СПБ | СИСТЕМЫ ПРАКТИЧЕСКОЙ БЕЗОПАСНОСТИ

ИМПОРТОЗАМЕЩЕНИЕ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СИСТЕМАХ ПЛАТЁЖНЫХ КАРТ

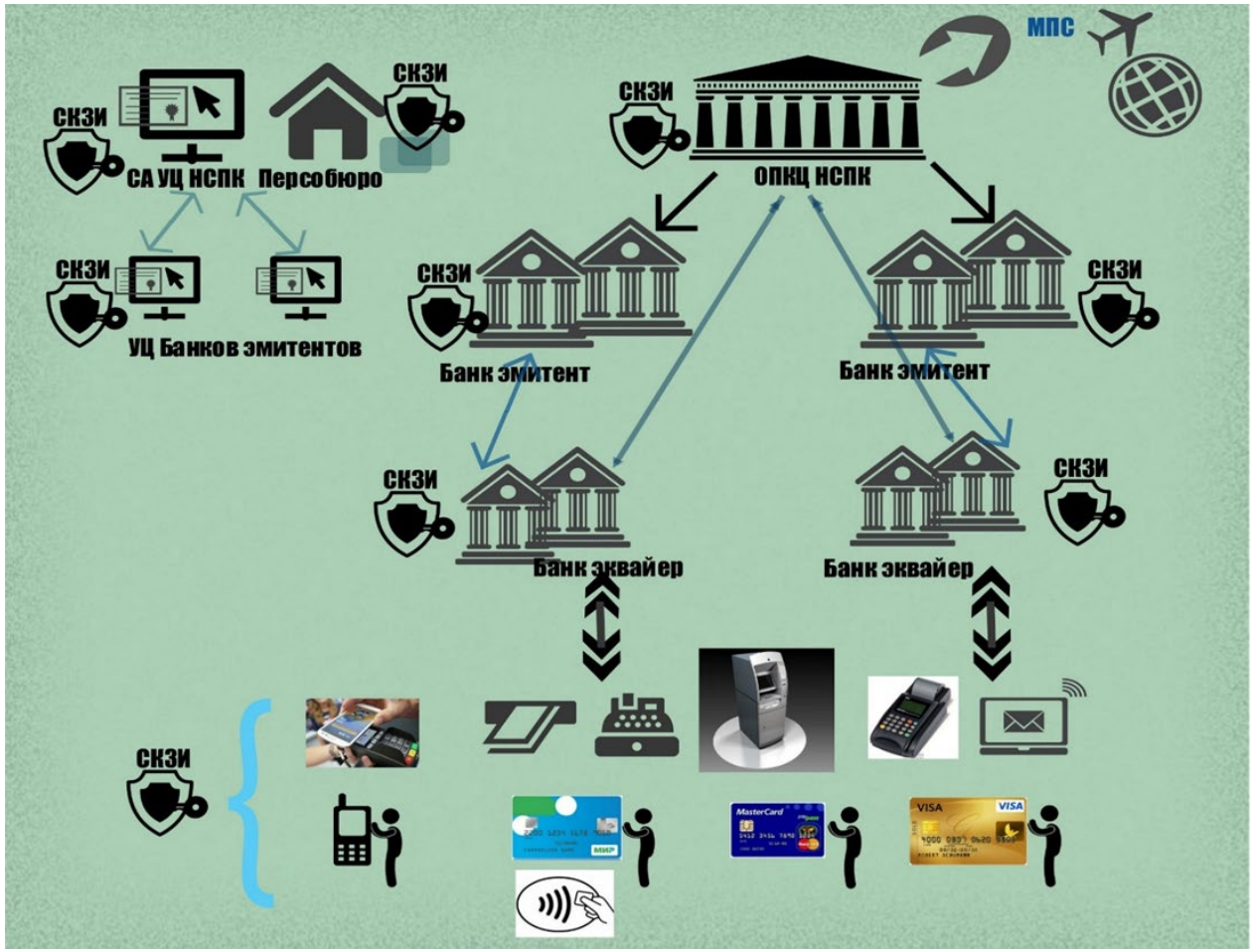
«Новые» угрозы и практические шаги

ВЗГЛЯД ВЕНДОРА

Елена Мареева,

заместитель генерального директора по НТР

Атаки на систему платёжных карт – это целевые атаки на элементы инфраструктуры платёжных карт



