

#PAYMENTSECURITY

Цифровой рубль: пять ловушек, которые накроют банки в 2026 году

Константин Стародубов

Яндекс

5–6 августа 2026



Константин Стародубов

Рук. группы комплаенса ИБ финансовых сервисов · Яндекс

- к.т.н., доцент МИЭМ ВШЭ (2 учебных пособия, более 100 публикаций)
- эк. Департамент информационной безопасности **Банка России** (написал СТО БР 1.8, ГОСТ 57580.1, ФЗ-572, банковскую нормативку, 16-МР, 18-МР, 19-МР 2-МР и т.д.)

EMAIL

starodubovkv@yandex-team.ru

TELEGRAM

@skvtmb

Пять ловушек, которые накроют банки в 2026 году

01	Операционные риски	Любая ошибка стоит дороже, чем в привычной банковской архитектуре
02	Правила пишутся на ходу	Как добиться анонимности?
03	Ограничения самой платформы	Все транзакции идут через инфраструктуру ЦБ
04	Лицензии ФСБ	Работа без нужного пункта лицензии грозит штрафом и конфискацией СЗИ
05	Вендоры и оценка влияния	Зависимость закрепляется надолго

#PAYMENTSECURITY

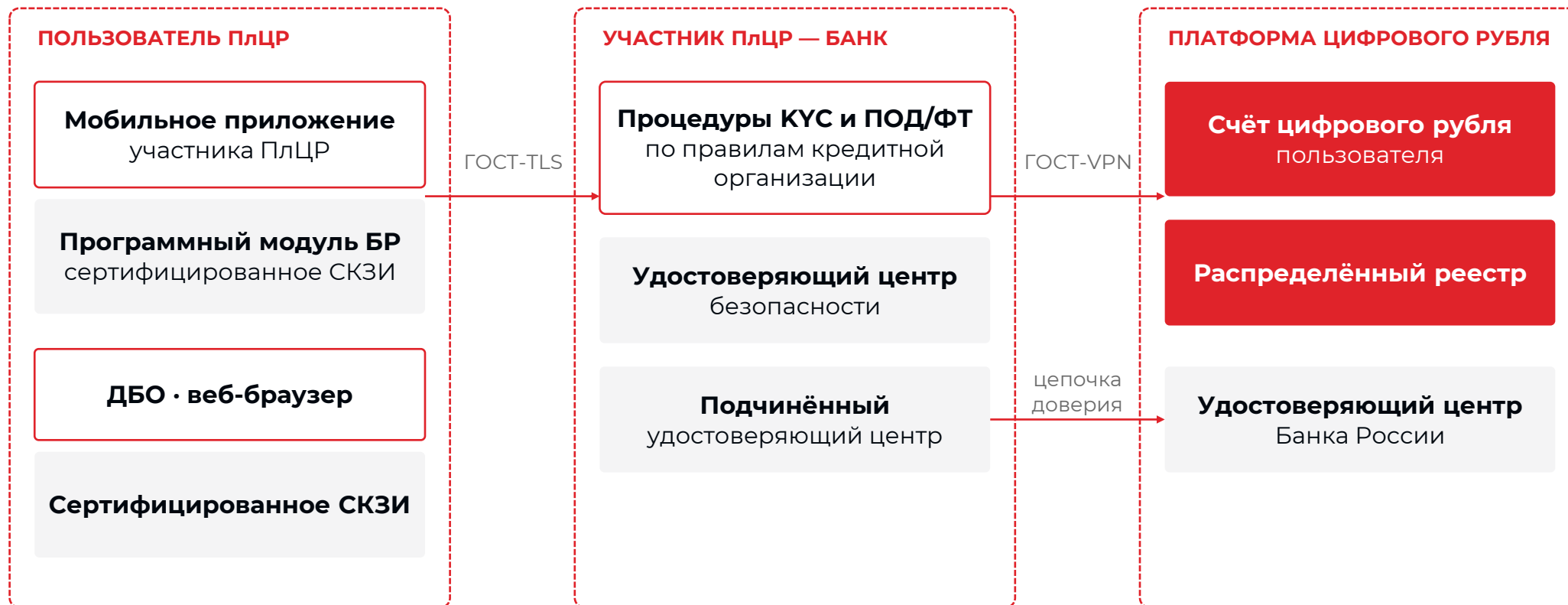
**Что такое ЦР?
Для чего нужен?**

Что такое цифровой рубль

- | | | |
|-----------|----------------------------------|--|
| 01 | Третья форма денег | Наряду с наличными и безналичными; эмитент — Банк России, всегда равен рублю |
| 02 | Обязательство государства | Счёт открывается на платформе ЦБ, а не в коммерческом банке |
| 03 | Это не криптовалюта | Курс фиксирован, эмиссия централизована, анонимности расчётов нет |
| 04 | Денежная масса не растёт | Меняется только её структура — выпуск ЦР новых рублей не создаёт |

Источник: Концепция цифрового рубля, Банк России, апрель 2021; «Цифровой рубль: текущий статус проекта», 30.06.2025

