Руководство по подключению и взаимодействию с ОПКЦ НСПК

Часть 1

Руководство по подключению к ОПКЦ НСПК (MasterCard и Visa)

(Версия от 12.02.2015)

Москва, 2015

1. Общие положения

1.1. Определения и обозначения

Участники - российские кредитные организации, являющиеся участниками МПС;

МПС – международные платежные системы;

TPP (Third Party Processor) – процессор третьей стороны, операционный центр, обеспечивающий техническое взаимодействие между Участниками и ОПКЦ НСПК.

Иные термины, используемые в настоящем Руководстве, применяются в значениях, установленных Федеральным законом № 161-ФЗ от 27.06.2011, иными нормативными актами и Правилами оказания операционных услуг и услуг платежного клиринга АО «НСПК».

- Информация

- Необходимо сделать Участнику

1.2. Документация НСПК

№	Документ
1.	Правила оказания операционных услуг и услуг платежного клиринга АО «НСПК»
2.	Руководство по подключению и взаимодействию с ОПКЦ НСПК (Часть 1 - руководство по подключению к ОПКЦ НСПК)
3.	Руководство по подключению и взаимодействию с ОПКЦ НСПК (Часть 2 - руководство по операционному взаимодействию с ОПКЦ НСПК)
4.	Инструкция по установке и настройке клиентского модуля СЭДО НСПК
5.	Организация работы с криптографическими ключами
6.	Инструкция по подключению к среде сертификации ОПКЦ НСПК
7.	Процедура проведения сертификации Участника

1.3. Цель и задачи документа

Цель документа – дать представление Участникам о порядке подключения к ОПКЦ НСПК, а также об особенностях применяемых ОПКЦ НСПК решений и процедур, реализация которых потребует внесения Участниками изменений в используемые их операционными центрами процессинговые решения.

Основные задачи документа:

- определить перечень и последовательность мероприятий по подключению Участников к ОПКЦ НСПК;
- представить порядок сертификационного тестирования настроенного подключения Участников к ОПКЦ НСПК.

1.4. Аудитория документа

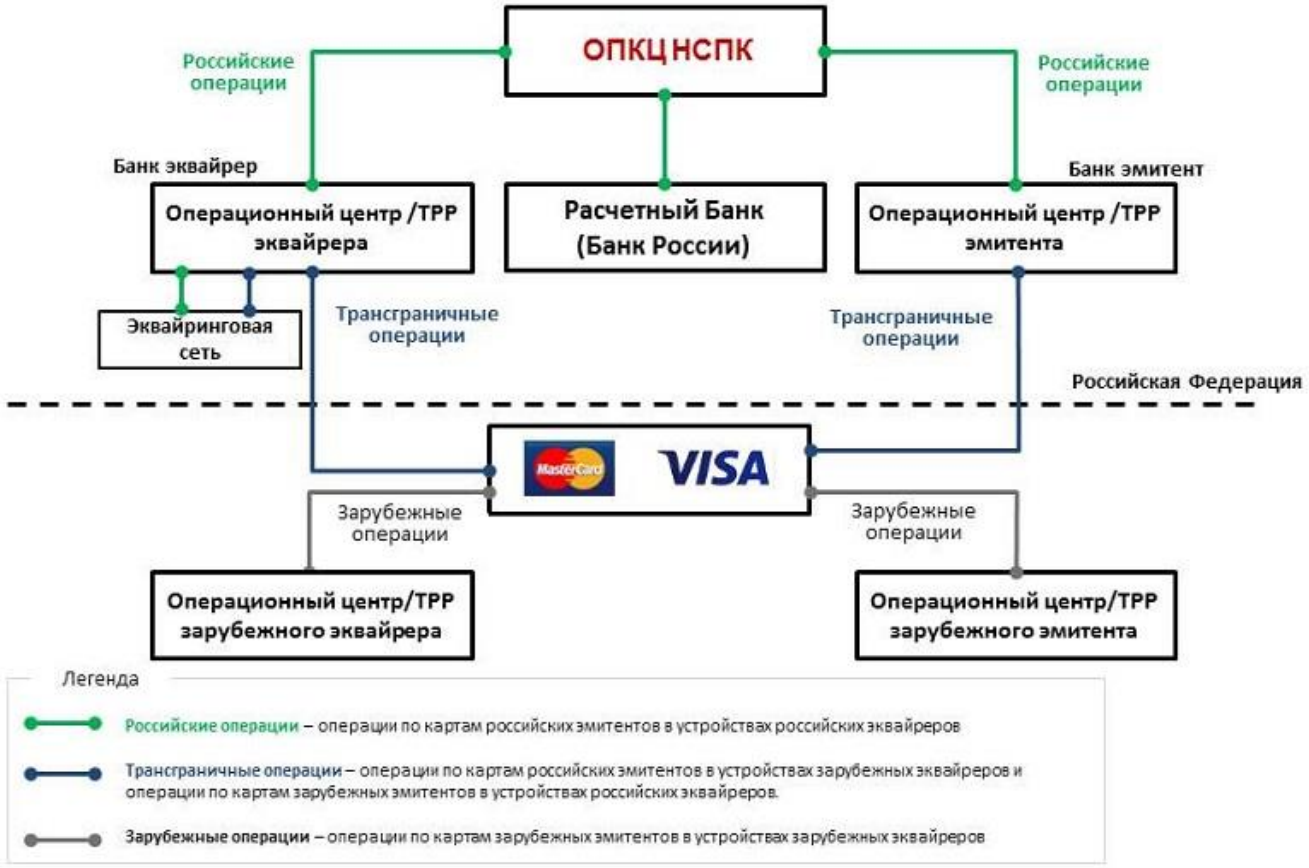
Настоящий документ предназначен для специалистов:

- Процессингового центра;
- Службы Информационных Технологий;
- Операционной службы;
- Служб, ответственных за работу с технологиями платежных карт;
- Служб обеспечения информационной безопасности.

