Interchange message specifications»*. 2023.

[75] НСПК. *Правила платёжной системы «Мир»*. 2026.

[76] Mastercard. *Mastercard U.S. Region Merchant Rates 2025–2026*. 2025.

[77] Parliament of the United Kingdom. *Financial Services and Markets Act 2023, c. 29*. 2023.

[78] FCA. *Access to Cash, Policy Statement PS24/8*. 2024.

[79] Interac. *Accept Interac Debit*. 2025.

[80] Наталья Азисова. *Что такое клиринг, как он работает и реализован на примере платёжной системы «Мир»*. 2022.

[81] U.S. Payments Forum. *Transit Contactless Open Payments: Technical Solution for Pay As You Go (PAYG), v2.0*. 2018.

[82] Visa. *Smarter STIP: Stand-In Processing with Deep Learning*. 2020.

[83] Visa. *V.I.P. System Overview*. 2005.

[84] ISO. *ISO 4217:2015 «Currency codes»*. 2015.

[85] Visa. *Request and Response Codes*. 2026.

[86] EMVCo. *EMV Integrated Circuit Card Specifications for Payment Systems*. 2026.

[87] jPOS. *jPOS ISO 8583:1987 packager «base1.xml»*. 2026.

[88] NIBSS. *POS ISO 8583:1987 Interface Specification, Data Element Definitions*. 2026.

[89] myPOS. *What Is the ISO 8583 Standard and Why Is It Important*. 2026.

[90] EMVCo. *Why EMV?* 2026.

[91] EMVCo. *EMV Book 1 «Application Independent ICC to Terminal Interface Requirements»*. Вер. 4.4. 2022.

[92] Visa. *EMV Liability Shift*. 2017.

[93] Visa. *Chip Technology Helped Reduce Counterfeit Fraud by 80 percent*. 2019.

[94] American Banker / PaymentsSource. *EMV's proving its mettle in counterfeit reduction*. 2019.

[95] GlobalPlatform. *GlobalPlatform Card Specification*. Вер. 2.3.1. 2018.

[96] EMVCo. *Chip & Platform Approval Process*. 2025.

[97] EMVCo. *EMVCo Becomes an Accredited ISO/IEC Certification Body*. 2024.

[98] Eurosmart и BSI. *Security IC Platform Protection Profile with Augmentation Packages (BSI-CC-PP-0084-2014)*. 2014.

[99] NXP Semiconductors. *JCOP 4 EMV: Advanced Java Card™ OS for Payment and Transit*. 2019.

[100] ISO/IEC. *ISO/IEC 7816-2:2007 «Smart card contact dimensions and location»*. 2007.

[101] ISO/IEC. *ISO/IEC 7816-3:2006 «Smart card electrical interface and transmission protocols»*. 2006.

[102] ISO/IEC. *ISO/IEC 7816-4:2020 «Smart card APDU and commands»*. 2020.

[103] UnionPay International. *UnionPay International cooperates with NSPK in card-issuance*. 2016.

[104] ISO/IEC. *ISO/IEC 8825-1:2021 «ASN.1 Basic Encoding Rules (BER)»*. 2021.

[105] EMV Lab. *EMV tag 9F22: Certification Authority Public Key Index*. 2026.

[106] EMV Lab. *EMV tag 9F4C: ICC Dynamic Number*. 2026.

[107] EMVCo. *EMV Contactless Book C-3 «Kernel 3 (Visa)»*. 2024.

[108] EMVCo. *EMV Contactless Book C-2 «Kernel 2 (Mastercard)»*. 2024.

[109] Mike Bond и др. *Chip and Skim: Cloning EMV Cards with the Pre-play Attack*. 2014. DOI: 10.1109/SP.2014.11.

[110] EMVCo. *EMVCo Newsletter: Q1 2025*. 2025.

[111] EMV Decoder. *EMV Tag Decoder: AIP, TVR, TSI, CVM List*. 2026.

[112] Thredd. *Chip Parameters Guide*. Вер. 1.0. 2024.

[113] Amazon Web Services. *AWS Payment Cryptography: Visa-specific Functions and ARQC Verification*. 2025.

[114] Gemini Advisory. *Cybercriminals Deploy EMV-Bypass Cloning*. 2020.

[115] CNews. *Московский индустриальный банк — первый в России эмитент карт MasterCard PayPass*. 2011.

[116] АСРОС. *Альфа-Банк и Visa выпустили в России первую карту Visa payWave*. 2011.

[117] Правительство Санкт-Петербурга. *Петербургский метрополитен первым в России открыл приём бесконтактной оплаты на турникетах по технологии MasterCard PayPass*. 2015.

[118] Tadviser. *Moscow Metro implemented technology of contactless payment of journey*. 2016.

[119] Правительство Москвы. *Оплатить проезд банковскими картами теперь можно на 20 станциях метро*. 2016.

[120] Visa. *Quick Chip for EMV and qVSDC — Specification*. 2017.

[121] РИА Новости. *Сбербанк начал выпускать бесконтактные карты «Мир»*. 2017.

[122] UL Solutions. *Optimizing POS EMV Terminals*. 2016.

[123] EMVCo. *EMV «Card Personalisation Specification»*. Вер. 2.0. 2021.

[124] ISO/IEC. *ISO/IEC 14443-1:2018 «Contactless proximity objects — Part 1: Physical characteristics»*. 2018.

[125] ISO/IEC. *ISO/IEC 14443-2:2020 «Contactless proximity objects — Part 2: Radio frequency power and signal interface»*. 2020.

[126] ISO/IEC. *ISO/IEC 14443-3:2018 «Contactless proximity objects — Part 3: Initialization and anticollision»*. 2018.

[127] ISO/IEC. *ISO/IEC 14443-4:2018 «Contactless proximity objects — Part 4: Transmission protocol»*. 2018.

[128] EMVCo. *EMV Contactless Book A «Architecture and General Requirements»*. 2024.

[129] Lishoy Francis и др. *Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones*. 2011.

[130] EMVCo. *EMVCo Publishes EMV Contactless Kernel Specification*. 2022.

[131] Платёжная система Мир. *ВТБ начал выпуск кобейджинговых карт Мир–Maestro*. 2019.

[132] ISO/IEC. *ISO/IEC 7816-5:2004 «Smart card AID registration»*. 2004.

[133] BIS Journal. *Электронная коммерция и информационная безопасность. Безопасность карты «Мир»*. 2017.

[134] Росстандарт. *Рекомендация по стандартизации Р 1323565.1.015–2018 «Задание параметров алгоритмов электронной подписи и функции хэширования в профиле EMV сертификатов открытых ключей платёжных систем»*. 2018.

[135] Westpac. *Contactless card technology FAQs*. 2026.

[136] Zeller. *Understanding Contactless payment limits and PIN requirements*. 2026.

[137] Financial Conduct Authority. *Greater flexibility to be given for setting future contactless limits*. 2025.

[138] Известия. *ЦБ рассказал о дальнейшей работе карт Visa и Mastercard в России*. 2022.

[139] EMVCo. *EMV Mobile*. 2026.

[140] НСПК. *Банки представили прототип мобильного приложения под «Волну»*. 2025.

[141] Apple. *Apple Pay Component Security*. 2024.

[142] Google. *Host-based card emulation overview*. 2026.

[143] Google. *Device Tokenization Developer Site: Security*. 2026.

[144] European Commission. *Commission accepts commitments by Apple opening access to «tap and go» technology on iPhones*. 2024.

[145] Apple. *Developers can soon offer in-app NFC transactions using the Secure Element*. 2024.

[146] Google. *Fitbit Pay FAQ. Device Tokenization Developer Site*. 2024.

[147] Samsung. *Samsung Pay Security: TrustZone and TEE*. 2024.

[148] Google. *Titan M makes Pixel 3 our most secure phone yet*. 2018.

[149] NXP Semiconductors. *NXP and Garmin Team-up to Bring Secure and Convenient NFC Mobile Payments to New Fitness Wearables*. 2018.

[150] Garmin. *Работает ли Garmin Pay с системой платежей МИР?* 2022.

[151] Коммерсантъ. *Apple Pay официально прекратила поддержку карт «Мир»*. 2022.

[152] НСПК. *Программное обеспечение НСПК: мобильные решения, терминальные технологии (раздел SDK «Волна»)*. 2026.

[153] РБК. *«Сбер» перезапустил оплату айфоном по аналогии с Apple Pay*. 2025.

[154] PLUSworld. *Сбербанк запустил бесконтактную оплату iPhone при помощи технологии «Вжух»*. 2025.

[155] Т-Банк. *Бесконтактная оплата с T-Pay на iPhone*. 2025.

[156] Альфа-Банк. *AlfaPay: документация интернет-эквайринга*. 2025.

[157] НСПК. *Глава НСПК: «Мы стремимся предоставить универсальное решение гражданам»*. 2026.

[158] Apple. *Card provisioning security overview*. 2024.

[159] Google. *Device Tokenization Developer Site: Overview*. 2025.