Три стороны платформы цифрового рубля



Источник: Схема Банка России, «Информационная безопасность цифрового рубля», 05.03.2026

Зачем он нужен

01 Дешевле для бизнеса

Тариф за приём оплаты ниже эквайринга и ограничен предельной суммой

02 Единый кошелёк

Баланс и история одинаковы в любом банке, клиент не привязан к одному банку

03 Программируемость

Смарт-контракты: целевые выплаты, отложенные и регулярные переводы

04 Прозрачность бюджета

Счёт цифрового рубля Федерального казначейства и контроль расходования

Источник: Цели заявлены в Концепции цифрового рубля, Банк России, апрель 2021

СКОЛЬКО ЭТО СТОИТ

ДО 31 ДЕКАБРЯ 2026

0 ₽

все операции — без комиссии

С 1 ЯНВАРЯ 2027

Между гражданами — 0 ₽

Приём оплаты бизнесом — 0,3%, не более 1 500 ₽

Оплата ЖКУ — 0,2%, не более 10 ₽

Между юрлицами — 15 ₽ за перевод

Источник: Нулевой период продлён до 31.12.2026; тарифы утверждены Банком России

#PAYMENTSECURITY

Цифровой рубль · Стародубов

Банк перестаёт быть хранителем средств

01 Технологический интерфейс

Банк — точка доступа к платформе ЦБ; проценты на цифровые рубли не начисляются

02 Точка входа в госсистему

На банк ложится ответственность за защиту взаимодействия с платформой

03 Это не интеграция API

Меняется вся платёжная архитектура: mobile, backend, DevOps, криптография, антифрод

для пользователей

Для клиента изменения почти незаметны

10

01 Ещё один «счёт»

В приложении появляется кошелёк цифрового рубля

02 Единый баланс

Баланс и история операций одинаковы вне зависимости от банка входа

03 Первый вход через ЕСИА

Госуслуги, максимальный уровень подтверждённости; после этого задаётся «пароль ЦР»

01

ЛОВУШКА 01

Операционные риски

Ключевые мероприятия по ИБ

01	Встраивание ПМ БР	Программный модуль Банка России в мобильное приложение кредитной организации
02	СКЗИ в оба контура	Контур обработки и контур контроля плюс реализация замкнутой программной среды
03	Средства УЦ	Применение средств удостоверяющих центров требуемого класса
04	Антифрод-мероприятия	Отдельный блок работ в составе утверждённой дорожной карты

Источник: Приоритет реализации установлен для СЗКО: по ФЗ № 248-ФЗ они обеспечивают операции с ЦР с 01.09.2026 (Банк России, 05.03.2026)

Путь клиента в цифровой рубль



Биометрия не заменяет пароль ЦР · блокировка после 3 попыток минимум на 30 секунд · срок действия пароля 6 месяцев

Обновить корневые сертификаты можно только обновлением приложения: скачивание по сети запрещено

Источник: Требования к ПМ БР и интерфейсам — стандарты Банка России от 03.12.2024 и 29.11.2024

Как требования ложатся на инфраструктуру банка



п. 13.4 — средства УЦ не ниже КС3 · п. 14.1 — канал с платформой не ниже КС2, с 01.01.2025 КС3 · п. 14.2 — КС2 у банка и КС1 у клиента

Источник: Положение Банка России от 07.12.2023 № 833-П, пп. 13.4, 14.1, 14.2 и Приложение 1

Технические требования к УЦ

- | | | |
|-----------|---------------------------------|--|
| 01 | Ключи ЭП — только в HSM | Ключи подчинённого УЦ хранятся в HSM-модуле в зашифрованном виде |
| 02 | Схема разделения секрета | Доступ к ключам — минимум двух администраторов ИБ |
| 03 | Разделение ролей | Системный администратор, администратор ЭП, аудит |
| 04 | Реестр — 12 часов | Сведения о прекращении действия сертификата вносятся в реестр в течение 12 часов |

Своя инфраструктура или облако

On-premise

- Два ЦОД, HSM, кластеры УЦ и СУБД на балансе банка
- Свои лицензии ФСБ и штат администраторов ИБ
- Капитальные затраты и длинный срок ввода в эксплуатацию
- Полный контроль над средой функционирования СКЗИ

Облако и as-a-service

- Компоненты УЦ и контура обработки на выделенных ресурсах провайдера
- Подключение к платформе как услуга, операционная модель затрат
- Требования не смягчаются: те же классы СКЗИ, замкнутая среда, своя оценка влияния
- Каналы между контролируемыми зонами
- СКЗИ не ниже KB2 либо выделенные каналы

Служба безопасности и контроля

01	Обязательный орган	Отдельная служба, подчинённая руководителю блока ИБ
02	Требования к людям	Высшее образование в области ИБ; минимум один специалист с опытом работы от 3 лет
03	Защищённая разработка	Контроль по ГОСТ Р 56939-2024 и разделу 7.4 Профиля защиты Банка России
04	Целостность дистрибутива	Мониторинг распространённых версий МП и хранение эталонной версии

Цена ошибки выше, чем раньше

Централизованная система не прощает мелочей

Компрометация ключей, ошибки интеграций, неверные настройки доступа, человеческий фактор. В привычной банковской архитектуре часть таких ошибок гасится внутренними процессами. В контуре цифрового рубля ошибка сразу становится инцидентом, видимым регулятору.