1.5. Роль и место ОПКЦ НСПК в ландшафте МПС

ОПКЦ НСПК является операционным и платежным клиринговым центром МПС в соответствии с договорами, заключенными между НСПК и операторами этих платежных систем. В соответствии с этими договорами НСПК оказывает операционные услуги и услуги платежного клиринга Участникам на основе Правил и тарифов этих платежных систем.

Рисунок 1 Схема взаимодействия операционных центров и процессоров третьей стороны с ОПКЦ НСПК



1.6. Функциональность ОПКЦ НСПК

НСПК предоставит Участникам в качестве операционного и платежного клирингового центра МПС перечисленные ниже сервисы.

Сервис маршрутизации авторизационных и клиринговых сообщений

ОПКЦ НСПК будет получать онлайновые авторизационные запросы от операционных центров российских эквайреров и маршрутизировать их в операционные центры российских эмитентов, карты которых используются при выполнении операций в МПС. ОПКЦ также обеспечивает доведение авторизационных ответов эмитентов до операционных центров эквайреров.

Маршрутизация авторизационных запросов в ОПКЦ НСПК выполняется операционными центрами Участников НСПК с использованием БИН-таблицы, предоставляемой ОПКЦ НСПК. Аналогичным образом клиринговые сообщения направляются операционными центрами Участников в ОПКЦ НСПК для обработки и маршрутизации получателям.

Сервис поддержки авторизационных и клиринговых интерфейсов

Авторизационные сообщения будут направляться Участниками в ОПКЦ НСПК по протоколам соответствующих МПС.

ОПКЦ НСПК поддерживает следующие интерфейсы для обработки авторизационных сообщений:

- MasterCard CIS;
- Visa V.I.P. authorization only (BASE I);
- Visa V.I.P. full financial (SMS).

ОПКЦ НСПК поддерживает следующие клиринговые форматы:

- MasterCard IPM;
- Visa BASE II.

По картам МПС ОПКЦ НСПК поддерживает все основные типы операций, операции полной или частичной отмены (reversal, adjustment) основных операций, включая:

- оплата товаров и услуг с использованием банкоматов, POS-терминалов, терминалов самообслуживания;
- оплата товаров и услуг в сети Интернет (в том числе с использованием технологии 3D Secure);
- выдача наличных с использованием POS-терминалов и банкоматов;
- персональные денежные переводы (P2P) (с карты на карту или за счет вносимых наличных денежных средств);
- запрос баланса с использованием банкоматов, POS-терминалов, терминалов самообслуживания;
- смена PIN-кода с использованием банкоматов, POS-терминалов, терминалов самообслуживания.

Поддерживаются сообщения претензионного цикла: retrieval request, retrieval request response, chargeback, representment, second presentment, arbitration chargeback.

При этом будут поддерживаться все технологии, используемые в МПС, включая технологии:

- магнитной полосы;
- платежных приложений МПС для контактных карт стандарта EMV, включая приложения M/Chip (MasterCard) и VSDC (Visa);

- платежных приложений для бесконтактных карт, включая приложения MasterCard PayPass и Visa payWave;
- платежных приложений для мобильных платежей, включая Visa Mobile Payment Application (VMPA) и MasterCard Mobile PayPass (MMP).

Сервис безопасной обработки операций электронной коммерции на основе технологии 3D Secure

Поддержка операций электронной коммерции с применением технологии 3D Secure будет реализована путём сохранения процедуры аутентификации держателя карты в рамках существующей инфраструктуры МПС.

При этом авторизационная и финансовая части операции покупки (авторизационные и клиринговые сообщения) будут обрабатываться через ОПКЦ НСПК.

Сервис подготовки отчетности

Для Участников будут доступны клиринговые отчеты, предоставляемые им при работе в МПС.

Сервис поддержки БИН-таблиц

АО «НСПК» будет формировать и регулярно передавать операционным центрам Участников и/или их ТРР таблицы банковских идентификационных номеров (БИНов), содержащие информацию обо всех БИНах карточных продуктов Участников, подключенных к НСПК.

Сервис конвертации валюты операции

На территории Российской Федерации держатель карты может:

- в банкомате получить наличные средства в валютах, отличных от российского рубля;
- в магазине беспошлинной торговли (duty free) совершить покупку или возврат товара/отказ от услуги в валюте, отличной от российского рубля.

НСПК поддерживает конвертацию валюты операции в:

- валюту расчетов (рубль РФ);
- в валюту «cardholder billing currency» по правилам МПС. При этом, в случае операций по картам MasterCard, в качестве «cardholder billing currency» используется валюта, выбранная эмитентом при конфигурации своих БИНов. Для операций по картам Visa, в качестве «cardholder billing currency» всегда используется валюта расчетов (рубль РФ).

Сервис управления ключами

Защита передаваемой Участниками информации (в том числе операций) обеспечивается применением сертифицированных аппаратных криптографических модулей с использованием аппаратных средств шифрования передаваемых данных в соответствии со стандартами МПС и ГОСТ РФ.

Для шифрования передаваемых данных используются:

- Ключи шифрования трафика на канальном уровне (АПКШ «Континент»);
- Ключи шифрования ПИН-блоков для безопасной их передачи между Участниками и ОПКЦ НСПК (т.н. PEK - PIN Encryption Key).

