Подготовка стандартов, регламентирующих использование российских криптографических алгоритмов и механизмов в национальной системе платежных карт (ТК 26)

Сергей Петренко

Менеджер по развитию криптографических продуктов

Содержание доклада

Введение

Организационно-правовая сторона

Поддержка международных платежных систем

Техническая сторона

Заключение

НСПК – Национальная система платежных карт. Платежная система, созданная и функционирующая в соответствии с 161-ФЗ, целью которой является обеспечение бесперебойности, эффективности и доступности оказания услуг по переводу денежных средств.

Структура нормативных документов

1. N 161-ФЗ "О национальной платежной системе“
2. Положение ЦБ РФ № 382-П
3. План мероприятий (дорожная карта) по внедрению СКЗИ в НСПК

N 161-ФЗ "О национальной платежной системе“ от 27.06.2011

Статья 27. Обеспечение защиты информации в платежной системе

2. Контроль и надзор за выполнением требований, установленных Правительством РФ, осуществляются ФОИВ, уполномоченным в области обеспечения безопасности, и ФОИВ, уполномоченным в области ПДТР и ТЗИ…

3. Операторы … обязаны обеспечивать ЗИ при осуществлении переводов денежных средств в соответствии с требованиями, установленными Банком России, согласованными с ФОИВ, предусмотренными частью 2 настоящей статьи.

ЦБ РФ устанавливает требования к ЗИ и согласовывает их с Регуляторами.
Все участники НПС обязаны соблюдать требования.
Это сделано в положении ЦБ РФ N 382-П.

N 382-П, ..о требованиях к ЗИ при осуществлении переводов

2.9.1. Работы по обеспечению ЗИ с помощью СКЗИ проводятся в соответствии с N 63-ФЗ "Об ЭП", ПКЗ-2005 и технической документацией на СКЗИ.
В случае если операторы ... применяют **СКЗИ российского производителя**, указанные СКЗИ **должны иметь сертификаты** уполномоченного государственного органа.

2.9.5. **Оператор платежной системы определяет необходимость использования СКЗИ**.

АО «НСПК» (Оператор) сделает это, когда будут готовы необходимые методические рекомендации по стандартизации для применения отечественных СКЗИ для защиты банковских транзакций

План мероприятий по внедрению СКЗИ в НСПК, от 14.07.2015

Утвержден Первым заместителем председателя ЦБ РФ, согласован Начальником 8 Центра и Генеральным директором АО «НСПК»

Предписывает:

1. Подготовить предложения по использованию отечественной криптографии
2. Создать подкомитет при ТК 26

Создан ПК 3. Руководитель Голдовский И.М., АО «НСПК»

В рамках ПК 3 создана РГ, руководитель Мареева Е., «Системы практической безопасности»

3. Предоставить проекты методических рекомендаций
4. Зарегистрировать методические рекомендации

Резюме по организационно-правовой части

1. ЦБ РФ устанавливает требования к ЗИ и согласовывает их с Регуляторами. Все участники НСПК обязаны соблюдать требования.

2. Согласно N 382-П Оператор системы (т.е. АО «НСПК») должен определить необходимость использования СКЗИ.
   Что и будет сделано после подготовки необходимых методических рекомендаций по стандартизации.

3. Рабочая группа ПК 3 ТК 26 разрабатывает проекты рекомендаций.

Согласно Стратегии развития НСПК, система должна поддерживать как **национальные платежные инструменты,** так и **международные платежные карты** на территории РФ

Структура международных стандартов платежных систем

1. Стандарты EMVCo
2. Стандарты PCI

Краткая суть:

Оборудование и ПО, применяемое для электронных платежей по картам международных платёжных систем, должно быть сертифицировано на соответствие стандартам EMV и PCI.

1. Сертификация **EMV** подтверждает соответствие электрическим, механическим и функциональным параметрам.
2. Сертификация **PCI** подтверждает соответствие требованиям по безопасности (конструктивной, программной и алгоритмической защите данных).