833-П

требует полноценной
системы
предотвращения и
реагирования на ИБ-
инциденты

02

ЛОВУШКА 02

Правила пишутся на ходу

Веб-приложения: правила ещё не закрыты

Стандарт ОВ пока только про мобильные приложения

ЦБ планирует согласовать с 8 Центром ФСБ новую редакцию, по которой веб-приложения с функционалом ЦР будут оцениваться аналогично мобильным. Пока этого не произошло, объём работ по вебу нельзя оценить точно — но закладывать его в план уже нужно.

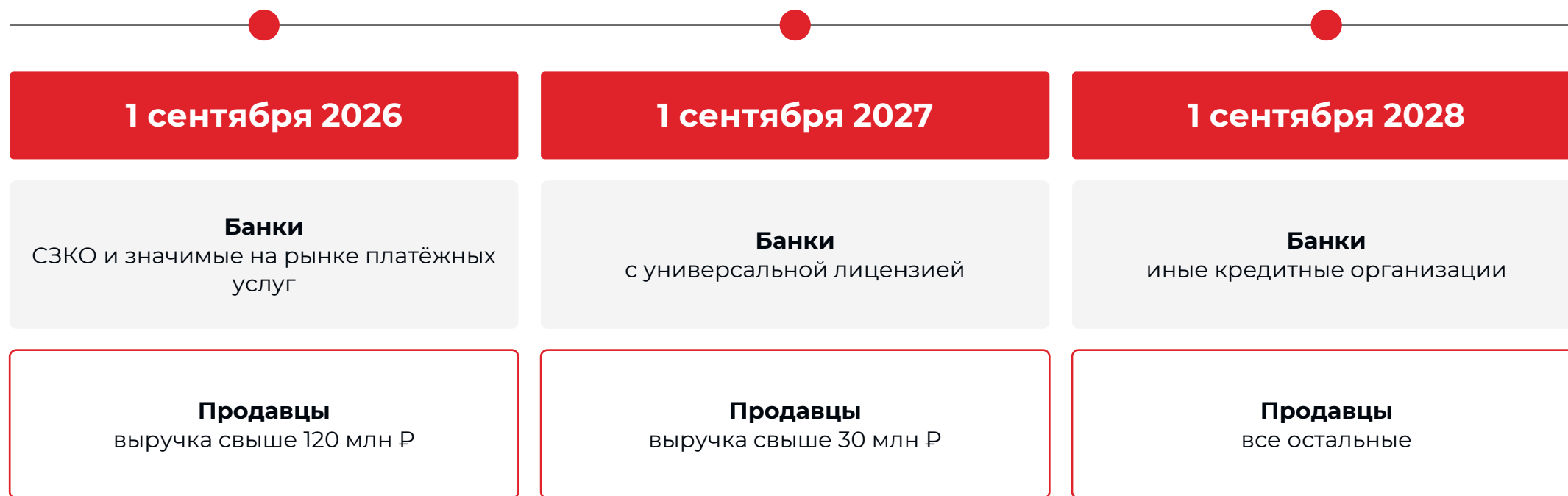
v14

текущая версия
уточнений к стандарту
ПлЦР: документы
обновляются на ходу

Что ещё не устоялось

01	Анонимность операций	Как обеспечить приватность в системе, где все транзакции идут через ЦБ
02	Пропускная способность	ЦБ не публикует показатели производительности — планировать нагрузку нужно по договорным SLA
03	Разрешение споров	Практика возврата средств и разбора инцидентов только формируется
04	Делегирование биометрии	Применение ЕБС уточняется

График обязательного внедрения



Торговый объект с выручкой менее 5 млн ₽ за предшествующий год принимать ЦР не обязан

Источник: Федеральный закон от 23.07.2025 № 248-ФЗ, статья 4. Яндекс Банк — в первой волне

Что работает, а что обещано

Работает сейчас

- Переводы между кошельками на платформе Банка России
- Смарт-контракты двух типов: отложенный и регулярный перевод
- Выплаты по реестрам для участников пилота с 20.02.2026
- Приём платежей в бюджет цифровыми рублями с 01.01.2026

Только заявлено

- Офлайн-платежи: незавершённое научное исследование
- Платформа коммерческих смарт-контрактов: концепция от 18.06.2026
- Трансграничные расчёты: концептуальная проработка
- Кошельки на балансе банков: эксперимент ориентировочно с 2029

Что работает сегодня

01	Всего два сценария	Регулярный перевод по расписанию и разовый отложенный перевод с датой
02	Создаёт только ЦБ	Ни банк, ни клиент собственный смарт-контракт сегодня написать не могут
03	37,4 тыс. исполнений	На 01.06.2026, в основном регулярные платежи; годом ранее было около 17 тысяч
04	Пилоты «окрашивания»	Татарстан, Ростовская область, Чувашия: субсидии и социальные выплаты