Для подписи данных (генерации электронной подписи), передаваемых по СЭДО, используются ключи ассиметричного шифрования. В НСПК поддерживается инфраструктура управления сертификатами с использованием УЦ (Удостоверяющего Центра).

Процедура обмена ключами шифрования ПИН-блоков проводится в соответствии со стандартами МПС, с использованием транспортных ключей, генерируемых и передаваемых НСПК уполномоченным представителям операционных центров Участников.

Сервис сертификационного тестирования операционного центра, подключаемого к НСПК Участника

В рамках сертификационного тестирования выполняется:

- проверка корректности загрузки БИН-таблицы ОПКЦ НСПК;
- проверка корректности формирования запросов и ответов в формате авторизационных протоколов МПС;
- проверка корректности формирования и обработки клиринговых файлов и отчетов;
- проверка корректности настройки программно-аппаратных средств, участвующих в техническом взаимодействии ОПКЦ НСПК и операционного центра Участника или его ТРР.

Сервис резервной авторизации (Stand-In)

Сервис резервной авторизации по картам эмитента будет предоставляться в случае временной недоступности хоста эмитента, при некорректном формате ответа эмитента, при превышении тайм-аута на время ответа эмитента или при ответе эмитента с определенным кодом ответа, согласно спецификациям МПС. Система осуществляет обработку авторизационных запросов от имени данного Участника в пределах заранее настроенных накопительных и количественных лимитов Участника. По факту восстановления работоспособности хоста

эмитента сервис поддерживает отправку уведомлений на хост банка в виде 0120-сообщений, содержащих информацию о результате обработки авторизационного запроса от имени Участника в режиме SAF (Store-and-Forward).

Сервис клиринговых услуг

ОПКЦ НСПК ежедневно (7 дней в неделю) рассчитывает платежные клиринговые позиции Участников на нетто-основе в разрезе МПС в валюте Российской Федерации (рубли РФ), при этом платежные клиринговые позиции косвенного Участника включаются в платежную клиринговую позицию соответствующего прямого Участника.

Нетто позиция Участника будет включать в себя:

- расчеты по межбанковским операциям между Участниками в рублях РФ:
  - по операциям, совершаемым в рублях;
  - по операциям, совершаемым в иных валютах, с конвертацией в валюту расчетов (рубли РФ), используя официальный курс, установленный Банком России на день осуществления расчета платежного клиринга;
- расчеты по межбанковским комиссиям Interchange Reimbursement Fee (IRF) согласно тарифам МПС;
- расчеты по платежам, взимаемым в пользу МПС в соответствии с тарифами и правилами МПС.

Списание или зачисление денежных средств на счета участников осуществляется по правилам и регламентам Банка России.

Вспомогательные сервисы

ОПКЦ НСПК будет поддерживать получение Участниками вспомогательных сервисов МПС, в случае использования Участниками этих сервисов сегодня. К таким сервисам относятся:

По системе MasterCard:

- AAV verification;
- M/Chip ARQC validation/ARPC generation;
- PayPass CVC3 validation;
- Recurring Payment Cancellation Service (RPCS).

По системе Visa:

- CAVV/CAAV verification для операций электронной коммерции, выполняемых по протоколу Verified-by-Visa;

- VSDC ARQC validation/ARPC generation;
- CAM validation.

При этом все Участники или их ТРР должны самостоятельно поддерживать верификацию ПИН-кода, CVV, CVV2, iCVV.

Сервис защищенного документооборота

Система электронного документооборота (СЭДО) предназначена для организации защищенной транспортной среды обмена данными Участников с НСПК. СЭДО обеспечивает:

- нотаризацию информационного обмена (невозможность участника документооборота отказаться от ранее переданной им в НСПК информации);
- целостность передаваемой информации, а также аутентификацию ее источника.

Последнее достигается подписанием Участниками передаваемых документов. Документ, переданный через СЭДО, подпись которого оказалась неверна, отклоняется.

2. Организация телекоммуникационного взаимодействия

2.1. Организационные аспекты подключения

2.1.1. Мероприятия, выполняемые ОПКЦ НСПК за счет средств АО «НСПК»

- организация каналов между площадками Участников и точками присутствия ОПКЦ НСПК на площадках MSK-IX M9/M10;
- оплата услуг операторов связи;
- предоставление абонентских комплектов оборудования из расчета по два комплекта на каждую площадку (ЦОД операционного центра) Участника;
- настройка оборудования абонентских комплектов в соответствии с информацией, предоставленной Участником (в том числе на площадке Участника);
- организация и сопровождение сертификационного тестирования.

2.1.2. Мероприятия, выполняемые Участником

Своевременное предоставление необходимой информации для организации подключения абонентского комплекта на площадке Участника или его ТРР, а именно:

- место установки операторского оборудования обоих провайдеров связи;
- порты для подключения;
- розетки электропитания в стойках;