[160] EMVCo. *EMV Contactless Chip*. 2026.

[161] EMVCo. *Wearable Level 1 Approval Process*. 2026.

[162] Saar Drimer и Steven J. Murdoch. «Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks». В: *Proceedings of the 16th USENIX Security Symposium*. 2007.

[163] Thomas Korak и Michael Hutter. *On the Power of Active Relay Attacks using Custom-Made Proxies*. 2014.

[164] Chong Hee Kim и Gildas Avoine. *RFID distance bounding protocol with mixed challenges to prevent relay attacks*. 2009.

[165] Ioana Boureanu и др. «Security Analysis and Implementation of Relay-Resistant Contactless Payments». В: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS 2020)*. 2020, с. 879—898. DOI: 10.1145/3372297.3417235.

[166] United States Department of Justice. *Alleged International Hacker Indicted for Massive Attack on U.S. Retail and Banking Networks*. 2009.

[167] Heartland Payment Systems. *Annual Report on Form 10-K for the fiscal year ended December 31, 2010*. 2011.

[168] PCI Security Standards Council. *PCI DSS Tokenization Guidelines*. 2011.

[169] НСПК. *Правила платёжной системы «Мир». Версия 4.3 (П.070)*. 2025.

[170] Датабанк. *Условия использования платёжного приложения Mir Pay*. 2026.

[171] Банк России. *Карты всех платежных систем в России продолжают нормально работать*. 2022.

[172] Ведомости. *Попавшие под санкции банки прекратят работу с Apple Pay и Google Pay*. 2022.

[173] Банк России. *Все платёжные карты российских банков продолжают нормально работать*. 2022.

[174] EMVCo. *EMV Payment Tokenisation «A Guide to Use Cases»*. Вер. 2.2.1. 2023.

[175] NIST. *NIST SP 800-38G: Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption*. 2016.

[176] Mastercard. *The Invisible Handshake: How Tokenization Is Revolutionizing Digital Interactions*. 2024.

[177] Mastercard. *MDES Token Connect — Token Requestor Implementation Guide and Specifications*. 2021.

[178] Visa. *Enable Digital Card Loading: Visa Card Enrollment Hub*. 2026.

[179] PCI Security Standards Council. *Tokenization Product Security Guidelines*. 2015.

[180] NIST. *NIST SP 800-38G Rev. 1 (2nd Public Draft): Methods for Format-Preserving Encryption*. 2025.

[181] Росстандарт. *ГОСТ Р 57580.1–2017 «Защита информации финансовых организаций. Базовый состав мер»*. 2017.

[182] ТК 26. *Рекомендации по стандартизации ТК 26*. 2026.

[183] Yves-Alexandre de Montjoye и др. «Unique in the shopping mall: On the reidentifiability of credit card metadata». В: *Science* 347.6221 (2015), с. 536—539. DOI: 10.1126/science.1256297.

[184] NIST. *SP 800-67 Rev. 2: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*. 2017.

[185] NIST. *NIST to Withdraw Special Publication 800-67 Revision 2*. 2023.

[186] NIST. *FIPS 197: Advanced Encryption Standard (AES)*. 2023.

[187] EMVCo. *EMVCo Security Evaluation FAQs for ECC*. 2022.

[188] EMVCo. *EMV Specifications & Associated Bulletins*. 2026.

[189] SECG. *SEC 1: Elliptic Curve Cryptography, Version 2.0*. 2009.

[190] Росстандарт. *ГОСТ 34.10–2018 «Процессы формирования и проверки ЭЦП»*. 2018.

[191] NIST. *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)*. 2024.

[192] NIST. *FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA)*. 2024.

[193] NIST. *FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA)*. 2024.

[194] EMVCo. *Quantum Computing and EMV Chip — What's the Threat?* 2025.

[195] EMVCo. *Security Position Statement: Quantum Computing and EMV Chip Cryptography*. 2025.

[196] Mastercard. *Migration to Post-Quantum Cryptography*. 2025.

[197] Mastercard. *Mastercard and partners deliver first contactless cards for quantum world*. 2022.

[198] Futurex. *Futurex Becomes Only HSM Supporting PQC That Has Been PCI HSM Validated*. 2025.

[199] NIST. *FIPS 140-3: Security Requirements for Cryptographic Modules*. 2019.

[200] PCI Security Standards Council. *PCI PIN Security Requirements*. 2026.

[201] PCI Security Standards Council. *PCI PTS Hardware Security Module (HSM) Standard*. 2026.

[202] Thales/Entrust. *payShield 10K Host Programmer's Manual (General Host Commands Reference, doc 007-001518)*. 2024.

[203] EFTlab. *Complete list of Thales HSM commands*. 2025.

[204] Банк России. *Функционально-технические требования от 28.02.2020 № ФТ-56-3/35 «Аппаратный модуль безопасности (HSM)»*. 2020.

[205] Банк России. *Положение от 17.08.2023 № 821-П «О защите информации при переводах денежных средств»*. 2023.

[206] Банк России. *Положение от 30.01.2025 № 851-П «О противодействии переводам без согласия клиента»*. 2025.

[207] ИнфоТеКС. *Получены сертификаты ФСБ России для ViPNet HSM*. 2023.

[208] ФСБ России. *Приказ от 27.12.2011 № 796 «Об утверждении требований к средствам электронной подписи и средствам удостоверяющего центра»*. 2011.

[209] ООО «КриптоПро». *КриптоПро HSM 2.0 R3 с Платёжным модулем*. 2024.

[210] АО «ИнфоТеКС». *ViPNet HSM PS — аппаратный криптомодуль для платёжных систем*. 2024.

[211] ООО «Системы Практической Безопасности». *SPB HSM PS: платёжное приложение модуля безопасности (base / Plus)*. 2024.

[212] NIST. *SP 800-57 Part 1: Recommendation for Key Management*. 2020.

[213] Accredited Standards Committee X9. *ANSI X9.24-3: Retail Financial Services Symmetric Key Management, Part 3: Derived Unique Key Per Transaction (DUKPT) Using AES*. 2017.

[214] Accredited Standards Committee X9. *Supplement to ANSI X9.24-3-2017 Test Vectors*. 2018.

[215] ISO. *ISO 9564-1:2017 «PIN management for ATM and POS»*. 2017.

[216] Stripe. *Testing: card numbers*. 2026.

[217] PCI Security Standards Council. *PCI Security Standards Bulletin: PCI SSC Announces Suspension of ISO Format 4 PIN Block Support Dates*. 2021.

[218] PCI Security Standards Council. *Information Supplement: Implementing ISO Format 4 PIN Blocks*. 2021.

[219] Росстандарт. *ГОСТ 34.11–2018 «Функция хэширования Стрибог»*. 2018.

[220] Росстандарт. *ГОСТ 34.12–2018 «Блочные шифры Кузнечик и Магма»*. 2018.

[221] Росстандарт. *ГОСТ 34.13–2018 «Режимы работы блочных шифров»*. 2018.

[222] Госстандарт СССР. *ГОСТ 28147–89 «Алгоритм криптографического преобразования»*. 1989.

[223] European Central Bank. *Report on Card Fraud in 2020 and 2021*. 2023.

[224] EMVCo. *EMV 3-D Secure White Paper «Introduction»*. 2025.

[225] European Parliament and Council. *Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*. 2015.

[226] CERT-EU. *Threat Memo: Credit-Card Web-Skimming Infections Can Last Several Months*. 2020.

[227] Adyen. *Address Verification System (AVS)*. 2026.

[228] Visa. *Visa Secure: User Interface Requirements for 3-D Secure 1.0.2*. 2019.

[229] Visa. *Visa Will Discontinue Support of 3-D Secure 1.0.2*. 2021.

[230] EMVCo. *Decoupled Authentication*. 2025.

[231] Visa. *Preparing for PSD2 SCA*. 2018.

[232] Visa. *Visa Secure Rules Will Be Updated*. 2021.

[233] European Commission. *Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication*. 2018.

[234] EMVCo. *Recurring and Installment Transactions — Technical Features*. 2025.

[235] PCI Security Standards Council. *What is the Payment Card Industry Data Security Standard (PCI DSS)?* 2012.

[236] PCI Security Standards Council. *Who are the founders of the PCI Security Standards Council?* 2021.

[237] United States Department of Justice. *International Hacker Pleads Guilty for Massive Hacks of U.S. Retail Networks*. 2009.

[238] PCI Security Standards Council. *Guidance for PCI DSS Scoping and Network Segmentation*. 2016.

[239] PCI Security Standards Council. *PCI Point-to-Point Encryption (P2PE) Standard*. 2024.

[240] PCI Security Standards Council. *Important Updates Announced for Merchants Validating to Self-Assessment Questionnaire A*. 2025.

[241] PCI Security Standards Council. *How does an e-commerce merchant meet the SAQ A eligibility criteria for scripts?* 2025.

[242] PCI Security Standards Council. *Why is SAQ A-EP used for Direct Post while SAQ A is used for iFrame or URL redirect?* 2015.