Источник: Концепция платформы коммерческих смарт-контрактов, Банк России, 18.06.2026

Платформа коммерческих смарт-контрактов

01 Витрина сценариев

Пользователь выбирает опубликованный контракт и настраивает его параметры

02 Разработчики

Юридические лица, соответствующие требованиям оператора платформы

03 Проверяющие организации

Проверка бизнес-логики, соответствия законодательству и требованиям ИБ

04 Поставщики данных

Оракулы: государственные и коммерческие системы, открытые источники

05 Оператор — Банк России

На первом этапе; в будущем возможен отдельный оператор

Источник: Публичное обсуждение концепции — до 30 сентября 2026; дорожной карты запуска в документе нет

Чего смарт-контракты не умеют

01	Не свой код, а параметры	Пользователь настраивает изменяемые параметры готового контракта
02	Лимит на вычисления	Регламентные ограничения через оценку количества допустимых операций
03	Иностранцы исключены	Доступ иностранных лиц к платформе на данном этапе не рассматривается
04	Риски признаёт сам ЦБ	Нагрузка на инфраструктуру, вредоносный код, сбои оракулов, утечки
05	Банк — «последняя миля»	Исполнение целиком на платформе ЦБ, банк лишь точка входа

Источник: Концепция ПКСК, Банк России, 18.06.2026, разделы 3.2 и 7

Офлайн-платежи: как задумано

01 Второй кошелёк

Помимо онлайн-кошелька клиенту открывается офлайн-кошелёк на смартфоне

02 Пополнение только онлайн

Перевод с онлайн-кошелька при наличии доступа к сети Интернет

03 NFC и Bluetooth

Технологии беспроводной передачи данных малого радиуса действия

04 Задуман как наличные

По докладу 2020 года расчёты окончательные и не требуют посредников

Источник: Концепция цифрового рубля, апрель 2021; доклад для общественных консультаций, 13.10.2020

Почему офлайн — это сложно

01	Архитектура не выбрана	ЦБ обещает доклад с несколькими решениями, а не одно готовое
02	Лимиты не названы	Намерение ограничивать сумму и число операций заявлено, цифр нет
03	Двойное списание	Скомпрометированный кошелек способен показать несуществующий остаток
04	Холодного хранения нет	Приватных ключей у пользователя нет, средства всегда на платформе ЦБ
05	Требований к банку нет	Ни спецификации, ни версии ПМ БР с офлайн-функциональностью не существует

Источник: Лимит 300 тыс. Р в месяц относится к пополнению онлайн-кошелька и к офлайну отношения не имеет

Трансграничные расчёты: пока концепция

Заявлены оба формата — двусторонний и многосторонний

«С рядом дружественных стран обсуждаются возможные варианты двусторонней интеграции национальных платформ ЦВЦБ», а по линии БРИКС «прорабатываются вопросы использования ЦВЦБ в трансграничных расчётах».

Конкретные страны-контрагенты не названы, сроков нет. Банк России отдельно оговаривает: для таких проектов нужны технические возможности у зарубежных партнёров.

0

действующих
трансграничных расчётов
в цифровых рублях на
июль 2026

Источник: Банк России, «Цифровой рубль: текущий статус проекта», 30.06.2025

#PAYMENTSECURITY

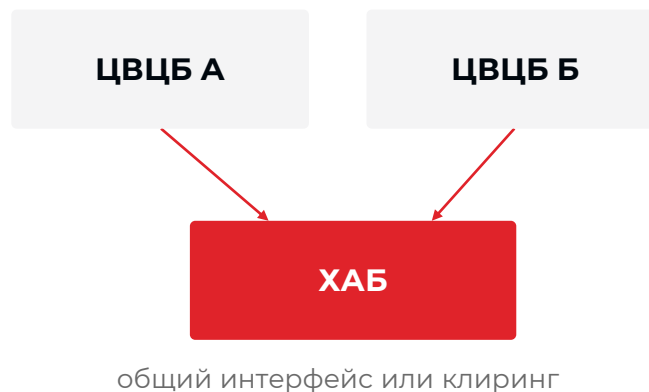
Три модели интеграции платформ ЦВЦБ

01 СОВМЕСТИМОСТЬ



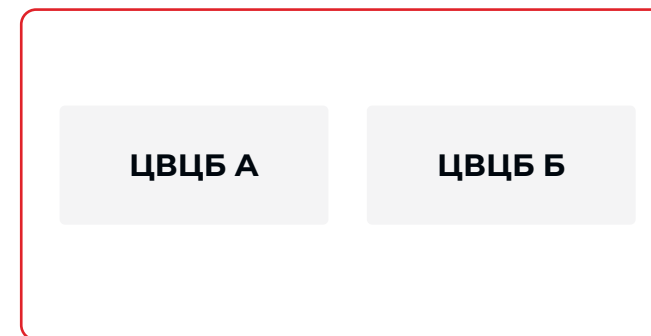
Раздельные системы работают по общим стандартам: форматы сообщений, криптография, данные