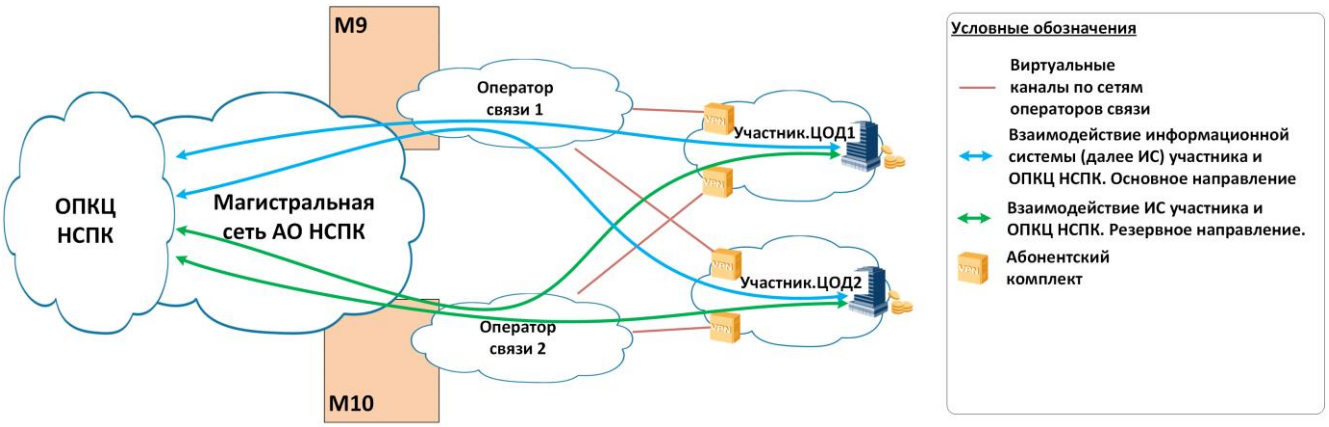
- адрес шлюза в сети площадки, через который обеспечивается связность с сегментом операционного центра Участника;
- Участник сообщает в АО «НСПК» адресные префиксы ИС операционного центра, с которыми организуется взаимодействие;
- настройка маршрутизации сетевого трафика в сети Участника, обеспечивающей возможность связности внутри Участника с сегментом операционного центра;
- организация кабельной инфраструктуры (кабельные трассы, патч-корды) для физического подключения абонентских комплектов в сеть площадки Участника;
- доступ в ЦОДы Участника для сотрудников АО «НСПК» или сервисной организации, обслуживающей или устанавливающей оборудование абонентских комплектов. Доступ должен предоставляться в рабочее время, процедура предоставления доступа определяется Участником, исходя из необходимости проведения оперативных работ.

2.1.3. Организация каналов связи

Организация телекоммуникационных каналов выполняется АО «НСПК» совместно с двумя провайдерами (Orange, Вымпелком).

Результатом данной работы будет являться создание каналов связи (основного и резервного) между операционным центром (центрами) Участника или его ТРР и ОПКЦ НСПК с пропускной способностью 2 Мбит/с.

Рисунок 2 Структурная схема телекоммуникационного взаимодействия Участника с ОПКЦ НСПК



2.2. Установка и настройка оборудования

2.2.1. Организация размещения и подключения оборудования АО "НСПК" на площадках Участника

Для организации присоединения Участника к НСПК на каждой площадке информационной системы Участника организуется присутствие магистральной сети ОПКЦ НСПК - устанавливается по два комплекта клиентского оборудования и организуются два канала различных операторов связи (Orange и Beeline).

Состав и характеристики оборудования одного абонентского комплекта приведен в таблице 1.

Таблица 1. Состав и характеристики оборудования одного абонентского комплекта

Наименование оборудования	Тип оборудования	Размеры, ШхВхГ мм, U	Мощность, W	Тепловыделение, BTU/h	Тип розетки, напряжение, частота
Huawei AR201	Маршрутизатор	482x44x216 (1U)	13	44	Евровилка (IEC/TR 60083), 220В, 50Гц
Континент IPC10	Криптошлюз	216x33.4x134.2	40	136	Евровилка (внешний адаптер переменного тока 19В, 2.1А) 220В 50Гц

Абонентские комплекты оборудования должны быть размещены в двух разных шкафах (стойках) в ЦОД Участника и подключены к разным вводам электропитания.

Маршрутизатор AR201 имеет возможность монтажа в телекоммуникационный шкаф 19”.

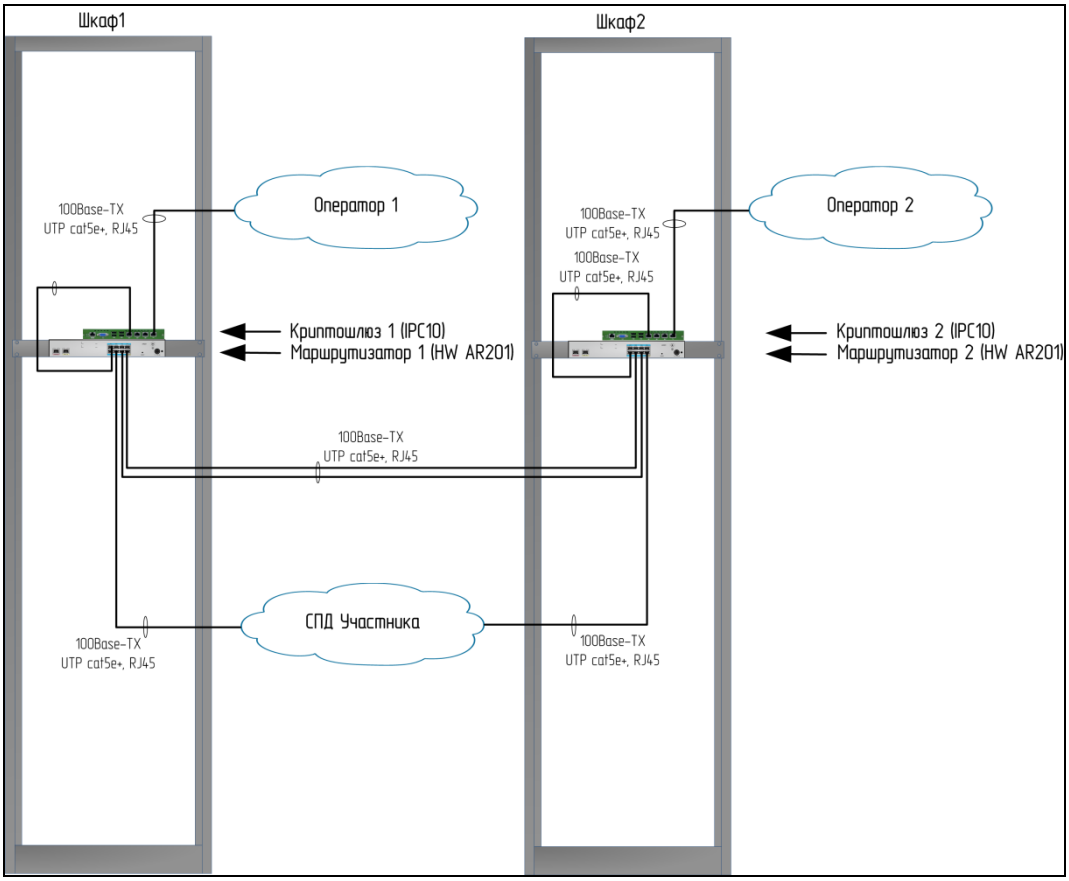
Для установки криптошлюза IPC-10 требуется полка в телекоммуникационный шкаф (но допускается и размещение на верхней плоскости корпуса маршрутизатора).

