НСПК

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПЛАТЕЖНОЙ СИСТЕМЕ «МИР»

Фомичев Максим Викторович

Начальник Отдела сопровождения информационной безопасности и развития систем защиты АО «НСПК»

МИР

Москва, 2017 г.

Национальная система платежных карт

Акционерное общество «Национальная система платежных карт» (АО «НСПК»)

создано 23 июля 2014 г.

Деятельность АО «НСПК» регулируется Федеральным законом № 161-ФЗ «О национальной платежной системе», «Стратегией развития Национальной платежной системы» и «Концепцией создания национальной системы платежных карт». 100% акций АО «НСПК» принадлежит Центральному Банку Российской Федерации.

Развитие национальной платежной системы – ключевой фактор обеспечения суверенитета национального платежного пространства. Национальная платежная система гарантирует безопасность и бесперебойность проведения внутрироссийских транзакций по банковским картам.

Миссия компании: «Для всех жителей России и для государства создаем и развиваем доступные, удобные и выгодные платежные сервисы, поддерживая суверенитет страны и формируя стандарты индустрии».

В задачи АО «НСПК» входят обеспечение бесперебойности операций по картам международных платежных систем на территории России, построение и развитие российской системы платежных карт.

НСПК
НАЦИОНАЛЬНАЯ СИСТЕМА ПЛАТЕЖНЫХ КАРТ

АО «НСПК» в платежной системе «Мир»

АО «НСПК» в национальной платежной системе «Мир» является:

– Оператором платежной системы «Мир»;
– Оператором услуг платежной инфраструктуры;

Основные цели и задачи создания национальной платежной системы «Мир»:

- Предоставление надежной услуги денежных переводов с использованием национальных платежных инструментов;
- Повышение доверия населения к безналичным способам оплаты;
- Создание российского платежного пространства, не зависящего от иностранных компаний;
- Эмиссия национальных платежных инструментов - банковских карт «Мир»;
- Представление платежной карты «Мир» на международном рынке.

Платежная система «Мир» в цифрах

376

банков-участников платежной системы «Мир»

81

банков выпускают платежную карту «Мир»

229

банков принимают карту «Мир» в своих устройствах

6 319 956

карт выпущено на данный момент

Платежная система «Мир» в цифрах

Правила платежной системы «Мир»

Платежная система «Мир», ПС «Мир» **- совокупность организаций, взаимодействующих по Правилам в целях осуществления перевода денежных средств, включающая Оператора, Операторов услуг платежной инфраструктуры и Участников.**

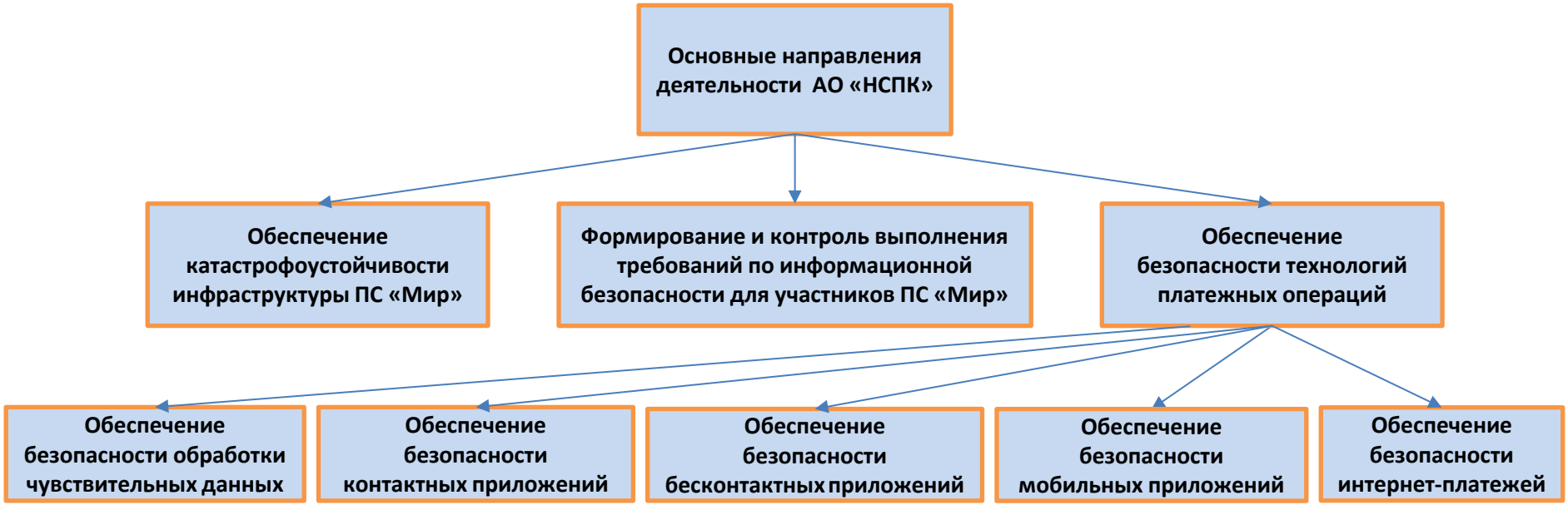
Целью организации платежной системы «Мир» является обеспечение бесперебойности, эффективности и доступности оказания услуг по переводу денежных средств с использованием платежных карт и иных электронных средств платежа, предоставляемых Клиентам Участниками в соответствии с Правилами.