«Новые» угрозы – формулировки 2015-2016 года

«Новые» угрозы – формулировки 2015-2016 года

Угрозы	Последствия
Управление ключевой информацией по зарубежным технологиям и стандартам, в том числе , из-за пределов РФ	Возможность несанкционированного управления ключами, отзыв сертификатов, работа на договорных ключах
Риск введения санкций против российской платежной системы, например, прекращение поставок оборудования	Нарушение функционирования российской платежной системы даже внутри РФ
Наличие скрытых функциональных возможностей (программные и/или аппаратные закладки) в импортном оборудовании	Несанкционированный доступ к информационным активам системы платёжных карт (ПД, PIN-кодам, информации о состоянии денежных счетов и т.д.), отказ в предоставлении услуг
Технологическая зависимость от импортного оборудования	Развитие национальной системы платёжных карт и применяемого оборудования по планам, навязанным иностранными технологиями и темпами развития
Скрытые функциональные возможности и известные уязвимости зарубежной криптографии	Несанкционированный доступ к информационным активам национальной системы платёжных карт, нарушение работоспособности системы
Замкнутость системы, невозможность парирования угроз, актуальных для национальной платёжной системы	Несанкционированный доступ к информационным активам национальной платёжной системы, нарушение работоспособности системы
Несоответствие требованиям надзорных и регулирующих органов, действующему законодательству РФ в области ИБ	Возникновение юридических препятствий для применения импортного оборудования, невозможность проведения сертификации на соответствие требованиям и нормам ИБ РФ

«Новые» угрозы и практические шаги - нормотворчество

2014 год – отключение от МПС (Visa и MasterCard) и запрет использования технологии в Крыму и банках, попавших под санкции.

Первый звонок

1. **План мероприятий по внедрению СКЗИ в НСПК, от 14.07.2015 утв. ЦБ РФ, 8 Центр ФСБ и АО НСПК**
2. **Корректировка 382-П (719-П), новые требования о применении в системах платёжных карт СКЗИ, являющихся российскими аналогами к 2024, с РКА к 2031 году**
3. **РГ в ТК-26. Утверждение 8 рекомендаций Росстандарта по использованию РКА в НСПК**
4. **РГ в ЦБ –результаты работы:**
   - **Разработка и утверждение требований к СКЗИ в информационной инфраструктуре платёжных систем http://www.cbr.ru/content/document/file/104752/ft_32.pdf**
   - **Разработка и утверждение ФТТ к аппаратному модулю безопасности (HSM -модуль) http://www.cbr.ru/content/document/file/104755/ft_35.pdf, к платёжным картам http://www.cbr.ru/content/document/file/104754/ft_34.pdf, к платёжным устройствам с терминальным ядром http://www.cbr.ru/content/document/file/104753/ft_33.pdf**
   - **Технологические карты осуществления переводов денежных средств, описывающие инфраструктурные процессы действующей системы проведения карточных платежей и эмиссии карт на территории РФ**
5. **Создание Центра тестирования во ФГУП НИИ «Восход»**

«Новые» угрозы и практические шаги - нормотворчество

ПОЛОЖЕНИЕ ЦБ РФ от 4 июня 2020 г. N 719-п «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств…» (ранее 382-П)

Новые требования о применении СКЗИ в системах платёжных карт :

- **являющихся российскими аналогами вступает в силу с 01.01.2024**

  5.5. абз.2 - **Оператор значимой платежной системы в соответствии с правилами платежной системы должен обеспечить использование в аппаратных модулях безопасности информационной инфраструктуры платежной системы СКЗИ, реализующих криптографические алгоритмы, не определенные национальными стандартами РФ, имеющих подтверждение соответствия требованиям, установленным ФОИВ в области обеспечения безопасности**

- **и с РКА вступает в силу с 01.01.2031**

  5.5. абз.3 - **в аппаратных модулях безопасности информационной инфраструктуры платежной системы СКЗИ, реализующих иностранные криптографические алгоритмы и криптографические алгоритмы, определенные национальными стандартами Российской Федерации, имеющих подтверждение соответствия требованиям, установленным ФОИВ в области обеспечения безопасности**

  5.5. абз.4 – аналогичный абз. 3 **про СКЗИ в иных технических средствах информационной инфраструктуры платежной системы, используемых при осуществлении переводов денежных средств**

  Разработка и эксплуатация СКЗИ, указанных в абзацах втором - четвертом пункта 5.5, должны проводиться в соответствии с Положением ПКЗ-2005.