02 ВЗАИМОСВЯЗАННОСТЬ



Общий технический интерфейс либо общий клиринговый механизм между системами

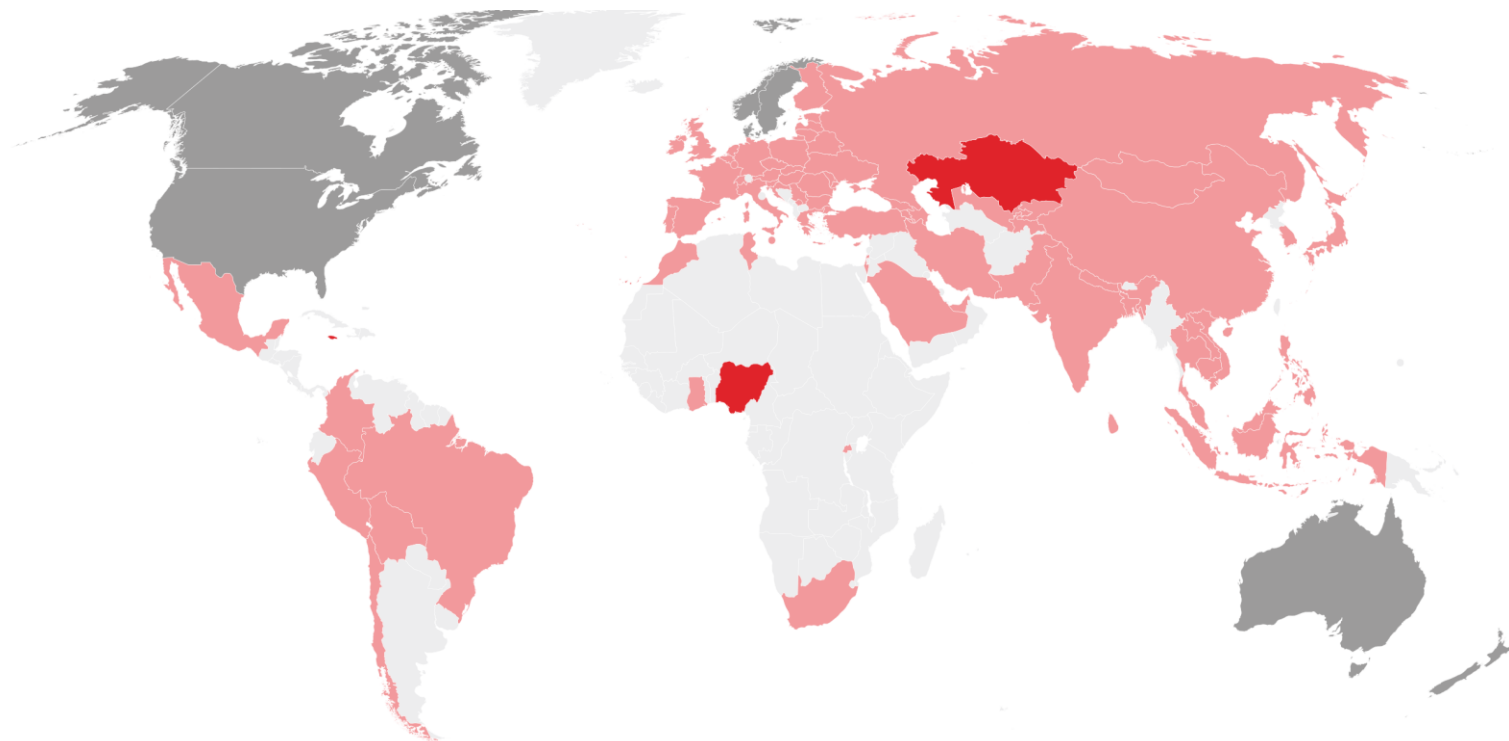
03 ЕДИНАЯ ПЛАТФОРМА



Один свод правил, одна техническая система, один круг участников

Источник: Таксономия BIS: BIS Papers № 115, март 2021; доклад CPMI, BIS, МВФ и Всемирного банка для G20, июль 2021

ЦВЦБ на карте мира



- Запущена розничная ЦВЦБ**
Багамы, Ямайка, Нигерия, Казахстан
- Пилот или разработка**
41 пилотный проект, 77 стран в продвинутых стадиях
- Свернули или заморозили**
США, Канада, Австралия, Норвегия, Швеция, Дания
- Изучают или не заявляли**
остальные юрисдикции

146 стран и валютных союзов изучают ЦВЦБ — свыше 98% мирового ВВП

Источник: Atlantic Council CBDC Tracker, обновление май 2026; статусы стран меняются быстро

#PAYMENTSECURITY

Цифровой рубль · Стародубов

Кто запустил, а кто свернул

01	Багамы — Sand Dollar	Первая розничная ЦВЦБ в мире, октябрь 2020; менее 0,5% наличной массы
02	Восточно-Карибский союз	DCash закрыт: разработка второй версии остановлена 13.02.2026
03	Казахстан — тенге	Цифровой тенге получил статус законного платёжного средства 18.07.2026
04	США — запрет	Исполнительный указ 14178 от 23.01.2025 запрещает работу над розничной ЦВЦБ