[243] PCI Security Standards Council. *If a merchant's e-commerce implementation meets the criteria that all elements of payment pages originate from a PCI DSS compliant service provider, is the merchant eligible to complete SAQ A or SAQ A-EP?* 2014.

[244] PCI Security Standards Council. *Self-Assessment Questionnaire (SAQ) Instructions and Guidelines*. 2024.

[245] PCI Security Standards Council. *Is a merchant website still in scope for PCI DSS if it meets all the criteria for SAQ A?* 2015.

[246] PCI Security Standards Council. *What is the intent of the SAQ eligibility criteria?* 2016.

[247] PCI Security Standards Council. *What is SAQ C-VT?* 2013.

[248] Visa. *Validation of Compliance: Merchant Levels*. 2026.

[249] Росстандарт. *ГОСТ Р 57580.2–2018 «Методика оценки соответствия»*. 2018.

[250] Коммерсантъ. *На оплату стикером без ввода PIN-кода установлен лимит в 3 тыс. руб.* 2023.

[251] TAdviser. *НСПК и «Инфосистемы Джет» разработали систему клиринга для платёжной системы «Мир»*. 2016.

[252] U.S. Department of the Treasury. *On Second Anniversary of Russia's Further Invasion of Ukraine and Following the Death of Aleksey Navalny, Treasury Sanctions Hundreds of Targets in Russia and Globally*. 2024.

[253] Lifecycle Integrity. *Contactless EMV cards content examples and timing samples*. 2023.

[254] EMVCo. *EMV Contactless Book B «Entry Point Specification»*. 2024.

[255] nexo standards. *nexo standards adds Mir and PURE to its globally adopted payment acceptance specification*. 2021.

[256] НСПК. *Mir Payment System Contactless Terminal Kernel Specification*. 2023.

[257] Банковское обозрение. *Больше, чем эквайринг*. 2019.

[258] ComNews. *Российский банк — мировой лидер по эквайрингу*. 2025.

[259] CNews. *НСПК — ОПКЦ: процессинг операционного платёжного и клирингового центра*. 2024.

[260] WonderNetwork. *Ping time between Moscow and other cities*. 2026.

[261] Denis Dubo-Chevalier. *How we ensure a fast response time for card authorization*. 2022.

[262] nexo standards. *About us*. 2019.

[263] nexo standards. *nexo Retailer Protocol*. 2024.

[264] *Федеральный закон от 22.05.2003 № 54-ФЗ «О применении контрольно-кассовой техники»*.

[265] Т-Банк. *Как оплатить проезд в транспорте и пополнить проездной*. 2026.

[266] NFCW. *Apple Pay and Google Pay suspend contactless mobile payments for Mir cardholders in Russia*. 2022.

[267] Хабр. *Сервис бесконтактной оплаты SberPay NFC снова работает на устройствах с Android*. 2022.

[268] Т-Банк. *Оплата телефоном с T-Pay: NFC-оплата для Android-смартфонов*. 2026.

[269] Visa. *Visa Suspends All Russia Operations*. 2022.

[270] Банк России. *All payment cards issued by Russian banks continue to operate as normal*. 2022.

[271] Visa. *Form 10-K for fiscal year ended September 30, 2023: Note 1 Summary of Significant Accounting Policies; Note 12 Settlement Guarantee Management*. 2023.

[272] Visa. *Form 10-K for fiscal year ended September 30, 2017*. 2017.

[273] Visa Canada. *VisaNet Disclosure: Bank of Canada Prominent Payment System Risk-Management Standards*. 2025.

[274] Mastercard. *Form 10-Q: Settlement and Other Risk Management*. 2024.

[275] Lynne Marek. *Visa, Mastercard depict bank failure impact*. 2023.

[276] НСПК. *Правила платёжной системы «Мир». Приложение 3. Методика определения размера гарантийного обеспечения Участника*. 2025.

[277] Visa. *Visa Merchant Business News Digest*. 2026.

[278] Visa. *Visa Direct Documentation*. 2026.

[279] Visa. *Visa Direct: How To*. 2025.

[280] Visa Acceptance Solutions. *Service Features: Capture and the TC 33.A file*. 2025.

[281] Visa. *Visa Prevents Approximately $25 Billion in Fraud Using Artificial Intelligence*. 2019.

[282] Mastercard. *Mastercard statement on suspension of Russian operations*. 2022.

[283] Mastercard. *Mastercard Switching explained*. 2026.

[284] U.S. Payments Forum. *Payment Network Host and Level 3 Requirements*. 2023.

[285] Susan Pandy, Marianne Crowe и Brian Russell. *Understanding the Role of Host Card Emulation in Mobile Wallets*. 2016.

[286] Mastercard. *Mastercard and AptPay speed disbursements across multiple industries*. 2020.

[287] Mastercard. *Mastercard Automatic Billing Updater Merchant External Summary*. 2020.

[288] Wind River Payments. *April 2026 Interchange and Network Fee Updates*. 2026.

[289] Fiserv. *June 2026 Card Brand Updates*. 2026.

[290] CNews. *НСПК и MasterCard договорились о переводе транзакций по картам MasterCard на процессинг НСПК*. 2015.

[291] Взгляд. *Visa перевела процессинг всех российских транзакций в НСПК*. 2015.

[292] НСПК. *Платежной системе «Мир» исполнилось 10 лет: от «пластика» до биометрии*. 2025.

[293] Российская Федерация. *Закон РФ от 07.02.1992 № 2300-1 «О защите прав потребителей»*. 1992.

[294] Банк России. *Национальная платёжная система: вопросы и ответы*. 2026.

[295] НСПК. *Кобейджинговая программа Мир–JCB*. 2015.

[296] JCB. *JCB Statement on Suspension of Russian Operations*. 2022.

[297] EFTlab. *Complete List of Registered Application Provider Identifiers (RID)*. 2024.

[298] Платёжная система Мир. *Mir Pay: помощь*. 2026.

[299] НСПК. *MirAccept: технология аутентификации держателя карты Мир при операциях без присутствия карты*. 2026.

[300] НСПК. *Правила и тарифы платёжной системы «Мир»: страница для участников*. 2026.

[301] НСПК. *Стандарт платёжной системы «Мир». Межбанковские вознаграждения в платёжной системе «Мир». Версия 2.11 (П.148)*. 2026.

[302] НСПК. *Правила платёжной системы «Мир». Приложение 4. Тарифы. Часть 1. Для Российских участников. Версия 4.14 (П.223)*. 2025.

[303] Правительство Российской Федерации. *Программа возмещения малому и среднему бизнесу комиссии при оплате через СБП (2021–2022)*. 2022.

[304] Федеральное Собрание Российской Федерации. *Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ*. 2001.

[305] Росстандарт. *Р 1323565.1.007–2017 «Использование алгоритмов блочного шифрования при формировании проверочного параметра платёжной карты и проверочного значения PIN»*. 2017.

[306] UnionPay International. *Introduction*. 2026.

[307] ООО «ЮнионПэй». *Правила Платёжной системы UnionPay в России. Редакция № 14 от 26.12.2025*. 2025.

[308] IHG Hotels & Resorts. *IHG Partners with China UnionPay, Pioneering a New Era of Digital Payments in the Hotel Industry*. 2024.

[309] UnionPay International. *Mobile Payment (UnionPay Mobile QuickPass)*. 2026.

[310] UnionPay International. *The List Of Recommended QuickPass Merchants*. 2026.

[311] UnionPay International. *Interchange Rate Fees*. 2025.

[312] EMVCo. *UnionPay 3-D Secure Version 2.1.0*. 2021.

[313] UnionPay International. *SecurePlus*. 2024.

[314] Mastercard. *Dynamic Currency Conversion (DCC) Performance Guide, Merchant Version*. 2025.

[315] UnionPay International. *UnionPay International and NSPK jointly issue the first UnionPay-MIR Debit Card*. 2017.

[316] Office of Foreign Assets Control. *Sanctions List Service*. 2026.

[317] The White House. *Executive Order 14114: taking additional steps with respect to the Russian Federation's harmful activities*. 2023.

[318] OFAC. *Updated Guidance for Foreign Financial Institutions on OFAC Sanctions Authorities Targeting Support to Russia's Military-Industrial Base*. 2024.

[319] Office of Foreign Assets Control. *A Framework for OFAC Compliance Commitments*. 2019.

[320] OFAC. *Who must comply with OFAC regulations?* 2026.

[321] UnionPay International. *Cross-border Remittance (UnionPay MoneyExpress)*. 2026.

[322] ISO. *ISO 3166-1:2020 «Country codes»*. 2020.

[323] Белкарт. *О Белкарт*. 2026.

[324] Adyen. *Debit Mastercard is replacing Maestro: what you need to know*. 2023.

[325] Белкарт. *Карточки БЕЛКАРТ: виды, их возможности и использование*. 2026.

[326] Onlíner. *В каких банках оформляют карту «Белкарт-Мир» и зачем она может вам понадобиться*. 2022.