Криптографические алгоритмы и механизмы в НСПК РФ ПК №3 ТК-26 – готовимся к 2031 году

ПК №3 организован в соответствии с утверждённым Планом мероприятий по внедрению СКЗИ в НСПК, от 14.07.2015

Первое заседание ПК №3 состоялось 25.12.2015 года. В рамках ПК №3 в январе 2016 года создана рабочая группа. В 2016-2018 годах рабочей группой ПК №3 разработаны и выпущены рекомендации по стандартизации:

- **Р 1323565.1.011-2017** «Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN»*
- **Р 1323565.1.009-2017** «Использование алгоритмов блочного шифрования при формировании прикладных криптограмм в платежных системах»*
- **Р 1323565.1.008-2017** «Использование режимов алгоритма блочного шифрования в защищенном обмене сообщениями между эмитентом и платежным приложением»*
- **Р 1323565.1.007-2017** «Использование алгоритмов блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN» (планируется обновление в 2022 году)*
- **Р 1323565.1.010-2017** «Использование функции диверсификации для формирования производных ключей платежного приложения»
- **Р 1323565.1.013-2018** «Использование режимов алгоритма блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт»*
- **Р 1323565.1.016-2018** «Использование режимов алгоритма блочного шифрования, алгоритмов электронной подписи и функции хэширования в процедуре оффлайновой аутентификации платежного приложения»
- **Р 1323565.1.015-2018** «Задание параметров алгоритмов электронной подписи и функции хэширования в профиле EMV сертификатов открытых ключей платежных систем»*

(* - планируется обновление в 2022 году)

Практические шаги – что было сделано после первого звонка вендором HSM модуля (ViPNet HSM PS)

Проведена инициативная разработка HSM как СКЗИ класса КВ с реализацией российских и импортных КА

↓

Изготовлены опытные образцы, проведены их ТИ, получен сертификат соответствия СКЗИ класса КВ

↓

Проведено тестирование совместимости с банковским ПО (Way4, TranzWare)

↓

Проведено тестирование в банках (Сбербанк, банк Россия)

↓

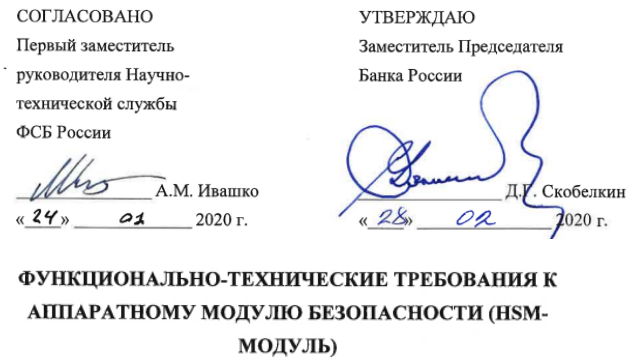
Разработаны рекомендации по использованию РКА в EMV
Участие в работе РГ в ЦБ

«Новые» угрозы и практические шаги - нормотворчество

2022 год – существенное расширение санкционного списка банков, запрет на поставки в РФ оборудования и технологий.

Второй звонок

1.Требуется корректировка и актуализация ранее принятых документов – технологические карты и ФТТ в соответствии с утверждённым документом «Порядок взаимодействия участников процесса поддержания актуального состояния ФТТ к СКЗИ»


СОГЛАСОВАНО
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020 г.

УТВЕРЖДАЮ
Заместитель Председателя Банка России
Д.Г. Скобелкин
«28» 02 2020 г.

ФУНКЦИОНАЛЬНО-ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К АППАРАТНОМУ МОДУЛЮ БЕЗОПАСНОСТИ (HSM-МОДУЛЬ)

2.РГ в ТК-26. Новые рекомендации в области электронной коммерции

План разработки документов по стандартизации в ТК 26 в 2022 году предусматривает разработку методических рекомендаций ТК 26 для реализации сервисов электронной коммерции в национальной системе платёжных карт:

- Использование российских криптографических алгоритмов в методе формирования ключей транзакций (DUKPT – Derived unique key per transaction).
- Формат и защита ключевого контейнера (TR31).
- Механизмы шифрования, сохраняющего формат (FPE).
- Механизмы формирования одноразовых паролей (OTA).