Источник: Atlantic Council CBDC Tracker и национальные центральные банки; статусы быстро меняются

Что мешает трансграну

01 Санкционный контур

Инфраструктура BIS недоступна странам под санкциями — заявление главы BIS

02 Разные стандарты

Форматы сообщений, криптография и требования к данным не унифицированы

03 COMPLAINTS

ПОД/ФТ и валютный контроль в трансграничных протоколах — отдельная задача

04 Плохая масштабируемость

Для N юрисдикций нужно $N \times (N-1)/2$ двусторонних связей

Источник: Банк России, 30.06.2025; BIS — выступление А. Карстенса 31.10.2024 и доклад CPMI d219

03

ЛОВУШКА 03

Ограничения платформы

На что можно рассчитывать по SLA

99,5%

доступность промышленного контура

В сутки — 7 минут 12 секунд допустимого простоя

За 7 дней — 50 минут 24 секунды

За год — 1 день 19 часов 48 минут

Тестовый контур: требований к доступности нет, поддержка в рабочие дни с 8:00 до 21:00 МСК

Пополнение и вывод средств — только в стандартный период регулярного сеанса ПС БР

Источник: Стандарт ПлЦР «Порядок подключения участника платформы к платформе цифрового рубля», версия 1.3

Оценка соответствия по ГОСТ Р 57580

01	Уровень зависит от банка	Усиленный — для СЗКО и значимых на рынке платёжных услуг, стандартный — для остальных (пп. 4.1–4.2)
02	Раз в два года	Периодичность — п. 15; итоговый уровень соответствия не ниже 4-го по ГОСТ Р 57580.2-2018 — п. 18
03	Только лицензиат ФСТЭК	Проверяющая организация с лицензией по техзащите информации
04	Область — сегмент ЦР	Оценивается контур цифрового рубля, а не весь банк — пункт 16

Источник: Положение Банка России от 07.12.2023 № 833-П; методика оценки — ГОСТ Р 57580.2-2018

Ежегодная проверка на проникновение

01	Ежегодно	Тестирование на проникновение и анализ уязвимостей — не реже раза в год, п. 19
02	Охват	Объекты инфраструктуры в выделенных сегментах контура цифрового рубля
03	Исполнитель не задан	833-П не требует лицензиата для пентеста — в отличие от оценки соответствия
04	Отчётность уходит в ЦБ	Результаты оценки соответствия отражаются в форме 0409071

Источник: Хранение отчёта проверяющей организации — не менее пяти лет, пункт 17 Положения 833-П

04

ЛОВУШКА 04

Лицензии ФСБ

Лицензия ФСБ: скрытый барьер

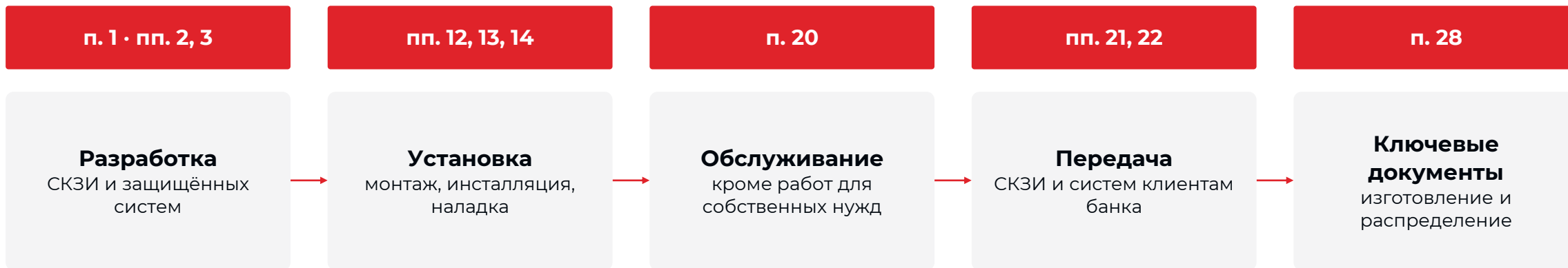
Лицензия нужна не «на всякий случай»

Виды деятельности, на которые требуется лицензия ФСБ, возникают сами собой при подключении к платформе цифрового рубля: разработка компонентов со встроенным СКЗИ, установка и эксплуатация СКЗИ, распространение мобильного приложения с ПМ БР, работа собственного удостоверяющего центра.