[327] ArCa. *О нас*. 2024.

[328] HUMO. *FAQ*. 2026.

[329] UZCARD. *UZCARD и UnionPay развивают партнёрство*. 2025.

[330] Газета.uz. *Взаимная интеграция банкоматов Humo и Uzcard в Узбекистане завершится до мая*. 2023.

[331] Газета.uz. *Интеграция банкоматов Uzcard и Humo завершена*. 2023.

[332] HUMO. *Bankomatlar bo'yicha rasmiy xabar*. 2023.

[333] Элкарт. *Национальная платежная система Элкарт*. 2026.

[334] Межбанковский процессинговый центр. *Информация о компании*. 2026.

[335] Interfax. *В Киргизии с 5 апреля прекратят обслуживать карты «Мир»*. 2024.

[336] Banks.az. *Azericard*. 2026.

[337] MilliKart. *About MilliKart*. 2025.

[338] The Paypers. *AzeriCard integrates Apple Pay and Google Pay with Akurateco's expertise*. 2024.

[339] Oninvest. *On July 19, Kazakhstan is launching a unified QR code payment system*. 2026.

[340] Kaspi.kz. *Payments Platform*. 2025.

[341] National Bank of Kazakhstan. *Statistics of payment cards*. 2024.

[342] Bloomberg. *Kazakh firm Kaspi.kz opens payment system to new users to compete with central bank*. 2024.

[343] TASS. *International acceptance of Mir cards grows despite sanctions — Bank of Russia*. 2025.

[344] Central Banking. *Iran launches second phase of payments link with Russia*. 2025.

[345] Finport.am. *Armenian Card to start issuing co-branded cards with MasterCard and Union Pay international payment systems*. 2025.

[346] НСПК. *Часто задаваемые вопросы о Системе быстрых платежей*. 2026.

[347] Банк России. *Порядок действий кредитных организаций (филиалов) для начала использования сервиса быстрых платежей (СБП) платёжной системы Банка России*. 2026.

[348] НСПК. *Вопросы и ответы для бизнеса о Системе быстрых платежей*. 2026.

[349] НСПК. *Приложение СБПэй*. 2026.

[350] *Федеральный закон от 24.07.2023 № 369-ФЗ «О защите клиентов от переводов без согласия»*.

[351] *Федеральный закон от 07.08.2001 № 115-ФЗ «О ПОД/ФТ»*.

[352] НСПК. *Часто задаваемые вопросы по переводам в Системе быстрых платежей*. 2026.

[353] Монета. *Протокол C2C. Сценарий Me2Me Pull*. 2026.

[354] Монета. *Описание полей для переводов СБП*. 2026.

[355] Ozon. *Как выбрать склад для торговли на Ozon*. 2024.

[356] Яндекс Маркет. *Модель работы на маркетплейсе: что это такое и какие модели существуют*. 2025.

[357] Банк России. *СБП: основные показатели, III квартал 2025 года*. 2025.

[358] НСПК. *Российский экспортный центр и ВТБ запустили сервис B2B-платежей через СБП*. 2024.

[359] НСПК. *Система быстрых платежей: оплата по QR, NFC, ссылке и с привязанного счёта*. 2026.

[360] НСПК. *Универсальный QR-код*. 2026.

[361] *Федеральный закон от 23.07.2025 № 248-ФЗ «О поэтапном внедрении цифрового рубля»*.

[362] Банк России. *Массовое внедрение цифрового рубля начнётся 1 сентября 2026 года*. 2025.

[363] НСПК. *Подписка СБП*. 2026.

[364] НСПК. *OpenAPI операционного клирингового центра СБП*. 2026.

[365] НСПК. *Правила оказания операционных услуг и услуг платежного клиринга в СБП*. 2026.

[366] Банк России. *Когда банк обязан приостановить перевод на два дня, даже несмотря на согласие клиента?* 2026.

[367] Банк России. *Информация о решении Совета директоров Банка России о ставках (тарифах) межбанковских вознаграждений и максимальных значениях размера платы в сервисе быстрых платежей*. 2023.

[368] Банк России. *Правила Системы быстрых платежей*. 2026.

[369] Банк России. *Цифровой рубль*. 2025.

[370] Banco Central do Brasil. *Pix*. 2025.

[371] Banco Central do Brasil. *Participantes do Pix*. 2026.

[372] Banco Central do Brasil. *Instant Payment System (SPI)*. 2025.

[373] Banco Central do Brasil. *Manual de Padrões para Iniciação do Pix*. 2025.

[374] Banco Central do Brasil. *Pix FAQ*. 2026.

[375] Banco Central do Brasil. *Manual de Tempos do Pix*. 2025.

[376] Banco Central do Brasil. *Manual de Segurança do Pix*. 2025.

[377] Banco Central do Brasil. *Manual de Fluxos do Processo de Efetivação do Pix*. 2025.

[378] Banco Central do Brasil. *Aprimoramentos no Mecanismo Especial de Devolução — MED 2.0*. 2025.

[379] NPCI. *Unified Payments Interface (UPI) — product overview*. 2024.

[380] NPCI. *Guidelines on volume cap for Third-Party App Providers (TPAPs) in UPI (UPI-OC No. 159)*. 2022.

[381] MediaNama. *NPCI Extends UPI Market Share Cap Deadline to 2026, Giving Google and PhonePe a Two-Year Relief*. 2025.

[382] NPCI. *Guidelines on usage of UPI APIs (UPI-OC No. 215-A FY 2025–26)*. 2025.

[383] NPCI. *UPI Circulars*. 2025.

[384] Board of Governors of the Federal Reserve System. *FedNow Service*. 2025.

[385] Federal Reserve Financial Services. *FedNow Service Resources*. 2025.

[386] U.S. Government. *12 CFR Part 210 Subpart C – Funds Transfers Through the FedNow Service*. 2025.

[387] Federal Reserve Banks. *Operating Circular No. 8 – Funds Transfers Through the FedNow Service*. 2026.

[388] Federal Reserve Banks. *FedNow Service Operating Procedures*. Вер. 3.2. 2025.

[389] Federal Reserve Financial Services. *FedNow Readiness Guide: ISO 20022 Messages Overview*. 2025.

[390] Federal Reserve Financial Services. *The FedNow Service Technical Overview and Planning Guide*. 2025.

[391] Federal Reserve Financial Services. *FedNow Readiness Guide: Managing Liquidity in an Instant Payments World*. 2020.

[392] European Payments Council. *2025 SEPA Instant Credit Transfer Rulebook (Version 1.1)*. 2025.

[393] European Central Bank. *TARGET Instant Payment Settlement (TIPS) – User Detailed Functional Specifications, v4.0.0*. 2023.

[394] European Parliament and Council. *Regulation (EU) 2024/886 (Instant Payments Regulation)*. 2024.

[395] European Central Bank. *Instant Payments Regulation (IPR)*. 2025.

[396] European Payments Council. *Verification Of Payee Scheme Rulebook*. 2025.

[397] Banco Central do Brasil. *Resolution BCB 1 of August 12, 2020 (Pix Regulation)*. 2020.

[398] Open Banking Limited. *Reference — Open Banking Standards*. 2026.

[399] Berlin Group. *PSD2 Access to Bank Accounts*. 2025.

[400] Open Banking Limited. *Payment Initiation API Profile — v3.1.11*. 2026.

[401] Open Banking Limited. *Variable Recurring Payments API Profile — v4.0.1*. 2026.

[402] Open Banking Limited. *Account Access Consents — v3.1.11*. 2026.

[403] Open Banking Implementation Entity (UK). *Read/Write API, Account and Transaction API Profile, v3.1.10*. 2023.

[404] Open Banking Limited. *Domestic Payments Consents — v3.1.11*. 2026.

[405] Open Banking Limited. *Authentication Methods — Open Banking Standards*. 2026.

[406] Plaid. *Plaid: financial data network*. 2026.

[407] U.S. Department of Justice, Antitrust Division. *Visa and Plaid Abandon Merger After Antitrust Division's Suit to Block*. 2021.

[408] TrueLayer. *Open banking payments and data*. 2026.

[409] Visa. *Visa Completes Acquisition of Tink*. 2022.

[410] Yodlee. *Yodlee: financial data aggregation platform*. 2026.

[411] Банк России. *Открытые API*. 2026.

[412] Ассоциация ФинТех (АФТ). *Стандарты открытых API российского финансового рынка*. 2026.

[413] Банк России. *Концепция внедрения открытых API в Российской Федерации*. 2022.

[414] Ассоциация ФинТех. *Банк России опубликовал стандарты Открытых API, разработанные на площадке Ассоциации ФинТех*. 2025.

[415] Банк России. *СТО БР ФАПИ.СЕК-1.6-2024 «Безопасность финансовых API через OpenID Connect»*. 2024.

[416] IETF. *RFC 9101: The OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR)*. 2021.

[417] N. Sakimura, J. Bradley и N. Agarwal. *RFC 7636: Proof Key for Code Exchange by OAuth Public Clients*. 2015.