Правила разработаны в соответствии с требованиями Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе», нормативных правовых актов Российской Федерации.

Участники присоединяются к Правилам в соответствии с порядком, определенным в Правилах. Присоединение к Правилам означает принятие Участником Правил и Стандартов платежной системы «Мир» в целом без каких-либо изъятий или ограничений!

Правила и Стандарты ПС «Мир» являются обязательными для исполнения всеми субъектами ПС «Мир»!

Требования по обеспечению ИБ в ПС «Мир»



Обеспечение информационной безопасности - задача каждого Участника ПС «Мир»!

Требования по обеспечению ИБ в ПС «Мир»

Объектами защиты в платежной системе «Мир» являются:

- Платежная информация (данные)
- Отправитель
- Получатель
- Работник, обеспечивающий работу системы
- Работник, обеспечивающий безопасность системы
- Процессы управления ИТ составляющей системы
- Процессы управления ИБ составляющей системы
- Процессы управления бизнес-составляющей системы
- Банк – эмитент
- Банк – эквайрер
- Процессинговый центр
- Платежный агрегатор
- Платежная система МИР
- Оператор связи
- ТСП
- Посредник Банка в выплате платежа
- Аппаратное обеспечение работника
- Операционная система работника
- Прикладное программное обеспечение работника
- Карта (чип)
- Элемент безопасности мобильного устройства
- Элемент безопасности веб-сайта эквайринга
- Компоненты защиты интернет-платежа (MirAccept)
- Платежный терминал / касса
- Банкомат
- Устройство генерации, хранения и обработки крипто-ключей
- Средство обработки платежа
- Средство маршрутизации платежа
- Средство защиты периметра
- Каналы связи
- Контактная карта – терминал
- Мобильное устройство (бесконтактная карта) – терминал
- Терминал – касса
- Касса – Сервер ТСП
- Сервер ТСП – Периметр ТСП
- Периметр ТСП – Периметр оператора связи ТСП
- Периметр оператора связи ТСП – Сервер оператора связи ТСП
- Периметр оператора связи ТСП - Периметр оператора связи Процессинга
- Периметр оператора связи Процессинга - Сервер оператора связи Процессинга
- Периметр оператора связи Процессинга - Периметр Процессинга
- Периметр Процессинга – Сервер Процессинга
- Периметр Процессинга - Периметр оператора связи ПС
- Периметр оператора связи ПС - Сервер оператора связи ПС
- Периметр оператора связи ПС - Периметр ПС
- Периметр ПС – Сервер ПС
- Периметр ПС - Периметр оператора связи Банка
- Периметр оператора связи Банка – Сервер Банка
- Периметр Банка – Периметр Посредника
- Периметр Посредника – Сервер Посредника
- Сервер Посредника – Устройство выдачи платежа
- Данные, необходимые для функционирования прикладного ПО работника

Требования по обеспечению ИБ в ПС «Мир»

В соответствии с Правилами платежной системы «Мир» основными нормативными документами, регламентирующими выполнение требований по обеспечению информационной безопасности, для всех субъектов ПС «Мир» являются:

- **Положение Банка России № от 9 июня 2012 г. № 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»;
- **Международный стандарт безопасности данных индустрии платежных карт PCI DSS** (Payment Card Industry Data Security Standard);

Субъекты Системы принимают на себя обязательства по обеспечению защиты информации при осуществлении операций в ПС «Мир» в соответствии с требованиями Правил, Стандартов ПС «Мир», законодательства Российской Федерации, а также обязательства по выполнению требований международного стандарта безопасности данных индустрии платежных карт PCI DSS.