5

пунктов лицензии ФСБ
закрывают полный цикл
работы банка с
цифровым рублём

Жизненный цикл СКЗИ и пункты лицензии



Изъятие «для собственных нужд» есть только у пункта 20 — монтаж и установка под него не подпадают

Для удостоверяющего центра дополнительно — статья 16 Федерального закона № 63-ФЗ

Источник: Перечень — приложение к Положению, утв. постановлением Правительства РФ от 16.04.2012 № 313 (ред. от 28.08.2023)

Работа без лицензии

Административная — ст. 13.13 КоАП

- Юридические лица: 10 000–20 000 ₽
- Должностные лица: 2 000–3 000 ₽
- Конфискация СЗИ факультативна: «или без таковой»
- Юрлицо и должностное лицо отвечают параллельно (ч. 3 ст. 2.1 КоАП)

Уголовная — ст. 171 УК РФ

- Часть 1, крупный размер свыше 3,5 млн ₽: штраф до 300 000 ₽, работы, арест до 6 месяцев
- Лишение свободы до 5 лет — только часть 2: организованная группа либо доход свыше 13,5 млн ₽
- Отвечает руководитель или фактически исполняющий его функции (п. 10 ППВС № 23 от 18.11.2004)

Главная сложность — криптография

01	Проверка в 8 Центре ФСБ	Лаборатория проверяет корректность реализации криптографии в приложении
02	Канал с платформой	СКЗИ не ниже КС2, с 1 января 2025 — КС3 (п. 14.1 Положения 833-П)
03	Канал с пользователем	КС2 на стороне банка и КС1 на стороне клиента (п. 14.2 Положения 833-П)
04	Автовыпуск сертификатов	Многие удостоверяющие центры ранее такую автоматизацию не поддерживали

Источник: Положение Банка России от 07.12.2023 № 833-П «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля»

05

ЛОВУШКА 05

Вендоры и оценка влияния

Кто обязан проходить оценку влияния

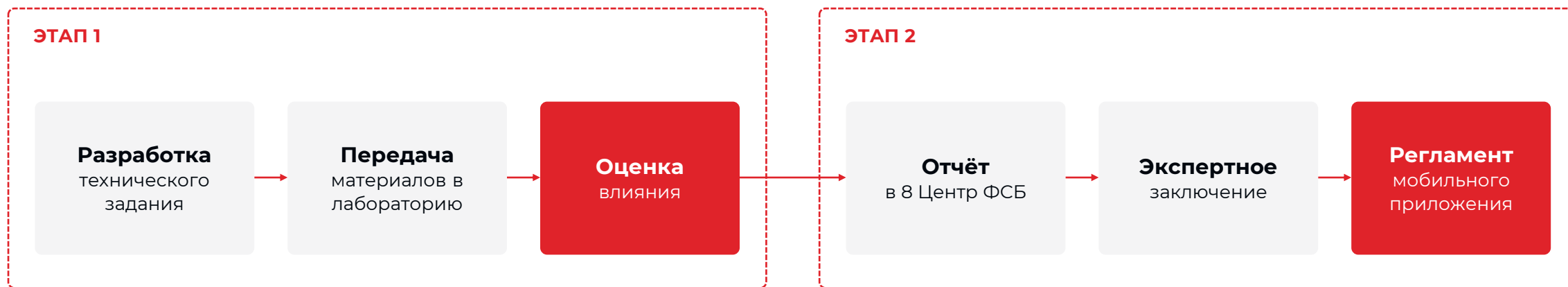
Участники ПлЦР, встраивающие ПМ БР

Оценка влияния обязательна для банков — участников платформы цифрового рубля, которые встраивают ПМ БР в мобильное или веб-приложение с функционалом ЦР. Источник требований — каталог ОВ: стандарт ПлЦР, уточнения v14, шаблон ТЗ и требования к материалам.

07.04.26

на эту дату действующий
стандарт ОВ
распространяется только
на мобильные
приложения

Процесс идёт в два этапа



2 месяца — срок рассмотрения материалов в 8 Центре ФСБ по каждому объекту оценки

Источник: Смена лаборатории обнуляет упрощённую процедуру и запускает полную оценку влияния заново

Упрощённая процедура: три года



Примечание: При упрощённой процедуре работать нужно с той же лабораторией, что проводила первичную оценку

Что регулятор уже упростил

01 Стандарт ОВ для мобильных устройств

ЦБ вместе с ФСБ выпустили стандарт, упрощающий ОВ для приложений с ПМ БР без ущерба релизам

02 Переиспользование ПМ БР

С начала 2025 модуль можно применять и вне ЦР — например, для защищённого канала к ЕБС

03 Автовыпуск сертификатов

Документ ЦБ по автоматизации выпуска

Что готовить для разработки ТЗ

01	Лицензия ФСБ	Копия по пп. 2 или 3 либо обоснование её отсутствия
02	Наименование приложения	Официальное название, под которым публикуется МП
03	Описание функционала ЦР	Не менее одной страницы А4
04	Вендор СКЗИ и ПМ БР	Валидата, КриптоПро или ИнфоТеКС
05	Технические данные	Архитектуры процессоров, версии ОС, языки программирования, фреймворки

Исходные коды: подготовка перед передачей

01 Убрать лишнее

Явно устаревший, неиспользуемый и дублирующийся код

02 Структурировать

Отделить основной функционал от тестовых и демонстрационных компонентов

03 Минимизировать заглушки

Закомментированные фрагменты и временные конструкции

04 Комментарии на русском

Отдельное требование к ПМ БР

05 Структура кодовой базы

Документ с ключевыми модулями и зависимостями (SBOM)