[418] OpenID Foundation. *Financial-grade API Security Profile 1.0 — Part 2: Advanced*. 2021.

[419] IETF. *RFC 9126: OAuth 2.0 Pushed Authorization Requests (PAR)*. 2021.

[420] IETF. *RFC 9449: OAuth 2.0 Demonstrating Proof of Possession (DPoP)*. 2023.

[421] OpenID Foundation. *FAPI 2.0 Security Profile*. 2025.

[422] OpenID Foundation. *FAPI 2.0 Message Signing*. 2025.

[423] Банк России. *СТО БР ФАПИ.СЕК-1.6-2024 «Безопасность финансовых API через OpenID Connect»*. 2024.

[424] OpenID Foundation. *Financial-grade API Security Profile 1.0 — Part 1: Baseline*. 2021.

[425] OpenID Foundation. *JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)*. 2022.

[426] ТК 26. *МР 26.2.002-2024 «Российские криптоалгоритмы в OpenID Connect»*. 2024.

[427] Банк России. *СТО БР ФАПИ.ПАОК-1.0-2024 «Профиль CIBA для российских открытых API»*. 2024.

[428] Банк России. *Приказ от 19.12.2025 № ОД-2892 «О введении стандарта согласия на доступ к счетам физлиц»*. Вер. 2.0.0. 2025.

[429] Банк России. *Приказ от 19.12.2025 № ОД-2895 «О введении стандарта согласия на доступ к счетам юрлиц»*. Вер. 2.0.0. 2025.

[430] Банк России. *Основные принципы и этапы внедрения Открытых API на финансовом рынке*. 2024.

[431] Банк России. *Банк России обновил комплекс стандартов Открытых API*. 2025.

[432] Ассоциация ФинТех. *Открытый банкинг России. Спецификации Открытых программных интерфейсов*. 2026.

[433] Банк России. *Приказ от 19.12.2025 № ОД-2887 «О введении общих положений и глоссария СТО БР по открытым API»*. 2025.

[434] Банк России. *Приказ от 19.12.2025 № ОД-2894 «О введении стандарта доступа к информации о счетах физлиц»*. Вер. 2.0.0. 2025.

[435] Банк России. *Стандарт «Открытые банковские интерфейсы. Инициирование перевода денежных средств клиента третьей стороной в валюте Российской Федерации»*. Вер. 1.2.1. 2020.

[436] ISO 20022 Registration Authority. *ISO 20022 «Financial services messaging»*. 2026.

[437] ISO 20022 Registration Authority. *ISO 20022 Business Areas*. 2025.

[438] Банк России. *Основные документы: ISO 20022 для платежной системы Банка России*. 2025.

[439] Банк России. *Система передачи финансовых сообщений: обмен сообщениями ISO 20022 в СПФС*. 2026.

[440] European Central Bank. *What are instant payments?* 2025.

[441] OXXO. *OXXO PAY — Negocios*. 2026.

[442] EMVCo. *EMV QRCPS «Merchant-Presented Mode»*. Вер. 1.1. 2020.

[443] EMVCo. *EMV QRCPS «Consumer-Presented Mode»*. Вер. 1.1. 2020.

[444] Банк России. *Что делать человеку, если он при переводе денег ошибся в реквизитах? Можно ли вернуть деньги?* 2026.

[445] Ant International. *Merchant-presented Mode Payment*. 2026.

[446] WeChat Pay. *WeChat Pay: оплата по платёжному коду, правила проверки пароля*. 2026.

[447] Ant International. *Alipay+ Mobile Payment Providers*. 2026.

[448] Banco Central do Brasil. *Relatório de Gestão do Pix: concepção e primeiros anos de funcionamento*. 2023.

[449] ПАО Сбербанк. *SberPay – платёжный сервис Сбербанка*. 2026.

[450] АО Т-Банк. *T-Pay (ранее Tinkoff Pay): платёжный сервис Т-Банка*. 2026.

[451] Альфа-Банк. *Alfa Pay от Альфа-Банка позволяет оплачивать покупки офлайн*. 2025.

[452] Банковское обозрение. *Альфа-Банк предоставил доступ к оплате iPhone в новом приложении*. 2025.

[453] ООО Яндекс.Пэй. *Yandex Pay – платёжный сервис Яндекса*. 2026.

[454] Яндекс. *Сплит – оплата частями от Яндекс Пэй*. 2026.

[455] ООО НКО «ЮМани». *ЮKassa – сервис приёма платежей для бизнеса*. 2026.

[456] ООО НКО «ЮМани». *ЮMoney – электронный кошелёк*. 2026.

[457] НСПК. *Биоэквайринг и оплата по лицу через Единую биометрическую систему*. 2026.

[458] АО «Центр биометрических технологий». *Единая биометрическая система (ЕБС)*. 2026.

[459] Банк России. *Итоги работы Банка России 2024: коротко о главном. Развитие системы платежей и расчетов*. 2025.

[460] Правительство Москвы. *Систему Face Pay для оплаты проезда запустили на всех станциях метро*. 2021.

[461] National Bank of Kazakhstan. *Version №257 от 27/02/2025 | Statistics of payment cards*. 2025.

[462] UZCARD. *UZCARD has changed its legal form*. 2024.

[463] National Bank of Kazakhstan. *Запуск в промышленную эксплуатацию Межбанковской системы платёжных карточек (МСПК)*. 2022.

[464] БИЗНЕС Online. *В РФ подтвердили, что банки-участники Armenian Card прекращают обслуживать карты «Мир»*. 2024.

[465] Банк России. *Основные направления развития национальной платёжной системы на 2025–2027 годы*. 2024.

[466] Klarna. *Settlement reports overview*. 2026.

[467] Т-Банк. *Долями: документация API*. 2026.

[468] Merchant Risk Council. *Boosting Authorization Success: A Practical Guide to Visa NTI and Mastercard Trace ID Mandates*. 2025.

[469] Visa. *Visa Installment Solutions*. 2026.

[470] Mastercard. *Mastercard Installments for BNPL*. 2026.

[471] CBS News. *Apple discontinues its buy now, pay later service in the U.S.* 2024.

[472] Apple. *New features come to Apple services this fall*. 2024.

[473] TechCrunch. *Klarna Confirms 800M USD Raise as Valuation Drops 85% to 6.7B USD*. 2022.

[474] Klarna Group plc. *Klarna completes initial public offering*. 2025.

[475] Precedence Research. *Buy Now Pay Later Market Size and Forecast*. 2025.

[476] Consumer Financial Protection Bureau. *The Buy Now, Pay Later Market: Data Spotlight*. 2025.

[477] PYMNTS. *BNPL Company Affirm Completes $264 Million PayBright Deal*. 2021.

[478] PayPal. *About Us: PayPal (Europe) S.à r.l. et Cie, S.C.A.* 2026.

[479] FDIC. *FDIC Approves the Deposit Insurance Application for Square Financial Services, Inc., Salt Lake City, Utah*. 2020.

[480] Saudi Central Bank. *SAMA licenses Tabby Finance to operate buy-now-pay-later services*. 2025.

[481] Tabby. *Tabby secures wallet licence in the UAE*. 2026.

[482] Т-Банк. *Долями – сервис рассрочки от Т-Банка*. 2026.

[483] Т-Банк. *Долями для бизнеса – подключение сервиса рассрочки*. 2026.

[484] ООО «А-Четыре Технологии». *Подели – сервис оплаты покупок по частям*. 2026.

[485] ООО «А-Четыре Технологии». *Подели для бизнеса*. 2026.

[486] ООО «Центр новых финансовых сервисов». *Плати частями*. 2026.

[487] Банк России. *Реестр операторов сервиса рассрочки*. 2026.

[488] *Федеральный закон от 31.07.2025 № 283-ФЗ «О деятельности по предоставлению сервиса рассрочки»*.

[489] Банк России. *Операторы сервиса рассрочки*. 2026.

[490] Банк России. *Указание от 12.01.2026 № 7274-У «О ведении Банком России реестра операторов сервиса рассрочки»*. 2026.

[491] Банк России. *Указание от 12.01.2026 № 7276-У «О порядке внесения сведений в реестр ОСР и перечне документов»*. 2026.

[492] European Parliament and Council. *Directive (EU) 2023/2225 on credit agreements for consumers (Consumer Credit Directive)*. 2023.

[493] Consumer Financial Protection Bureau. *Truth in Lending (Regulation Z); use of digital user accounts to access buy now, pay later loans*. 2024.

[494] Consumer Financial Protection Bureau. *Interpretive Rules, Policy Statements, and Advisory Opinions; Withdrawal*. 2025.

[495] HM Treasury. *Regulation of Buy-Now Pay-Later: government response and consultation*. 2025.

[496] FCA. *Regulating Buy Now Pay Later (BNPL)*. 2026.

[497] Australian Government, the Treasury. *Treasury Laws Amendment (Responsible Buy Now Pay Later and Other Measures) Act 2024*. 2024.

