

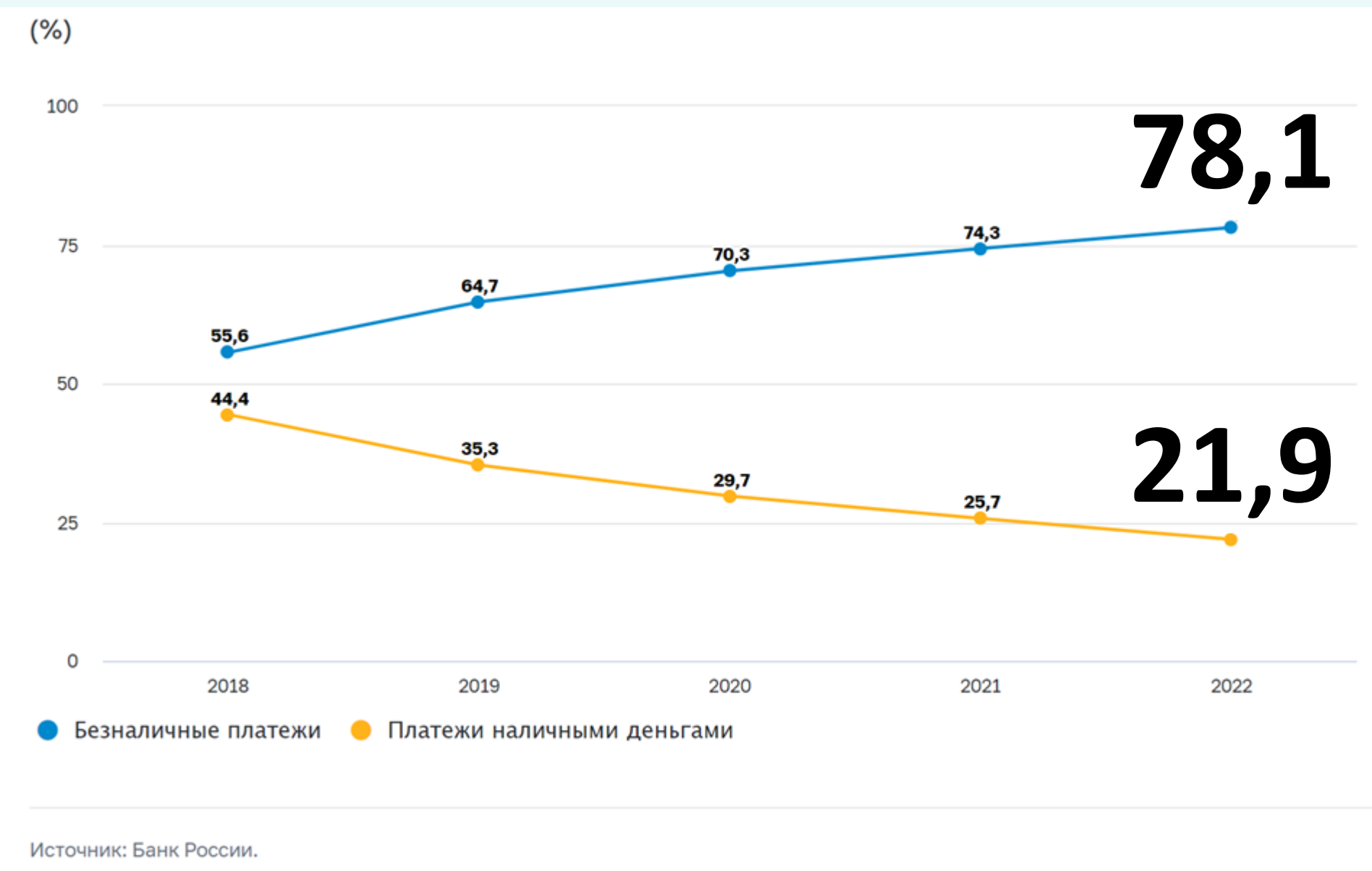


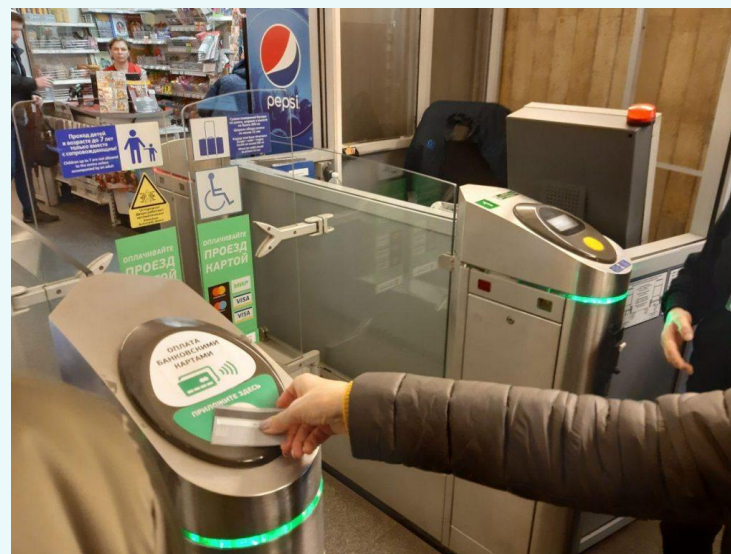
Выполнение требований регуляторов по импортозамещению зарубежных платежных криптографических HSM-модулей