Отчёты SAST и SCA

SAST

- Инструмент и его версия, конфигурация, объём анализа
- Результаты в формате JSON, SARIF или XML
- Для каждой уязвимости Critical и High
- обоснование невозможности эксплуатации

SCA

- SBOM обязателен
- Аналогичные обоснования для Critical и High
- Контекст данных, отсутствие вектора атаки или компенсирующие меры

Требования к ПМ БР в составе приложения

01	Без государственной тайны	Обработка сведений, составляющих гостайну, не допускается
02	Без опасных конструкций	Нет средств разработки, мониторинга криптоключей, eval и загрузки внешнего кода
03	Без потери криптосвойств	ПМ БР работает на сертифицированном СКЗИ
04	Отпечаток устройства	Сбор device fingerprint
05	Работа с CDVC-сообщениями	Подпись ключом ЭП пользователя, шифрование, расшифрование, проверка подписи

Зависимость закрепляется надолго

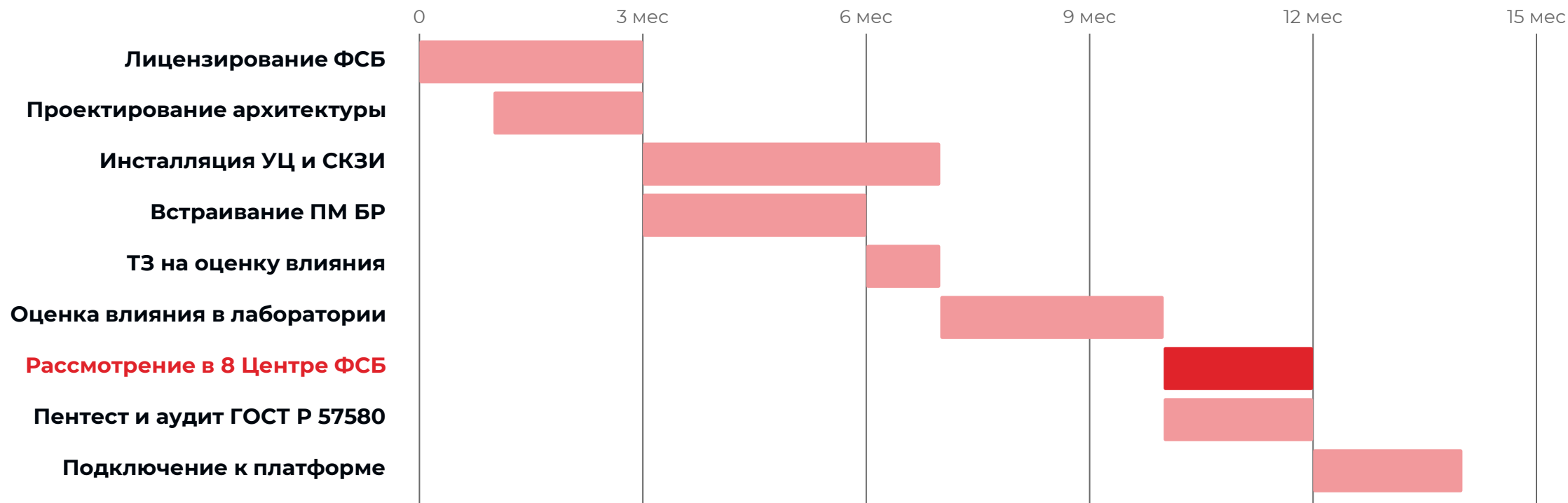
Рынок СКЗИ для ЦР фактически монополизирован

Смена поставщика СКЗИ требует повторной оценки влияния — со всеми материалами, стендами и сроками. Долгосрочные договоры с интеграторами закрепляют выбор ещё сильнее, а смена лаборатории обнуляет упрощённую процедуру.

3

вендора СКЗИ и ПМ БР
на рынке: Валидата,
КриптоПро, ИнфоТеКС

Сколько занимает подготовка



Полный цикл ≈ 14 месяцев

Источник: Длительности — экспертная оценка докладчика; нормативно подтверждён только срок в 8 Центре ФСБ — 2 месяца

Документы, на которые опирается доклад

01 Федеральные законы

248-ФЗ от 23.07.2025 — этапы 2026 / 2027 / 2028, ст. 4 · 340-ФЗ от 24.07.2023 — изменения в 161-ФЗ

02 Положения Банка России

833-П и 820-П от 2023 · 821-П и 851-П — переводы и операции без согласия клиента · 802-П

03 ПП РФ от 16.04.2012 № 313

Перечень работ и услуг, составляющих лицензируемую деятельность с СКЗИ

04 Стандарты и ГОСТы

Порядок подключения участника ПлЦР в. 1.3 · ГОСТ Р 57580.1-2017 · ГОСТ Р 56939-2024

#PAYMENTSECURITY

Цифровой рубль не меняет форму денег — он меняет правила их существования

Главный вывод

Комплаенс и контроль встроены глубже, чем раньше. Ответственность участников системы возрастает.

#PAYMENTSECURITY

Спасибо за внимание!

EMAIL

starodubovkv@yandex-team.ru

TELEGRAM

@skvtmb