



# РусКрипто

## XXVIII

НАУЧНО-ПРАКТИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

### **Российская криптография в финансовых сервисах. Прошлое, настоящее, будущее.**

Андрей Елистратов, к.ф.-м.н.

Департамент информационной безопасности Банка России



## 90-е и нулевые

1988 год: соглашение с VISA, сделавшее «Интурист» членом организации с правом эквайринга

21 сентября 1991 года: первая транзакция по карте, выпущенной российским банком

1992 год: СТБ Карт, Union Card, Золотая Корона.

Начало XXI в: более 60 российских банков  
Эмитировали Europay/Mastercard и Visa International





## 10-е годы

Mastercard и Visa International

Вырос рынок устройств, обеспечивающих  
платежи – POS-терминалы, банкоматы

Появляются и российские POS-терминалы



Security  
Standards Council®







**РусКрипто**  
XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ  
КОНФЕРЕНЦИЯ



Банк России



**2013-2015 годы**



**НСПК**

НАЦИОНАЛЬНАЯ  
СИСТЕМА  
ПЛАТЕЖНЫХ  
КАРТ

2014 год: АО «Национальная система платежных карт»

декабрь 2015 г: была выпущена первая карта «Мир»

В НСПК объяснили, как будут  
работать карты Visa и  
Mastercard в России



Visa и MasterCard решили  
остаться в России

«Мир» перешёл экватор. Росси  
платёжная система вытесняет  
продукты Visa и Mastercard





**2015-2017 годы**

## Система передачи финансовых сообщений

### ГЛОБАЛЬНОЕ ПОДКЛЮЧЕНИЕ К СИСТЕМЕ ПЕРЕДАЧИ ФИНАНСОВЫХ СООБЩЕНИЙ (СПФС) БАНКА РОССИИ

Источник: Банк России (по состоянию на январь 2024)



КОЛИЧЕСТВО  
ГОСУДАРСТВ,  
ПРИСОЕДИНИВШИХСЯ  
К СПФС

**20**



КОЛИЧЕСТВО  
БАНКОВ  
И КОМПАНИЙ,  
ИСПОЛЬЗУЮЩИХ  
СПФС

ИЗ НИХ  
НЕРЕЗИДЕНТОВ

**159**



На базе российских  
криптографических средств



## **2018 год**

Указание Банка России от 07.05.2018 № 4793-У «О внесении изменений в Положение Банка России от 9 июня 2012 года N 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»

**к 2024 году российские банки должны использовать только Российские HSM**

**к 2031 году в карточных платежах должны использоваться и российские криптографические алгоритмы**



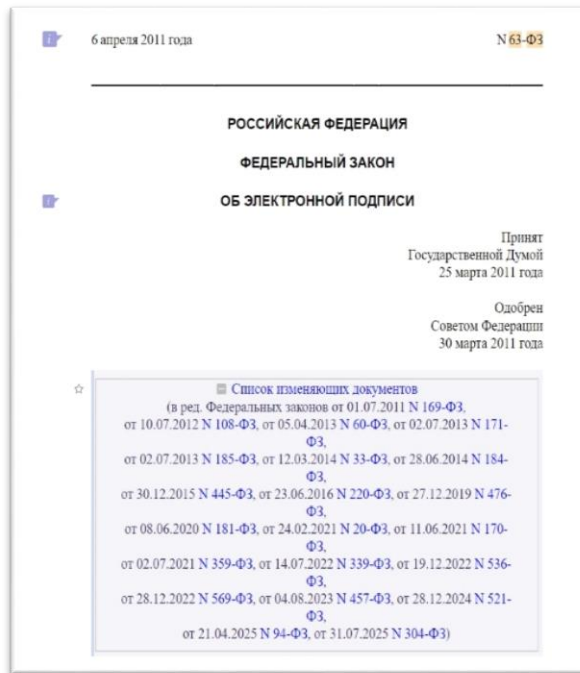
**2019 год**

Федеральный закон № 476-ФЗ «О внесении изменений в  
Федеральный закон «Об электронной подписи»

Статья 17.2.

«... такой сертификат создается и выдается  
удостоверяющим центром Центрального банка  
Российской Федерации в установленном  
Центральным банком Российской Федерации  
порядке...»