Маршрутизаторы Huawei AR201 подключаются в разные, дублирующие друг друга сетевые устройства участника интерфейсами 100BASE-TX (см. рисунок 3).

Подключение каждого абонентского комплекта в канал оператора производится одним интерфейсом 100BASE-TX на криптошлюзе Континент IPC-10 (см. рисунок 3).

Все подключения выполняются кабелями UTP, категории не ниже 5e, используется тип разъемов RJ45.

Рисунок 3. Схема подключения и размещения абонентского комплекта на одной площадке Участника



2.2.2. Справочная информация по каналам связи операторов

Требования к каналам операторов для подключения абонентских комплектов:

- уровень канала (ISO OSI) – канальный (L2);
- интерфейсные окончания и канальный уровень на стороне Участника – один порт 100BASE-TX, без тегирования трафика IEEE 802.1q;
- пропускная способность каждого канала – не менее 2 Мбит/с, CIR (гарантированный уровень пропускной способности);
- время задержки в канале (RTT) для объектов на территории:

- Центрального Федерального Округа - не более 50 мс;
- других Федеральных Округов - не более 150 мс;

- коэффициент доступности канала – не менее 0.995;
- количество потерянных пакетов – в соответствии с нормативами в области связи РФ;
- среднее время восстановления – не более 4-х часов.

2.2.3. Организация коммуникационного присоединения Участника к ОПКЦ НСПК

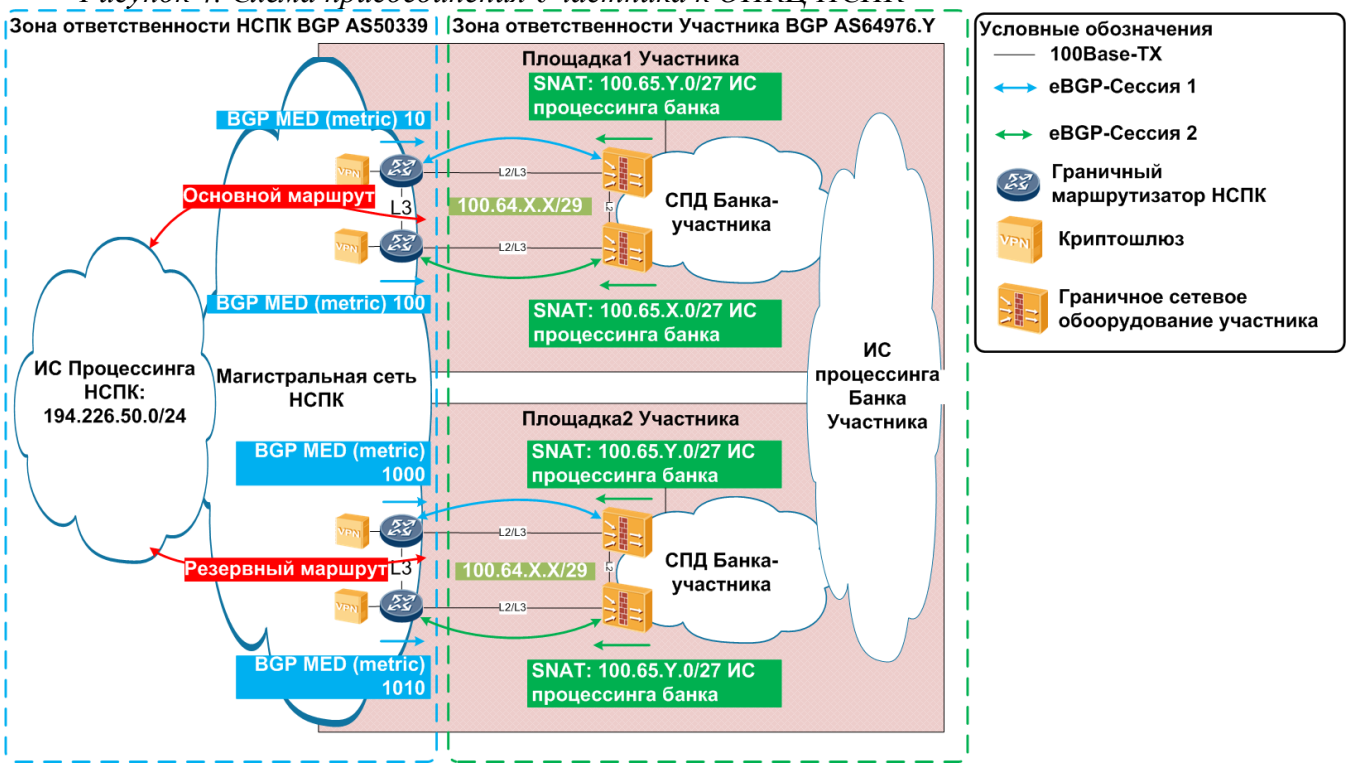
Подключение выполняется на сетевом уровне, путем включения пары граничных маршрутизаторов ОПКЦ НСПК из состава двух абонентских комплектов в активное сетевое оборудование системы передачи данных (СПД) участника.