[498] Raphael Auer, Giulio Cornelli и Jon Frost. *Rise of the central bank digital currencies: drivers, approaches and technologies*. 2020.

[499] *Бюджетный кодекс Российской Федерации*.

[500] Банк России. *Положение от 07.12.2023 № 833-П «О защите информации для участников платформы цифрового рубля»*. 2023.

[501] Банк России. *Цифровой рубль: текущий статус проекта*. 2025.

[502] Банк России. *Реестр кредитных организаций, признанных Банком России значимыми на рынке платёжных услуг*. 2026.

[503] Банк России. *Решение Совета директоров от 28.08.2026 «Об определении тарифов на услуги оператора платформы цифрового рубля и размера вознаграждения участникам платформы»*. 2026.

[504] Банк России. *Концепция цифрового рубля*. 2021.

[505] Банк России. *Стандарт платформы цифрового рубля «Порядок подключения участника платформы к платформе цифрового рубля». Версия 2.0*. 2026.

[506] Банк России. *Стандарт платформы цифрового рубля «Требования операционно-технологического взаимодействия на платформе цифрового рубля». Версия 5.0*. 2026.

[507] Etherscan. *Ethereum Daily Transactions Chart*. 2026.

[508] Working Group on E-CNY Research and Development of the People's Bank of China. *Progress of Research & Development of E-CNY in China*. 2021.

[509] Минфин России. *Проведены первые платежи цифровым рублем*. 2025.

[510] Банк России. *Концепция платформы коммерческих смарт-контрактов*. 2026.

[511] Банк России. *Thousands of payments per second: Bank of Russia statistics*. 2025.

[512] Газпромбанк. *Газпромбанк продемонстрировал прототипы смарт-контрактов на платформе цифрового рубля*. 2025.

[513] Atlantic Council. *Central Bank Digital Currency Tracker*. 2026.

[514] The State Council of the People's Republic of China. *China to enhance digital yuan management with deposit features starting 2026*. 2025.

[515] European Central Bank. *Eurosystem moving to next phase of digital euro project*. 2025.

[516] European Central Bank. *Preparation phase of a digital euro — Closing report*. 2025.

[517] Bank of England. *Progress update: Digital Pound design phase*. 2025.

[518] Bank of England. *The digital pound*. 2026.

[519] The White House. *Executive Order: Strengthening American leadership in digital financial technology*. 2025.

[520] Federal Reserve Bank of New York. *Project Cedar*. 2023.

[521] U.S. House of Representatives. *Anti-CBDC Surveillance State Act (H.R. 1919)*. 2025.

[522] Bank for International Settlements. *Project mBridge reaches minimum viable product stage*. 2024.

[523] Seoul Economic Daily. *Saudi Arabia Exits China-Led Digital Currency Platform*. 2026.

[524] Bank for International Settlements. *Project Agorá: bringing tokenised commercial bank deposits and tokenised wholesale central bank money on the same unified ledger*. 2025.

[525] Bank for International Settlements. *Project Agorá shows how tokenisation can improve wholesale cross-border payments; work will advance to real-value testing*. 2026.

[526] Eastern Caribbean Central Bank. *DCash pilot ends after 34 months*. 2024.

[527] Eastern Caribbean Central Bank. *DCash 2.0: vendor request for information*. 2025.

[528] Digital Pound Foundation. *Eastern Caribbean Central Bank Seeking Technology Partners for DCash 2.0 CBDC Project*. 2023.

[529] Eastern Caribbean Central Bank. *Communique of the 112th Meeting of the ECCB Monetary Council*. 2026.

[530] ECB. *ECB Commits to Distributed Ledger Technology Settlement Plans with Dual-Track Strategy: Pontes and Appia*. 2025.

[531] Банк России. *Положение от 13.01.2025 № 850-П «Об операционной надёжности»*. 2025.

[532] Банк России. *Положение от 29.06.2021 № 762-П «О правилах перевода денежных средств»*. 2021.

[533] Банк России. *Указание от 27.06.2023 № 6470-У «О формах и сроках отчётности операторов платёжной системы и перевода денежных средств»*. 2023.

[534] Банк России. *Указание от 10.04.2023 № 6406-У «О формах отчётности кредитных организаций»*. 2023.

[535] Правительство Российской Федерации. *Постановление от 26.06.1995 № 608 «О сертификации средств защиты информации»*. 1995.

[536] Росстандарт. *ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности»*. 2013.

[537] *Федеральный закон от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации»*.

[538] Банк России. *Положение от 24.12.2004 № 266-П «Об эмиссии платёжных карт»*. 2004.

[539] *Федеральный закон от 03.06.2009 № 103-ФЗ «О деятельности по приёму платежей физических лиц, осуществляемой платёжными агентами»*.

[540] *Закон Российской Федерации от 02.12.1990 № 395-1 «О банках и банковской деятельности»*.

[541] Банк России. *Отозвана лицензия на осуществление банковских операций у КИВИ Банк (АО)*. 2024.

[542] Банк России. *Реестр операторов по приёму платежей*. 2024.

[543] РБК. *НСПК установила комиссии для банков по картам ушедших Visa и Mastercard*. 2022.

[544] Interfax. *НСПК обяжет банки участвовать в системе оспаривания операций в СБП с 30 июня*. 2023.

[545] Банк России. *Приказ от 05.11.2025 № ОД-2506 «О признаках перевода без согласия клиента»*. 2025.

[546] Банк России. *Положение от 15.10.2015 № 499-П «Об идентификации клиентов в целях ПОД/ФТ»*. 2015.

[547] Банк России. *Вопросы и ответы: банковский сектор*. 2025.

[548] FATF. *FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)*. 2013.

[549] Правительство Российской Федерации. *Постановление от 28.11.2011 № 977 «О ЕСИА (Единая система идентификации и аутентификации)»*. 2011.

[550] Т-Банк. *T-ID: единый вход в приложения и на сайты партнёров*. 2026.

[551] *Федеральный закон от 29.12.2022 № 572-ФЗ «Об идентификации и аутентификации по биометрическим персональным данным»*.

[552] *Федеральный закон от 31.12.2017 № 482-ФЗ «Об удалённой идентификации по биометрии»*.

[553] Центр биометрических технологий. *Приложение «Госуслуги Биометрия»*. 2026.

[554] Российская газета. *Упрощённая, стандартная и подтверждённая биометрия: отличия*. 2024.

[555] Центр биометрических технологий. *Регистрация подтверждённой биометрии*. 2026.

[556] Центр биометрических технологий. *Открытие счёта физического лица по биометрии*. 2026.

[557] Президент Российской Федерации. *Указ Президента Российской Федерации от 30.09.2022 № 693 «Об определении организации, обеспечивающей развитие цифровых технологий идентификации и аутентификации»*. 2022.

[558] *Федеральный закон от 01.04.2025 № 41-ФЗ «О создании ГИС противодействия правонарушениям с использованием ИКТ»*.

[559] UIDAI. *Aadhaar Authentication*. 2026.

[560] e-Estonia. *ID-card*. 2026.

[561] ISO/IEC. *ISO/IEC 30107-3:2023 «Biometric presentation attack detection»*. 2023.

[562] CEN-CENELEC. *CEN/TS 18099: Biometric data injection attack detection*. 2024.

[563] NIST. *Digital Identity Guidelines (SP 800-63-4)*. 2025.

[564] Biometric Update. *Deepfake-as-a-Service revolutionizing biometrics spoofing and identity fraud: report*. 2026.

[565] European Parliament and Council. *Regulation (EU) 2024/1183 on the European Digital Identity (eIDAS 2.0)*. 2024.

[566] European Commission. *European Digital Identity Architecture and Reference Framework (ARF)*. 2025.

[567] Банк России. *Что такое платформа «Знай своего клиента»*. 2026.

[568] Банк России. *Открытие общего доступа к сервису «Знай своего клиента»*. 2024.

[569] Sumsub. *KYC, KYB, AML & transaction monitoring platform*. 2026.

[570] ComplyAdvantage. *AI-driven AML & financial crime detection*. 2026.

[571] FATF. *Targeted update on implementation of the FATF standards on virtual assets and VASPs*. 2025.

[572] UK Government. *The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, regulation 64C*. 2017.

[573] European Banking Authority. *Guidelines on Travel Rule under Regulation (EU) 2023/1113*. 2024.

[574] FATF. *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. 2025.

[575] Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ). *О ЕАГ: миссия, страны-члены, региональная FATF-style body*. 2026.

[576] Росфинмониторинг. *Приказ от 26.01.2026 № 13 «О порогах обязательного контроля сделок с недвижимостью»*. 2026.

[577] Банк России. *Положение от 18.06.2025 № 860-П «О требованиях к ПВК в целях ПОД/ФТ»*. 2025.

[578] Банк России. *Указание от 17.06.2025 № 7081-У «О представлении кредитными организациями сведений в Росфинмониторинг»*. 2025.

[579] Росфинмониторинг. *Приказ от 08.02.2022 № 18 «О представлении в Росфинмониторинг информации по 115-ФЗ»*. 2022.