Практические шаги – что делаем после второго звонка SPB HSM ₽S

Проведена переработка аппаратной платформы и ПО (лицензий) в соответствии с требованиями к СКЗИ ft_32 и ФТТ к HSM -модулю ft_35

⇩

Изготовлен первый опытный образец **SPB HSM ₽S High**, проведено первое тестирование совместимости с ПО БПЦ (SmartVista)

⇩

Требуется тестирование совместимости с банковским ПО других производителей OW (Way4), CompasPlus (TranzWare)

⇩

Требуется тестирование в банках и ПС (приглашаем желающих)

Возможна организация тестирования по VPN

⇩

Требуется провести сертификационные исследования на соответствие требованиям к СКЗИ класса КВ и специфическим ft_32 и получить сертификат

⇩

Изготовление серии и организация внедрения

SPB HSM ₽S - https://systempb.ru/catalog/produkty/hsm-ps/

Практические шаги – что требует решения *Cito*

Каким требованиям безопасности должен соответствовать HSM модуль?

- ***Требования к СКЗИ и ФТ-32 НТС ФСБ***
- ***Требования PCI PTS HSM Modular Security Requirements Version 3.0 June 2016 (уже есть 4.0) и PCI PTS Device Testing and Approval Guide***

Как можно организовать сертификацию в PSI при наличии санкций? Необходимо знать позицию ЦБ и НСПК

Заместитель Председателя Банка России
_____ Д.Г. Скобелкин
«15» 01 2020 г.

Первый заместитель руководителя Научно-технической службы ФСБ России
_____ А.М. Ивашко
«24» 01 2020 г.

ТРЕБОВАНИЯ К СРЕДСТВАМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ПЛАТЕЖНЫХ УСТРОЙСТВАХ С ТЕРМИНАЛЬНЫМ ЯДРОМ, СЕРВЕРНЫХ КОМПОНЕНТАХ ПЛАТЕЖНЫХ СИСТЕМ (HSM МОДУЛЯХ), ПЛАТЕЖНЫХ КАРТАХ И ИНЫХ ТЕХНИЧЕСКИХ СРЕДСТВАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПЛАТЕЖНОЙ СИСТЕМЫ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ, УКАЗАННЫХ В ПУНКТЕ 2.20 ПОЛОЖЕНИЯ БАНКА РОССИИ ОТ 9 ИЮНЯ 2012 Г. № 382-П

Практические шаги – что требует решения *Cito*

Требуется поддержание в актуальном состоянии документов, определяющих функционально-технические требования.

Регулирование через РГ при ЦБ возможно, но как это сделать оперативно, как попасть в «закрытый клуб» участников?

Практические шаги – что требует решения *Cito*

Как с минимальными затратами организовать тестирование HSM модулей. В настоящее время требуется пройти функциональное тестирование:

1. У разработчиков банковского ПО, поддерживающих процессы (эмиссия, эквайринг, авторизация, мобильные платежи, 3-DSecure) систем платёжных карт. У каждого и по каждому процессу.

2. В банке, персобюро, платёжной системе…

3. Каждой новой версии с каждым новым релизом банковского ПО

Как минимизировать разнообразие?

Банк или ПС не выбирают HSM модуль, банк выбирает вендора программного обеспечения, а вендор включает HSM модуль в список совместимости.

Центр тестирования введён в опытную эксплуатацию, но пока не может заменить ни первую, ни вторую ступени тестирования

Практические шаги – что требует решения *Cito*

Проверка корректности встраивания в систему в соответствии с ПКЗ-2005. Необходимо организовать и поддержать методически.

Как организовать эксплуатацию. Требуется обучить сотрудников работе с новым оборудованием.

Как обеспечить плавный переход на новое оборудование, особенно на высоконагруженных участках авторизации транзакций с переносом баз данных держателей карт. Индивидуальный план миграции для каждого банка?