**Финансовые организации получают сертификаты ключей проверки УКЭП в Банке России**





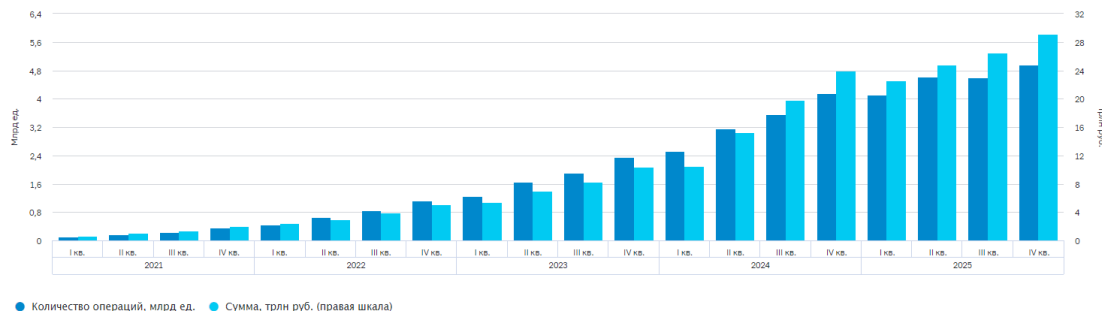


**2019 год**

## Система быстрых платежей



Среднее количество операций в сутки в 2025 году составило 50 млн, превысив значение 2024 года на треть



На основе российских криптографических средств

**Средства на расчётный счёт поступают мгновенно**  
Ведите бизнес без кассовых разрывов вне зависимости от часовых поясов и времени суток.

**Принимайте безналичную оплату без карт от клиентов разных банков и экономьте на эквайринге**

**Принимайте и совершайте платежи без ошибок ввода реквизитов**  
Для оплаты через СБП не нужно вручную вводить платёжные реквизиты получателя, что поможет избежать ошибок ввода данных.

**Сократите расходы на оборудование**  
СБП — современная альтернатива эквайрингу: для приёма платежей наличие терминала и другого оборудования не обязательно.

**Продавайте в социальных сетях и мессенджерах**  
Отправляйте клиентам ссылку на оплату. Перейдя по ней, клиент попадёт в мобильное приложение своего банка и подтверждает платёж.





2022 год

## Санкции

- 2022 г. Западные поставщики банкоматов, POS-терминалов прекратили деятельность в России.
- В мае 2022 года компания Thales (HSM-модули) ушла из России
- 2022 г. EMVCo официально известило о «временном прекращении транзакций» со всеми российскими организациями

инфографика

### Страны-лидеры по числу введенных санкций

В эквиваленте \$ млрд.  
Данные на 12 февраля. Без учета секторальных санкций





2022 год

## Санкции

До 2023 г.

- Большая часть банкоматов.
- Большая часть POS-терминалов
- 100% HSM модулей

Иностранного производства



LENTA.RU

США допустили санкции за  
поддержку карт «Мир» за  
пределами России

Runet

Мария Арялина

Сотрудничающим с системой «Мир»  
компаниям могут грозить санкции



**2023-2024 год**

## Российские HSM-модули

Разработаны HSM:

- ООО «Системы практической безопасности»
- ООО «КриптоПро»



СИСТЕМЫ  
ПРАКТИЧЕСКОЙ  
БЕЗОПАСНОСТИ



В 2024 году завершена замена HSM-модулей в банках



## Финансовые технологии в конце 10-х начале 20-х

2018 год: Единая биометрическая система (ЕБС)



Единая  
Биометрическая  
Система

2021 год: запущена первая система биоэквайринга



2024 год: АО НСПК запустило мультибиоэквайринг для системы СБП







## Финансовые технологии в конце 10-х начале 20-х

**2022-2026: Открытые банковские интерфейсы**

**Open API**

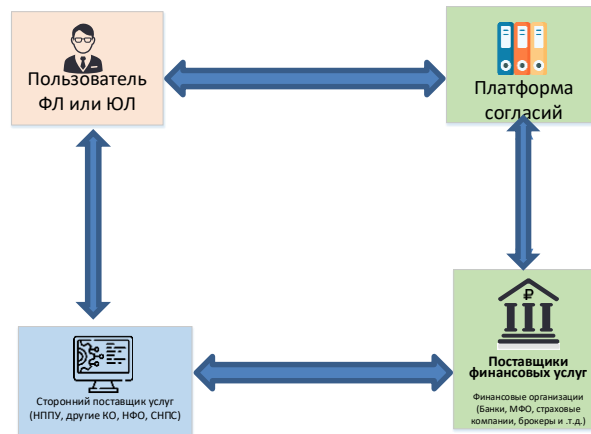
**ТК 26** «Криптографическая защита информации»