Павел Луцик,
директор по развитию бизнеса



Доля наличных и безналичных платежей в РФ





Криптографическая защита карточных транзакций



Криптографическая защита карточных транзакций



Монополия Thales



80%

Карточных транзакций в мире
защищаются с помощью платежных
криптографических модулей Thales



Important Dates for payShield 9000

30th June 2020 – last time buy on hardware

31st December 2022 – end-of-life for support

Уход Thales из России



Масштаб

261

банков в РФ

242

из них «карточных»



Риски ухода Thales



Регуляторы



Банк России



НСПК
НАЦИОНАЛЬНАЯ
СИСТЕМА
ПЛАТЕЖНЫХ
КАРТ



Импортозамещение СЗИ

- ▶ Пр-1380 от 16.07.2016 (О переводе госорганов на отечественную криптографию)
- ▶ Нацпроект от 01.10.2018 (Цифровая экономика)
- ▶ 1236-ПП от 16.11.2015 (Об установлении запрета на допуск иностранного ПО)
- ▶ 166-УП от 30.03.2022 (О мерах по обеспечению технологической независимости и безопасности КИИ РФ)
- ▶ 250-УП от 01.05.2022 (О дополнительных мерах по обеспечению ИБ РФ)

С 31.03.2022 запрещено закупать иностранное ПО

С 01.01.2025 запрещено использовать иностранное ПО

Импортозамещение платежных криптографических модулей

Положение БР 719-П от 04.06.2020 «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств...»

Оператору (НСПК) национально значимой платёжной системы («МИР») необходимо обеспечить в информационной инфраструктуре платежной системы:

- ▶ с 01.01.2024 использование сертифицированных ФСБ платежных криптографических модулей, реализующих **иностранные** криптоалгоритмы
- ▶ с 01.01.2031 использование сертифицированных ФСБ платежных криптографических модулей, реализующих **иностранные и российские** криптоалгоритмы

Требования к СКЗИ (ФСБ России + Банк России)

№ФТ-56-3/32 от 28.02.2020 «Требования к СКЗИ в платежных устройствах...»



Банк России

Требования международных платежных систем (VISA, MASTER CARD) к платежным криптографическим модулям

- ▶ Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module **Modular Security** Requirements Version 3.0 June 2016.
- ▶ Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module **Modular Derived Test** Requirements Version 3.0 June 2016.

Попытка сертификации по требованиям международных платежных систем

- ▶ Проведено изучение открытой документации компании Thales
- ▶ Подготовлены технические решения по выполнению требований PCI
- ▶ Технические решения направлены в сертификационную лабораторию PCI

Избыточность сертификации по требованиям РСІ

- ▶ Международные платежные системы ушли из РФ и внутрироссийские операции по их картам обслуживает НСПК
- ▶ НСПК является **национально значимой** платежной системой и при ее функционировании должны выполняться положения 161-ФЗ "О НПС"
- ▶ Выполнение требований **ЦБ и ФСБ** являются **достаточным** условием для возможности эксплуатации модулей в национально значимых ПС, в том числе в НСПК
- ▶ В текущих условиях применение нормативных документов **РСІ избыточно**

Достаточность сертификации по требованиям ФСБ и ЦБ

Бюллетень НСПК от 31.05.2023 «О HSM, допустимых к использованию в ПС «Мир»

- ▶ С целью исполнения 719-П и 250-УП допустимо использование HSM, сертифицированных ФСБ России по классу не ниже КВ

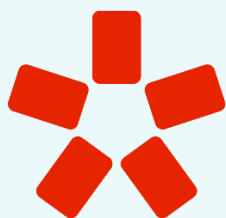


НСПК
НАЦИОНАЛЬНАЯ
СИСТЕМА
ПЛАТЕЖНЫХ
КАРТ



Совместимость с банковским ПО при импортозамещении платежных криптографических модулей

- ▶ Программа и методика испытаний **на совместимость** платежных криптографических модулей с банковским ПО

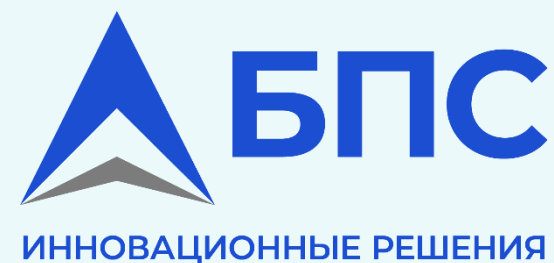


НСПК

НАЦИОНАЛЬНАЯ
СИСТЕМА
ПЛАТЕЖНЫХ
КАРТ



Банковское ПО



Российские сертифицированные платежные криптографические модули для импортозамещения



КриптоПро HSM 2.0 R3

СПБ HSM PS



Письмо ДИБ ЦБ РФ о необходимости импортозамещения платежных криптографических модулей в Банках

- ▶ Для обеспечения операционной надежности (787-П от 12.01.2022) и в связи с уходом из РФ компании Thales рекомендуется провести тестирование модулей, соответствующих требованиям НСПК (от КристоПро и СПБ), в качестве возможной замены иностранным решениям



Банк России



Что происходит сейчас?

- ▶ Продолжает функционировать рабочая группа в составе: ЦБ, ФСБ, НСПК, Банки, разработчики HSM и банковского ПО
- ▶ Банки продолжают тестировать отечественные криптографические модули
- ▶ ЦБ проводит многосторонние встречи для разрешения возникающих при тестировании Банками сложностей и ускорения процесса импортозамещения

Спасибо!

Личный адрес: plutsik@cryptopro.ru

Общие вопросы: info@cryptopro.ru

Телефон: 8(926)185-24-42