Подключение предусматривает использованием динамической маршрутизации и протокола BGP.

Благодаря использованию протокола динамической маршрутизации, предлагаемый способ подключения позволяет обеспечить высокую скорость сходимости сети, как при неполадках активного сетевого оборудования, так и при обеспечении переключения между ЦОДами Участника.

Механизм переключения между площадками Участника обеспечивается протоколом BGP. Участник может самостоятельно активировать переключение активного маршрута в любую из подключенных к ОПКЦ НСПК площадок путем конфигурирования со значениями атрибутов MED и AS-Path префиксов Участника, анонсируемых в НСПК.

Рисунок 4. Схема присоединения Участника к ОПКЦ НСПК



Требования к телекоммуникационной инфраструктуре Участников для присоединения к ОПКЦ НСПК:

- на физическом и канальном уровне OSI:
  - комплекты оборудования АО «НСПК» на площадке Участника должны быть установлены в двух разных стойках/шкафах и подключены к разным вводам электропитания;
  - интерфейсы стыка – 2 x 100BASE-TX, подключение к двум взаимно резервируемым устройствам СПД Участника;
  - участник обеспечивает связь на канальном уровне (ISO OSI Layer 2) между маршрутизаторами комплектов и своим граничным оборудованием;
- на сетевом уровне OSI:
  - сеть присоединения (стыковочная сеть, P2P) – IP-адресация назначается Участнику в виде сегмента сети /29 из диапазона 100.64.0.0/16 для каждой пары клиентского оборудования; Пример распределения IP-адресов для одной площадки Участника:
    - P2P-сеть 100.64.1.16/29;
    - маршрутизатор НСПК-1: 100.64.1.17/29;
    - маршрутизатор Участника-1: 100.64.1.18/29;
    - маршрутизатор НСПК-2: 100.64.1.21/29;
    - маршрутизатор Участника-2: 100.64.1.22/29;

- маршрутизация - динамическая маршрутизация по протоколу eBGP:
  - организуется две eBGP-сессии между маршрутизаторами ОПКЦ НСПК и оборудованием Участника (см. рис.3).
  - со стороны ОПКЦ НСПК будет использовать AS50339;
  - со стороны Участника номер AS назначается ОПКЦ НСПК из диапазона 4-октетных номеров AS 64976.1 - 64976.65535; Например, 64976.24
  - передаются только префиксы ИС Участника и ОПКЦ НСПК.
- адресация ИС процессинга ОПКЦ НСПК:
  - ОПКЦ НСПК использует глобально маршрутизируемые PI адреса IPv4 из префикса 194.226.50.0/24;
  - в сторону Участника могут анонсироваться несколько сетей из префикса 194.226.50.0/24, принадлежащего НСПК. Состав анонсируемых ОПКЦ НСПК подсетей со временем может изменяться в связи с развитием ОПКЦ (оставаясь при этом в рамках 194.226.50.0/24);
  - трансляция адресов (NAT) не используется;
- адресация ИС Участника:
  - размер выделяемого пула определяется количеством систем (серверов) Участника, взаимодействующих с ОПКЦ НСПК;
  - по умолчанию для адресов сервисов ИС Участника централизованно назначается ОПКЦ НСПК адресное пространство в виде сегмента сети /27 из диапазона 100.65.0.0/16 (RFC6598). Например: 100.65.24.0/27;
  - на граничном оборудование Участник обеспечивает трансляцию адресов (NAT) сервисов ИС в диапазон адресов, централизованно назначенный ОПКЦ НСПК.

3. Система электронного документооборота НСПК

3.1. Общие положения

Система электронного документооборота ОПКЦ НСПК предназначена для организации защищенного управляемого файлового обмена между Участником и ОПКЦ НСПК. Для использования СЭДО Участник:

- получает дистрибутив прикладного ПО клиентского модуля СЭДО;
- устанавливает его на удовлетворяющую требованиям платформу;
- генерирует ключевой материал (открытый и закрытый ключ электронной подписи), а

также формирует и передает запрос на выдачу сертификата публичного (открытого) ключа электронной подписи (ЭП) в удостоверяющий центр ОПКЦ НСПК (далее по тексту «УЦ НСПК»);

- получает сертификат открытого ключа электронной подписи.

После этого СЭДО может использоваться для передачи файлов между Участником и ОПКЦ НСПК. Более подробная информация содержится в документе «Инструкция по установке и настройке клиентского модуля СЭДО НСПК».

3.2. Клиентский модуль СЭДО НСПК

Клиентский модуль СЭДО выполнен в виде автономной программы. Он должен быть постоянно запущен в системе Участника. Прикладные системы Участника должны быть сконфигурированы для отправки и получения файлов через каталоги, управляемые СЭДО.
Клиентский модуль СЭДО устанавливается в инфраструктуре Участника НСПК.