**МР.26.2.002-2024**

**ТК 122** «Стандарты финансовых операций»

**СТО БР ФАПИ.СЕК-1.6-2024**

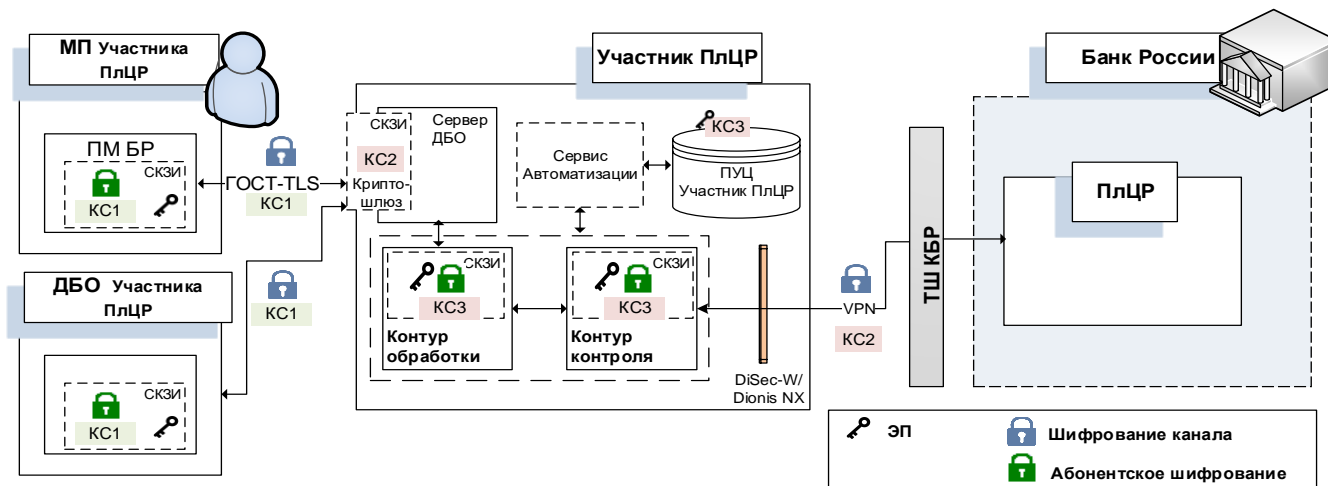
**СТО БР ФАПИ.ПАОК-1.0-2024**





2023-2026 годы

Цифровой рубль

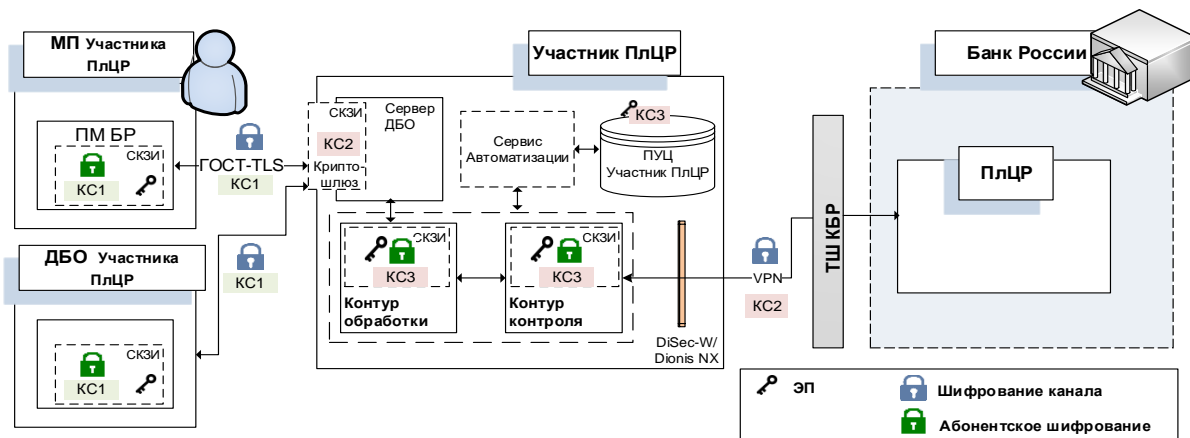


Положение Банка России от 07.12.2023 № 833-П «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля»