[580] FATF. *Guidance for a Risk-Based Approach: The Banking Sector*. 2014.

[581] Банк России. *Методические рекомендации от 21.07.2017 № 19-МР «О снятии наличных по корпоративным картам юрлиц и ИП»*. 2017.

[582] Банк России. *Методические рекомендации от 21.07.2017 № 18-МР «О подходах к управлению риском ПОД/ФТ»*. 2017.

[583] Банк России. *Методические рекомендации от 29.02.2024 № 4-МР «Об усилении контроля за операциями физических лиц»*. 2024.

[584] Bruno Deprez и др. *GARG-AML against Smurfing: A Scalable and Interpretable Graph-Based Framework for Anti-Money Laundering*. 2025.

[585] U.S. Congress. *31 U.S.C. 5324: Structuring transactions to evade reporting requirement prohibited*. 1986.

[586] NICE Actimize. *Silencing the Noise: Effective Strategies for Reducing False Positives in Transaction Monitoring*. 2024.

[587] Ahmad Naser Eddin и др. *Anti-Money Laundering Alert Optimization Using Machine Learning with Graphs*. 2022.

[588] FATF. *High-risk and other monitored jurisdictions*. 2026.

[589] FATF. *FATF Statement on the Russian Federation*. 2023.

[590] Евразийская группа (ЕАГ). *Взаимные оценки государств-членов ЕАГ*. 2026.

[591] FATF. *Guidance on Correspondent Banking*. 2016.

[592] Chainalysis. *Blockchain data platform for compliance and investigation*. 2026.

[593] TRM Labs. *TRM Labs Announces $70M Series C to Scale AI Solutions to Disrupt Criminal Networks and Counter National Security Threats*. 2026.

[594] European Parliament and Council. *Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets*. 2023.

[595] European Parliament and Council. *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)*. 2023.

[596] U.S. Department of the Treasury. *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*. 2022.

[597] Росфинмониторинг. *Перечень организаций и физических лиц, в отношении которых имеются сведения о причастности к экстремистской деятельности или терроризму*. 2026.

[598] Межведомственная комиссия по противодействию финансированию терроризма. *Решения Межведомственной комиссии о замораживании (блокировании) денежных средств или иного имущества*. 2026.

[599] Directorate-General for Financial Stability, Financial Services and Capital Markets Union. *Consolidated list of persons, groups and entities subject to EU financial sanctions*. 2026.

[600] United Nations Security Council. *United Nations Security Council Consolidated List*. 2026.

[601] Office of Foreign Assets Control. *Treasury disrupts Russia's sanctions evasion schemes (Keremet Bank designation)*. 2025.

[602] Акчабар. *Последствия санкций? «Керемет Банк» потерял свыше 40 % клиентских средств*. 2025.

[603] Коммерсантъ. *Турецкие банки отказываются работать с российскими*. 2024.

[604] Council of the European Union. *Council Regulation (EC) No 2580/2001 on combating terrorism*. 2001.

[605] Foreign, Commonwealth and Development Office. *UK Sanctions List*. 2026.

[606] Foreign, Commonwealth and Development Office. *Moving to a single list for UK sanctions designations: 28 January 2026*. 2026.

[607] Department of Foreign Affairs and Trade. *Consolidated List of persons and entities subject to Australian sanctions*. 2026.

[608] AUSTRAC. *Persons designated for targeted financial sanctions (Reform)*. 2026.

[609] Norton Rose Fulbright. *Australia's AML/CTF Reforms: A New Era in Financial Crime Prevention*. 2025.

[610] Monetary Authority of Singapore. *Targeted Financial Sanctions: Lists of Designated Individuals and Entities*. 2026.

[611] The White House. *Executive Order 13662: blocking property of additional persons contributing to the situation in Ukraine*. 2014.

[612] U.S. Department of the Treasury. *Sectoral Sanctions Identifications (SSI) List*. 2025.

[613] Office of Foreign Assets Control. *OFAC 50 % Rule guidance*. 2014.

[614] U.S. Bureau of Industry and Security. *One Year Suspension of Expansion of End-User Controls for Affiliates of Certain Listed Entities*. 2025.

[615] Council of the European Union. *Council Regulation (EU) 2022/345 amending Regulation (EU) 833/2014 (SWIFT disconnection)*. 2022.

[616] Council of the European Union. *Russia's war of aggression against Ukraine: comprehensive EU's 14th package of sanctions cracks down on circumvention and adopts energy measures*. 2024.

[617] Unicode Consortium. *Unicode Standard Annex #15: Unicode Normalization Forms*. 2025.

[618] Vladimir I. Levenshtein. «Binary codes capable of correcting deletions, insertions, and reversals». В: *Doklady Akademii Nauk SSSR* 163.4 (1965), с. 845—848.

[619] Fred J. Damerau. «A technique for computer detection and correction of spelling errors». В: *Communications of the ACM* 7.3 (1964), с. 171—176. DOI: 10.1145/363958.363994.

[620] Matthew A. Jaro. «Advances in Record-Linkage Methodology as Applied to Matching the 1985 Census of Tampa, Florida». В: *Journal of the American Statistical Association* 84.406 (1989), с. 414—420. DOI: 10.1080/01621459.1989.10478785.

[621] William E. Winkler. *String Comparator Metrics and Enhanced Decision Rules in the Fellegi-Sunter Model of Record Linkage*. 1990.

[622] James Turk и contributors. *jellyfish: approximate and phonetic matching of strings*. 2026.

[623] Robert C. Russell. *Soundex coding: U.S. Patent No. 1 261 167*. 1918.

[624] Lawrence Philips. «Hanging on the Metaphone». В: *Computer Language Magazine* 7.12 (1990), с. 39—43.

[625] ISO. *ISO 9:1995 «Cyrillic transliteration»*. 1995.

[626] U.S. Board on Geographic Names and Permanent Committee on Geographical Names. *Romanization of Russian: BGN/PCGN 1947 System*. 2022.

[627] International Civil Aviation Organization. *Doc 9303 Machine Readable Travel Documents, Part 3: Specifications Common to all MRTDs*. 2021.

[628] Anton Zhiyanov и contributors. *iuliia: transliterate Russian Cyrillic to Latin by established schemas*. 2026.

[629] SWIFT. *ISO 20022 for cross-border payments: end of MT/MX coexistence on 22 November 2025*. 2025.

[630] SWIFT. *Cross-Border Payments and Reporting Plus (CBPR+) usage guidelines*. 2025.

[631] RedCompass Labs. *Swift delays ISO 20022 structured address deadline*. 2026.

[632] U.S. Department of the Treasury. *Treasury Targets Gazprombank and Russian Financial Facilitators*. 2024.

[633] OFAC. *Russia-related General License 113 «Authorizing the Wind Down of Transactions Involving Certain Financial Institutions Blocked on November 21, 2024»*. 2024.

[634] OFAC. *Russia-related Sanctions*. 2026.

[635] Council of the European Union. *Council Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*. 2014.

[636] New York State Department of Financial Services. *Order against Standard Chartered Bank: AML and sanctions violations*. 2012.

[637] New York State Department of Financial Services. *Consent order against Standard Chartered Bank*. 2019.

[638] U.S. Department of Justice. *BNP Paribas Agrees to Plead Guilty and to Pay 8.9 Billion USD for Illegally Processing Financial Transactions for Countries Subject to U.S. Economic Sanctions*. 2014.

[639] NYDFS. *Deutsche Bank to Pay 258 Million USD for Transactions on Behalf of Iran, Sudan and Other Sanctioned Entities*. 2015.

[640] Basel Committee on Banking Supervision. *Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-Border Wire Transfers*. 2009.

[641] U.S. Department of Justice. *BNP Paribas Pleads Guilty In Manhattan Federal Court To Conspiring To Violate U.S. Economic Sanctions*. 2014.

[642] Office of Foreign Assets Control. *How to Search OFAC's Sanctions Lists*. 2021.

[643] Mastercard. *Building Digital Trust by Combating Scams and Fraudulent Merchants*. 2025.

[644] Visa Consulting & Analytics. *Authorization Management*. 2020.

[645] Mastercard. *Strengthen Authentication with First-Party Trust*. 2026.

[646] Peter Eckersley. «How Unique Is Your Web Browser?» В: *Privacy Enhancing Technologies (PETS 2010)*. 2010.

[647] EMVCo. *EMV 3-D Secure White Paper v2 «Technical Features»*. 2025.

[648] scikit-learn developers. *Metrics and scoring: quantifying the quality of predictions*. 2026.

[649] Martin Mihelich, François Castagnos и Charles Dognin. *Interplay of ROC and Precision-Recall AUCs: Theoretical Limits and Practical Implications in Binary Classification*. 2024.

[650] Stripe. *Radar Risk Evaluation*. 2026.

[651] Merchant Risk Council и Cybersource. *2024 Global eCommerce Payments & Fraud Report*. 2024.