3.3. Системные требования к платформе выполнения клиентского модуля СЭДО

Платформа для клиентского модуля СЭДО НСПК должна удовлетворять следующим требованиям:

- соблюдение Положения Центрального банка РФ № 382-П от 09.06.2012;
- выполнение требований, приведенных в эксплуатационной документации на СКЗИ КриптоПро JCP 1.0.54;
- обеспечение следующих параметров технологической среды:
  - 64-битная ОС Windows 7 или Windows 8 (требование СКЗИ КриптоПро JCP 1.0.54);
  - достаточный объем дискового пространства для хранения пересылаемых файлов, квитанций и журналов;
  - JDK версии 1.7.0_13;
  - средство криптографической защиты КриптоПро JCP версии 1.0.54 и лицензия на него;
  - настроенная сеть TCP/IP с обеспечением доступа к серверному модулю СЭДО НСПК;
  - настроенные на межсетевых экранах правила, разрешающие исходящие соединения на указанные адреса сервисов СЭДО НСПК.

4. Обмен ключевой информацией

4.1. Организация работы информационного взаимодействия

4.1.1. Общие положения

Участник назначает сотрудников (не менее двух человек), которым предоставляется право осуществлять информационное взаимодействие с АО «НСПК», включая работу с ЭП (далее по тексту «Субъекты информационного обмена»).

АО «НСПК» предоставляет Субъекту информационного обмена съемный носитель информации, содержащий все необходимые материалы.

4.1.2. Регистрация

Шаг 1.

В целях организации взаимодействия с АО «НСПК» и получения Услуг ОПКЦ НСПК Участник предоставляет в АО «НСПК» документы в соответствии с Правилами оказания операционных услуг и услуг платежного клиринга АО «НСПК».

АО «НСПК» проводит проверку предоставленного комплекта документов; в случае положительного результате рассмотрения комплекта документов сотрудник Управления безопасности АО «НСПК» связывается посредством электронной почты, телефонной связи либо иным доступным средством связи с Субъектом информационного обмена и приглашает его в АО «НСПК» в целях осуществления регистрации в УЦ НСПК.

Субъект информационного обмена в дату и время, обозначенное сотрудником Управления безопасности АО «НСПК», прибывает в АО «НСПК». Специалист Управления Безопасности АО «НСПК» регистрирует Субъекта информационного обмена путем внесения информации о нем в реестр УЦ НСПК, а также формирует HTML-форму, содержащую данные, внесенные в реестр УЦ НСПК при регистрации Субъекта информационного обмена (далее по тексту «HTML-форма»).

Шаг 2.

Сотрудник Управления Безопасности АО «НСПК» передает Субъекту информационного обмена съемный носитель информации с программным обеспечением СЭДО и СКЗИ, HTML-форму.

Факт получения вышеуказанного съемного носителя информации подтверждается подписанием Субъектом информационного обмена акта приема-передачи.

4.1.3. Получение сертификата ключа ЭП

Шаг 3.

Субъект информационного обмена с использованием программного обеспечения СКЗИ генерирует открытый и закрытый ключ ЭП, которые будет использоваться в СЭДО.

Закрытый ключ ЭП сохраняется на носителе ключевой информации.

Шаг 4.

На основании информации, содержащейся в HTML-форме, Субъект информационного обмена создает запрос на выдачу сертификата открытого ключа ЭП. Запрос на выдачу сертификата открытого ключа ЭП направляется в УЦ НСПК в электронном виде посредством электронной почты (адрес будет сообщен дополнительно).

Шаг 5.

В случае положительного решения АО «НСПК» о выдаче сертификата открытого ключа ЭП сотрудник Управления безопасности АО «НСПК» формирует соответствующий сертификат открытого ключа ЭП в электронном виде, а также оформляет на бумажном носителе копию сертификата открытого ключа в двух экземплярах, заверяет бумажные копии собственноручной подписью и проставляет оттиск печати АО «НСПК». Сертификат открытого ключа ЭП, сформированный в электронном виде, направляется Субъекту информационного обмена посредством электронной почты. Сертификат открытого ключа ЭП, оформленный на бумажном носителе направляется Субъекту информационного обмена заказным почтовым отправлением с уведомлением о вручении, курьерской службой либо выдается Субъекту информационного обмена лично под роспись.

Субъект информационного обмена собственноручно подписывает обе копии сертификата открытого ключа ЭП и ставит на них оттиск печати Участника. Одна из копий сертификата открытого ключа ЭП, удостоверенная Субъектом информационного обмена, направляется в АО «НСПК» заказным почтовым отправлением с уведомлением о вручении, курьерской службой либо передается в АО «НСПК» лично Субъектом информационного обмена.

Шаг 6.

В случае неполучения АО «НСПК» заверенной Субъектом информационного обмена бумажной копии сертификата открытого ключа ЭП в течение 10 рабочих дней с момента его предоставления Субъекту информационного обмена, АО «НСПК» аннулирует сертификат открытого ключа ЭП.

В случае отрицательного решения АО «НСПК» о выдаче сертификата открытого ключа ЭП на электронный адрес Субъекта информационного обмена направляется соответствующее уведомление с указанием причины отказа.

4.2. Получение криптографических ключей HSM

4.2.1. Общие положения

Участник назначает офицеров безопасности (минимум три человека). Офицеры безопасности осуществляют внедрение и сопровождение системы генерации криптографических ключей для HSM Участника (далее по тексту «Система»), контроль и обнаружение различных угроз, которым подвергается Система и ее информационные ресурсы, а также реагируют на эти угрозы в реальном масштабе времени, выполняют административные мероприятия по установке, настройке и поддержке в работоспособном состоянии средств криптографической защиты информации, эксплуатируемых в Системе, включая работу с ключевой информацией.