Требования по обеспечению ИБ в ПС «Мир»

№ 1216/796

Сертификат Соответствия
CERTIFICATE OF COMPLIANCE

Digital Security

Настоящий сертификат подтверждает, что проведенная
ООО «Диджитал Секьюрити» проверка показала соответствие

АО «НСПК»
115184, Москва, ул. Большая Татарская, д.11

требованиям стандарта PCI DSS версии 3.2
13 декабря 2016

National System of Payment Cards
Joint-stock Company
11 Bolshaya Tatarskaya Street, Moscow, Russia, 115184

has been assessed by Digital Security Ltd. and found to be
in compliance with the requirements of PCI DSS version 3.2
on December 13, 2016

This is to certify that

Сертификат действителен в течение 12 месяцев
This certificate remains valid for 12 month

Илья Медведовский, генеральный директор
Ilya Medvedovsky, CEO

Андрей Гайко, ведущий QSA-аудитор
Andrey Gaiko, lead QSA

Digital Security является QSA-аудитором, сертифицированным Советом PCI SSC / Digital Security is a Qualified Security Assessor (QSA) certified by PCI SSC
Digital Security: +7 (812) 703-15-47, www.dsec.ru. 197046, Россия, г. Санкт-Петербург, ул. Петроградская набережная 16/ Petrogradskaya naberezhnaya, 16, Saint-Petersburg, Russia

Требования по обеспечению ИБ в ПС «Мир»

Построение и обслуживание защищенной сети и систем

1. Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт

2. Не использовать пароли и другие системные параметры, заданные производителем по умолчанию

Защита данных держателей карт

3. Обеспечить безопасное хранение данных держателей карт

4. Обеспечить шифрование данных держателей карт при их передаче через сети общего пользования

Программа управления уязвимостями

5. Защищать все системы от вредоносного ПО и регулярно обновлять антивирусное ПО

6. Разрабатывать и поддерживать безопасные системы и приложения

Внедрение строгих мер контроля доступа

7. Ограничить доступ к данным держателей карт в соответствии со служебной необходимостью

8. Определять и подтверждать доступ к системным компонентам

9. Ограничить физический доступ к данным держателей карт

Регулярный мониторинг и тестирование сети

10. Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт

11. Регулярно выполнять тестирование систем и процессов обеспечения безопасности.

Поддержание политики информационной безопасности

12. Разработать и поддерживать Политику информационной безопасности для всего персонала организации

Отчетность Участников ПС «Мир»

1. Отчетность по форме № 0403203 Банка России «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

В срок, не позднее 15-го рабочего дня месяца, следующего за отчетным!

При отсутствии Инцидентов в отчетном периоде отчет не предоставляется!

2. Отчетность по форме № 0403202 Банка России «Сведения о выполнении операторами платежных систем, операторами услуг платежной инфраструктуры, операторами по переводу денежных средств требований к обеспечению защиты информации при осуществлении переводов денежных средств».

Теперь только по письменному запросу Оператора ПС «Мир» АО «НСПК»!

Что нового в платежной системе «Мир»?

АО «НСПК», как Оператор платежной системы «Мир», вошло в состав Совета по стандартам безопасности данных индустрии платежных карт (Payment Card Industry Security Standards Council, PCI SSC).

Основная задача Совета PCI SSC – создание универсального международного стандарта безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard, PCI DSS). Платежные системы – участники Совета, в рамках его деятельности определяют программы подтверждения соответствия стандартам PCI для всех категорий своих партнеров – Банков, поставщиков услуг и торгово-сервисных предприятий. Платежная система «Мир» в рамках построения собственной системы стандартов безопасного хранения и передачи данных присоединяется к международным стандартам PCI, а также сможет включать в них дополнительные региональные требования к участникам. АО «НСПК» будет доступно использование общепризнанной системы сертификации по девяти стандартам PCI, при этом новые требования, предложенные недавно сформированной Экспертной рабочей группой, состоящей из ведущих QSA-аудиторов Российской Федерации и специалистов АО «НСПК», для российского рынка, будут учитываться глобальной системой контроля и аудита индустрии платежных карт.