[652] European Central Bank и European Banking Authority. *Report on Payment Fraud (data for 2024)*. 2025.

[653] Huanjing Wang и др. *Feature Selection Strategies: A Comparative Analysis of SHAP-Value and Importance-Based Methods*. 2024.

[654] Lianhong Ding и др. *An AutoEncoder Enhanced Light Gradient Boosting Machine Method for Credit Card Fraud Detection*. 2024.

[655] Visa. *Payment Account Validation: How to Use*. 2026.

[656] João Gama и др. *A Survey on Concept Drift Adaptation*. 2014.

[657] Marco Tulio Ribeiro, Sameer Singh и Carlos Guestrin. *Why Should I Trust You?: Explaining the Predictions of Any Classifier*. 2016.

[658] Scott M. Lundberg и Su-In Lee. *A Unified Approach to Interpreting Model Predictions*. 2017.

[659] EMVCo. *EMV 3-D Secure Protocol and Core Functions Specification v2.3*. 2024.

[660] Mastercard. *Decision Intelligence for Fraud and Risk Management*. 2026.

[661] Chargeback Gurus. *What is a Chargeback Fee?* 2024.

[662] Visa. *Improving Authorization Management for Transactions with Stored Credentials*. 2017.

[663] Cybersource. *Initial Transactions*. 2026.

[664] Cybersource. *Mastercard Subsequent MIT Subscription Payments*. 2026.

[665] European Banking Authority. *Q&A 2019_4792: Merchant Initiated Transactions exemption for hotel transactions*. 2021.

[666] Mastercard. *Announcement AN 11418 — Transaction Link Identifier (TLID) Data Integrity Update*. 2025.

[667] Visa. *Stored Credential Transaction Framework — VBS-10*. 2017.

[668] Visa. *Restrictions on Standing Instruction MITs Related to Card-on-File Tokens (AI11237)*. 2021.

[669] Verisave. *Mastercard's 2025-2026 Rate Changes: A Timeline*. 2026.

[670] Nuvei. *MasterCard Excessive Authorization Attempts*. 2025.

[671] TabaPay. *Merchant Advice Code (MAC)*. 2025.

[672] Mastercard. *Automatic Billing Updater Privacy Notice*. 2025.

[673] Visa. *Visa Account Updater Overview*. 2026.

[674] Visa. *Credential Lifecycle Management*. 2026.

[675] Visa. *Visa Account Updater FAQ*. 2026.

[676] Stripe. *Stripe Billing: subscription management and usage-based pricing*. 2026.

[677] Chargebee. *Subscription management platform*. 2026.

[678] Recurly. *Subscription management and recurring billing platform*. 2026.

[679] Lago. *Lago: open source metering and usage-based billing*. 2026.

[680] Kill Bill. *Kill Bill: open-source subscription billing & payments platform*. 2026.

[681] Recurly. *Failed Payment Recovery: What the Data Shows*. 2026.

[682] Visa. *The Technology Behind Visa*. 2025.

[683] Visa. *Authorization Framework Will Be Updated To Simplify Authorization Processing Time Frames*. 2023.

[684] Mastercard Europe SA. *Mastercard Clearing Management System – PFMI Disclosure Report*. 2025.

[685] Visa Acceptance Solutions. *Enhanced Capture File Specifications: TC 33.A and TCR layout*. 2025.

[686] Visa. *Resolve*. 2026.

[687] Mastercard. *Dispute Management & Enhanced Purchase Experience*. 2026.

[688] Mastercard. *Ethoca Consumer Clarity*. 2025.

[689] Adyen. *Dispute timeframes*. 2026.

[690] Visa. *Evolution of Compelling Evidence — Merchant FAQs*. 2023.

[691] Mastercard. *Mastercard rules and compliance programs*. 2026.

[692] Visa. *Visa Acquirer Monitoring Program Overview*. 2025.

[693] J.P. Morgan. *MasterCard Excessive Chargeback — Merchant Program Guide*. 2019.

[694] Mastercard. *Mastercard Bill Qkr Streamlines Bill Payment Services*. 2026.

[695] Mastercard. *Mastercard — Making Payment Processing Simpler and Safer*. 2026.

[696] Visa. *Trust in digital payments*. 2022.

[697] Mastercard. *Mastercard Payment Optimization Platform uses the power of data to drive more approvals*. 2025.

[698] Chargebacks911. *Visa Excessive Reattempts Rule: 2026 Retry Limits & Fees*. 2026.

[699] IETF. *RFC 6749: The OAuth 2.0 Authorization Framework*. 2012.

[700] Juspay. *Hyperswitch: open-source payments switch*. 2026.

[701] Primer. *Unified payment infrastructure: control every transaction*. 2026.

[702] Spreedly. *The Ultimate Guide to Payments Orchestration*. 2026.

[703] Gr4vy. *Cloud-native payment orchestration platform*. 2026.

[704] Juspay. *Juspay Reports Record Profitability with Strong 61% YoY Revenue Growth in FY25*. 2025.

[705] Intel Market Research. *Payment Orchestration Platform Market Growth Analysis, Dynamics, Key Players and Innovations, Outlook and Forecast 2026–2034*. 2026.

[706] Stripe. *Idempotent requests*. 2026.

[707] Adyen. *API idempotency*. 2026.

[708] Stripe Engineering. *Ledger: Stripe's system for tracking and validating money movement*. 2024.

[709] H. Krawczyk, M. Bellare и R. Canetti. *RFC 2104: HMAC: Keyed-Hashing for Message Authentication*. 1997.

[710] Stripe. *Webhooks*. 2026.

[711] M. Jones, J. Bradley и N. Sakimura. *RFC 7519: JSON Web Token (JWT)*. 2015.

[712] Stripe. *API Reference*. 2026.

[713] АО НКО ЮMoney. *ЮKassa API: справочник для разработчиков*. 2026.

[714] АО «Клаудпэйментс». *CloudPayments API*. 2026.

[715] Stripe. *Place a hold on a payment method*. 2026.

[716] Adyen. *Adyen glossary*. 2026.

[717] Stripe. *Receive payouts*. 2026.

[718] Stripe. *Balances and settlement time*. 2026.

[719] Modern Treasury. *Ledgers Overview*. 2026.

[720] Modern Treasury. *Modern Treasury Raises $50 Million From SVB Capital, Salesforce Ventures in Its Series C Round*. 2022.

[721] Formance. *Formance Ledger: programmable financial core ledger*. 2026.

[722] Y Combinator. *Formance: open source infrastructure for the financial internet*. 2026.

[723] Blnk Finance. *Blnk: open-source ledger and financial core for fintech*. 2026.

[724] TigerBeetle. *Debit/Credit: The Schema for OLTP*. 2026.

[725] Adyen. *Manage your balances*. 2026.

[726] Stripe. *Minimum balances for automatic payouts*. 2026.

[727] BRICS. *BRICS 2026 — About BRICS*. 2026.

[728] *Федеральный закон от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле»*.

[729] Банк России. *Инструкция от 16.08.2017 № 181-И «О представлении документов валютного контроля»*. 2017.

[730] CIPS. *About CIPS*. 2026.

[731] BRICS Business Council. *BRICS Pay*. 2026.

[732] SWIFT. *Interoperability between instant payment systems*. 2026.

[733] SWIFT. *Transaction Manager: Supporting adoption of ISO 20022 and the future of global payments*. 2023.

[734] Accredited Standards Committee X9. *ANSI X9.24-1: Retail Financial Services Symmetric Key Management, Part 1: Using Symmetric Techniques*. 2017.

[735] КриптоПро. *Получены сертификаты соответствия на КриптоПро HSM 2.0 R3 с Платёжным модулем*. 2023.

[736] Visa Acceptance Solutions. *Service Features: Edit Package*. 2025.

[737] Банк России. *Глоссарий платёжной системы*. 2026.

[738] Банк России. *Положение от 25.07.2022 № 802-П «О защите информации в платёжной системе Банка России»*. 2022.

[739] Visa. *PCI DSS Validation Best Practice Review*. 2018.

[740] Mastercard. *Service Provider Categories and PCI*. 2019.

[741] PCI Security Standards Council. *I have had an external vulnerability scan completed by an ASV — does this mean I am PCI DSS compliant?* 2025.

[742] Банк России. *Проекты нормативных актов Банка России*. 2026.

[743] PCI Security Standards Council. *When should an entity implement PCI DSS requirements noted as best practices until a future date?* 2024.

[744] Mastercard. *MasterCard Contactless*. 2026.

КОЛОФОН

Шрифты — PT Serif (текст), PT Sans (заголовки), PT Mono (код). Семейство ParaType, 2009 (А. Королькова, О. Умпелева, В. Ефимов).

Схемы — Inkscape.

РАСКРЫТИЕ

Использовались языковые модели Claude (Anthropic) разных версий — при подготовке инфраструктуры сборки и скриптов, перепроверке фактов и терминологии, а также при сквозной редактуре. Структура книги, отбор материала и ответственность за содержание остаются за автором.

`commit;`