2023-2026 годы

Цифровой рубль



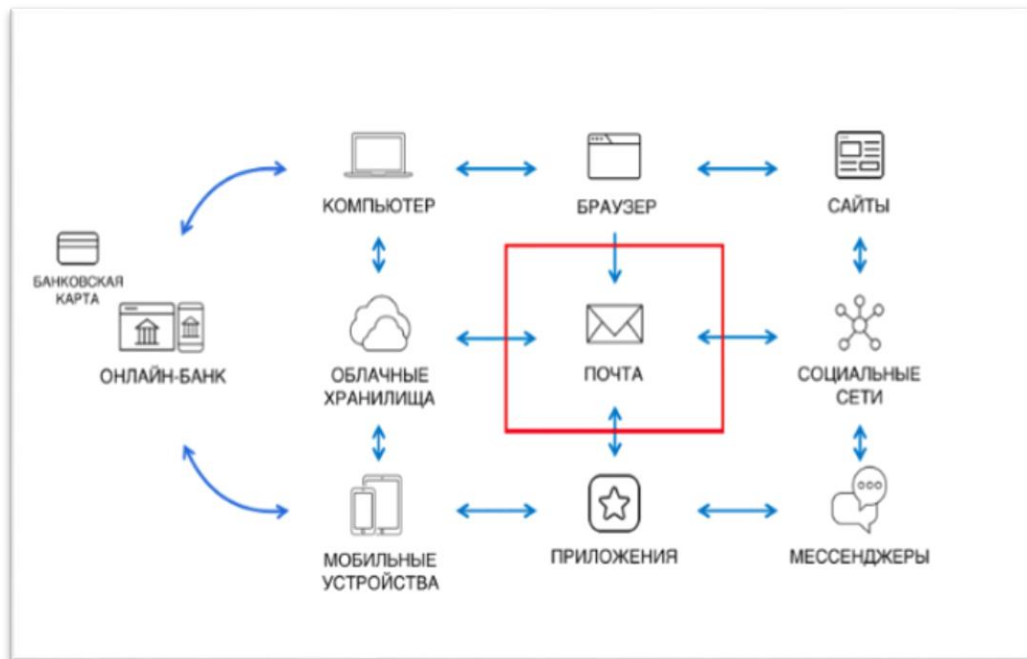
- Создание типовых программных модулей (ПМ БР)
- Автоматизация выпуска сертификатов клиентов
- Изменения подходов по проведению оценки влияния среды функционирования на используемое криптографическое средство



## Будущее финансовых технологий

### Вызовы

- Инфраструктура цифровой идентификации
- Инфраструктура цифровых платежей
- Инфраструктура цифрового обмена данными



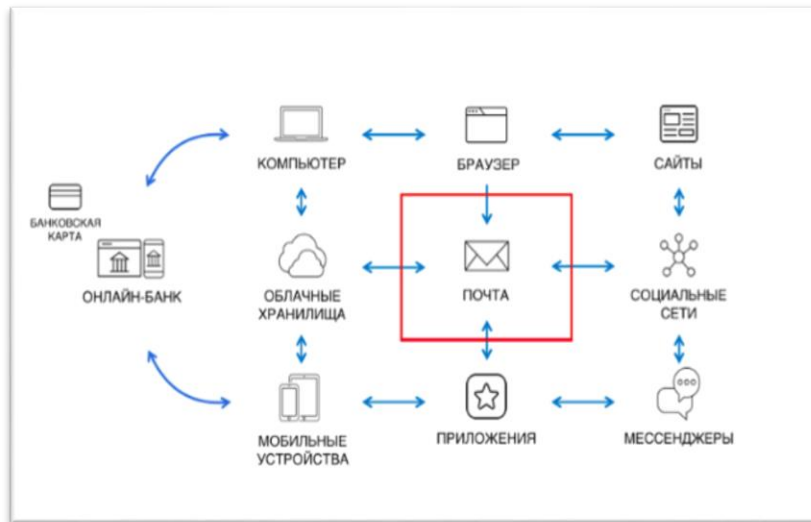




## Будущее финансовых технологий

### Задачи

- Развитие методов идентификации клиентов финансовых организаций
- Развитие цифровых трансграничных платежей и новых криптографических механизмов
- Развитие криптографических протоколов семейства OpenIDConnect





## Будущее финансовых технологий

### Развитие ПС «Мир» 2025-2031

- Разработка МР ТК26 «Информационная технология. Криптографическая защита информации. Протокол бесконтактной обработки транзакций».
- Разработка МР ТК26 «Информационная технология. Криптографическая защита информации. Протокол контактной обработки транзакций».



Русский "Мир": что  
нужно знать о  
национальной  
платежной системе



**РусКрипто**  
**XXVIII** НАУЧНО-ПРАКТИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

# Спасибо за внимание!

**Елистратов Андрей Алексеевич**

Департамент информационной безопасности  
Банка России