PCI Security Standards Council®

Новые технологии аутентификации в ПС «Мир»

Одно платежное приложение — много форм-факторов

Карта с контактным чипом

Контактно-бесконтактная карта

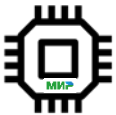
Контактные

Бесконтактный стикер

Бесконтактные

USIM
«на SIM-карте»

eSE
«В чипе» на борту телефона



rSE
Извлекаемая карта в формате SD

Мобильные

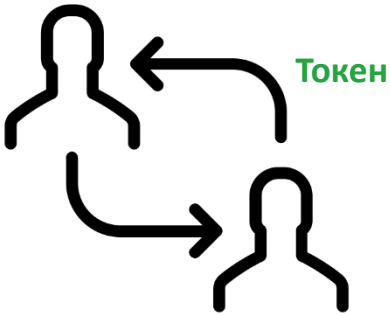
Система для реализации платежей с использованием мобильного приложения эмитента на базе различных платформ

Технологии токенизации и детокенизации

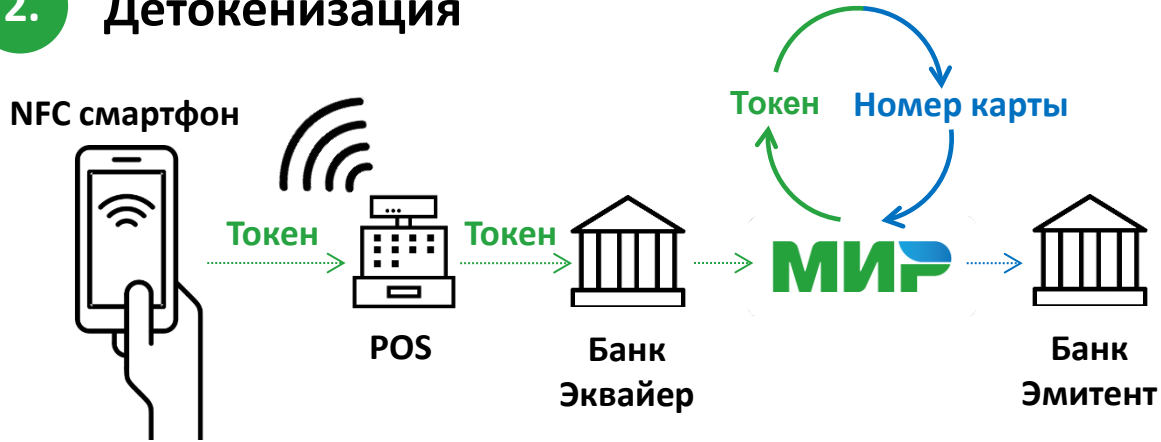
Токен – цифровой «псевдоним номера карты «Мир».

У одной карты «Мир» может быть много токенов!

1. Токенизация



2. Детокенизация



Потому что БЕЗОПАСНО:

- в смартфоне
- в сети Интернет

Внедрение технологии MirAccept 2.0

MirAccept 2.0 – сервис надежной аутентификации Держателя Карты ПС «МИР» на основе технологии 3D-Secure 2.0, не зависимой от VISA!

Загружаемое приложение магазина с компонентом 3DS SDK от ПС «МИР»

Аутентификация держателя карты «Мир» на его смартфоне или планшете во время операции электронной коммерции, в котором такую процедуру берет на себя загружаемое приложение со встроенным в него компонентом 3DS SDK платежной системы «Мир»

Неплатежная аутентификация

Проверка подлинности личности держателя карты «Мир» системой эмитента при совершении неплатежной операции электронной коммерции. Например, при добавлении карты «Мир» в регистрационную запись клиента в мобильное приложение магазина

OOB (out of band authentication)

Проверка держателя карты любым внешним способом, например, через вызванное из мобильного приложения магазина мобильное приложение банка эмитента

Frictionless Flow

Информационный поток без непосредственного обращения эмитента к держателю карты

Спасибо
за внимание!

Вопросы?

Фомичев Максим Викторович
Начальник Отдела сопровождения информационной безопасности и развития систем защиты АО «НСПК»

Вопросы?

Фомичев Максим Викторович
Начальник Отдела сопровождения информационной безопасности и развития систем защиты АО «НСПК»

Требования по обеспечению ИБ в ПС «Мир»