Использование HSM зарубежных производителей в банках ведет к серьезным рискам, таким как:
- запрет использования технологии или прекращение поставок оборудования в РФ;
-управляемые «нарушителем» результаты работы криптоалгоритмов;
-отказ в обслуживании или получение несанкционированного доступа к данным.

Для выполнения одной из основных задач НСПК по построению национальной операционно-независимой платформы для обработки операций как международных, так и национальных платежных карт на территории РФ эту ситуацию необходимо менять.

Построение гибридной архитектуры

Все оборудование
(карты, терминалы, HSM) должно:
-Поддерживать функционал:
-**EMVCo&PCI** и **ПС МИР** в части СКЗИ
-Иметь двойную сертификацию: **EMVCo&PCI** и **ФСБ РФ**
(не факт, что это возможно)
- Иметь независимые СКЗИ (автономные или в составе устройств) с разделением на прикладном уровне транзакций по МПС и ПС МИР. В этом случае каждое СКЗИ имеет свою систему требований и соответственно сертификатов

Двойная сертификация: EMVCo&PCI и ФСБ РФ

Варианты:

1. Создание в РФ аккредитованных **EMVCo** и **PCI** лабораторий

- По линии EMVCo обсуждают в Минпромторге
- По линии PCI обсуждают в ПК 3 ТК 26

2. Отказ от сертификации EMVCo и PCI

То есть функциональная поддержка в отечественных решениях стандартов **EMVCo&PCI** и **поддержка ПС МИР**, но сертификация только в ФСБ РФ по линии СКЗИ

Есть основания полагать, что вариант 2 возможен, так как сейчас банковские HSM в РФ не имеют сертификатов PCI HSM

«Новая » сертификация для работы в рамках НСПК

В АО НСПК в настоящее время формируются требования
к функциональным характеристикамоборудования.
Предполагается, что проверку на соответствие данным требованиям будут проводить аккредитованные НСПК лаборатории, которые будут выдавать заключения о соответствии функциональных характеристик устройств требованиям ПС «МИР».
В части СКЗИ для применения в системе необходимо будет иметь сертификат ФСБ России на СКЗИ и заключение аккредитованной лаборатории о соответствии характеристик.

Перечень стандартов

Экспертами рабочей группой ПК 3 ТК 26 определен перечень рекомендаций по вопросам, относящимся к стандартизации в области криптографической защиты информации, необходимых для применения российских СКЗИ для защиты информации при осуществлении банковских транзакций и эмиссии платёжных карт

В настоящее время перечень содержит 12 документов

Статус разработки

На текущий момент подготовлено:
- 4 проекта методических рекомендаций, содержащих описание предлагаемого решения (3 шт. – СПБ и ИнфоТеКС, 1 шт. – УЭК)
- 4 криптографических исследования и обоснования криптографических качеств (3 шт. – КриптоПро, 1 шт. – ИнфоТеКС)

Находится в процессе:
- 2 проекта методических рекомендаций (СПБ)

№	Краткое название	Полное официальное название	Проект методических рекомендаций	Результаты криптографических исследований
1	KDF	Использование функции диверсификации для формирования производных ключей платежного приложения	Да	Да
2	VKO	Использование алгоритмов согласования ключа и блочного шифрования при оффлайновой проверке PIN	Да	Да
3	ARQC	Использование криптографических алгоритмов при формировании криптограмм в электронной коммерции	Да	Да
4	SCP-F2	Использование режимов алгоритма блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт	Да	Да
5	3OC	Использование режимов алгоритма блочного шифрования и имитозащиты в защищённом обмене сообщениями между эмитентом и платёжным приложением	В процессе	
6	CVV/PVV	Использование алгоритма блочного шифрования при формировании проверочного значения платежной карты и проверочного значения PIN	В процессе	

infotecs

Спасибо за внимание!

Сергей Петренко
Sergey.Petrenko@infotecs.ru
+7 (495) 737-61-92 (5240)
+7 (903) 687-69-97