Практические шаги – есть решение от вендора SPB HSM ₽S

- Инициализация платёжных карт при их производстве
- Эмиссия платёжных карт, включая генерацию секретных величин, электрическую персонализацию и печать пин-конвертов
- Авторизация платёжных транзакций
- Эквайринг, обработка транзакций от платёжных устройств
- 3-D Secure
- Поддержка режима работы НСПК в качестве ОПКЦ
- Генерация, смена, резервирование, экспорт локальных, зональных, терминальных, транспортных мастер ключей, которые используются в вышеперечисленных процессах

Практические шаги – есть решение от вендора SPB HSM ₽S

Характеристика	Параметры
Интерфейс, протокол и API с HOST системой	*SPB HSM ₽S high* - ***10 GbE, UDP, TCP/IP с прикладным протоколом «команда-ответ»***
	SPB HSM ₽S base - ***1GbE, UDP, TCP/IP с прикладным протоколом «команда-ответ»***
Производительность	*SPB HSM ₽S high* ***– 40 000 tps****
	SPB HSM ₽S base ***– 1000 tps****
Интерфейс и протокол управления	*1 GbE, Web интерфейс по защищённому TLS в соответствии с ГОСТ Р 1323565.1.030-2018 «Использование РКА в протоколе безопасности транспортного уровня TLS»*
Лицензии (ПО)	*1 Основная или Core (эмиссия, эквайринг, авторизация, 3-DS, управление ключами для НСПК и МПС)* *2 Обеспечивающая совместимость или Legacy* *3 Обеспечивающая совместимость с IC 1119-0902 или Legacy P3*

** - число перешифрований PIN блока с ключа на ключ в секунду*

Практические шаги – есть решение от вендора SPB HSM ₽S

Характеристика	Параметры
Иностранные криптографические алгоритмы и механизмы	*DES/3DES – NIST FIPS 46-3 SP 800-67 и ISO 10116,* *AES – NIST FIPS 197,* *RSA – RFC 3447 NIST FIPS 186-4,* *SHA-1 – RFC 3174 и NIST FIPS 180-4,* *SHA-224, SHA-384, SHA-256, SHA-512 – ISO/IEC 10118-2 и NIST 180-4,* *MAC – ISO 9797 и NIST FIPS 198-1, HMAC – ISO/IEC 9797-2*
	Global Platform v.2.2.1, *EMV CPS 1.1, EMV3.1.1, EMV 4.1, EMV 4.3 (ARQC/ARPC/AAC), IDN,* *Union Pay (ARQC/ARPC), CVP/iCVP/CVP2, CVC/CVV/CVC3,* *PVV, MST ,MasterCard CAP,CAVV,* *PIN Block (ISO 9564-1), в т.ч. ISO-0, ISO-3, ISO-4,* *IBM 3624, ANSI X9-24 (DUKPT)*
Российские криптографические алгоритмы	*Блочный шифр «Кузнечик» ГОСТ Р 34.12-2015 в режимах ГОСТ Р 34.13-2015, хэш функция ГОСТ Р 34.11-2012, электронная подпись ГОСТ Р 34.10-2012*
Форматы ключевых контейнеров	*ASC X9 TR-31-2018, Variant Scheme, ANSI X9.17, PKCS #1 v1.5*

Практические шаги – есть решение от вендора SPB HSM ₽S

Характеристика	Параметры
Конструктивное исполнение	*2U для монтажа в 19”стойку, глубина -700 мм* *Конструкция, обеспечивающая защиту от НСД, использование различных систем обнаружения НСД и датчиков вскрытия – механические микропереключатели, датчик объема, деление на отсеки* *Защита от ПЭМИН обеспечивается рядом конструктивных, схемотехнических, алгоритмических мер* *Активная система охлаждения*
Электропитание	*220 В, резервированное питание, возможность горячей замены блоков питания на объекте эксплуатации*
Локальные мастер ключи	*Генерация с использованием ФДСЧ, вариантный метод и метод keyblock хранения ключей под LMK.* *Стирание при обнаружении попытки НСД и по кнопке экстренного стирания.* *Резервирование в виде компонент на смарт-картах с применением конструктивных и алгоритмических мер защиты*

Будем ждать третий звонок??

Спасибо за внимание!

Вопросы???

СПБ | СИСТЕМЫ ПРАКТИЧЕСКОЙ БЕЗОПАСНОСТИ

Санкт-Петербург, ул. Политехническая, 22 АБ
+7 (812) 468-15-61 | systempb.ru