В рамках взаимодействия с АО «НСПК» офицеры безопасности Участника (или уполномоченные сотрудники его ТРР) получают от АО «НСПК» ПИН-конверты с 3 компонентами транспортного ключа для Системы Участника или ТРР Участника, а также криптограммы рабочих ключей для каждого из интерфейсов (AWK, IWK для Visa Base I, Visa SMS, PEK – для MasterCard CIS), зашифрованные на транспортном ключе.

4.2.2. Процедура получения криптографических ключей для HSM

Шаг 1.

В случае положительного результата рассмотрения комплекта документов, представленных Участником в АО «НСПК» в соответствии с Правилами оказания операционных услуг и услуг платежного клиринга АО «НСПК», АО «НСПК» в соответствии с внутренним порядком осуществляет генерацию транспортного ключа и криптограмм рабочих ключей для Участника.

Шаг 2.

В результате генерации транспортного ключа для Участника формируется три ПИН-конверта с его компонентами. В АО «НСПК» остается криптограмма данного ключа.

Шаг 3.

Каждый сформированный ПИН-конверт с 2-мя экземплярами акта приема-передачи ПИН-конверта упаковывается в отдельный сейф-пакет (конверт с контролем вскрытия). Письмо (сейф-пакет) с пометкой «лично» направляется одному из трех офицеров безопасности Участника

заказным почтовым отправлением с уведомлением о вручении, курьерской службой либо передается офицеру безопасности Участника лично.

Шаг 4.

Факт получения сейф-пакета с вложенным ПИН-конвертом, содержащим компоненту транспортного ключа, целостность сэйф-пакета и ПИН-конверта подтверждается собственноручной подписью офицера безопасности Участника в акте приема-передачи ПИН-конверта, который он обязан направить в АО «НСПК» заказным почтовым отправлением с уведомлением о вручении, курьерской службой либо передать АО «НСПК» лично.

Шаг 5.

АО «НСПК» генерирует криптограммы 3-х рабочих ключей (IWK, AWK Visa и PEK MasterCard) для Участника, полученные на транспортном ключе Участника.

Шаг 6.

Зашифрованные рабочие ключи (криптограммы) направляются АО «НСПК» на электронный адрес офицеров безопасности Участника. АО «НСПК» направляет два экземпляра акта приема-передачи криптограмм рабочих ключей заказным почтовым отправлением с уведомлением о вручении, курьерской службой либо передается офицеру безопасности Участника лично.

Шаг 7.

Факт получения зашифрованных рабочих ключей подтверждается подписанием офицером безопасности Участника акта приема-передачи криптограмм рабочих ключей. Участник обязан оформить и передать один экземпляр акта приема-передачи криптограмм рабочих ключей в АО «НСПК».

В случае непредставления офицером безопасности Участника в АО «НСПК» оформленного акта приема-передачи ПИН-конвертов и криптограмм рабочих ключей в течение 10 рабочих дней с момента получения вышеуказанных актов от АО «НСПК», транспортный и рабочие ключи Участника будут считаться скомпрометированными.

5. Организационно-технологические изменения на стороне Участника и его операционного центра

5.1. Общие положения

Участник самостоятельно определяет состав и порядок реализации организационно-технологических изменений, необходимых для подключения к ОПКЦ НСПК.

5.2. Контрольный перечень изменений

Комплекс возможных изменений на стороне Участника и его операционного центра может включать в себя, среди прочего, следующие мероприятия:

- организацию физического подключения к ОПКЦ НСПК с использованием абонентских комплектов (см. раздел 2. Организация телекоммуникационного взаимодействия);
- развёртывание клиентских мест СЭДО НСПК (см. раздел 3. Система электронного документооборота НСПК);
- получение и загрузку криптографических ключей для HSM и сертификата ключа ЭП для СЭДО (см. раздел 4. Обмен ключевой информацией);
- настройку дополнительных интерфейсов обмена с ОПКЦ НСПК авторизационными сообщениями по протоколам Visa Base I, Visa SMS, MasterCard CIS;
- настройку маршрутизации:
  - авторизационных сообщений согласно БИН-таблицам, полученным от ОПКЦ НСПК,
  - клиринговых сообщений:
    - в соответствии с каналом авторизации;
    - согласно БИН-таблицам, полученным от ОПКЦ НСПК, при отсутствии онлайн авторизации.
- обеспечение ежедневного формирования клиринговых файлов для ОПКЦ НСПК, приема и обработки клиринговых файлов от ОПКЦ НСПК;
- обеспечение поддержки операционным центром Участника проверки ПИН-кода, CVV, CVV2, iCVV
- настройку новой схемы расчетов (в том числе поддержку правил конвертации валют, установленные расчётным банком) с расчетным банком;
- обработку набора отчетов от ОПКЦ НСПК;

- организацию необходимой доработки информационных систем Участника (АБС, карточный бэк-офис, пр.), обеспечивающих взаимодействие с ОПКЦ НСПК или своим операционным центром;
- актуализацию внутренних операционных регламентов и иных нормативных документов Участника;
- информирование и организация изменений в работе косвенных участников;
- обучение персонала работе с ОПКЦ НСПК;
- создание тестового контура для проведения сертификационного тестирования с ОПКЦ НСПК.

6. Сертификационное тестирование

6.1. Общие положения

Сертификационное тестирование (далее по тексту «тестирование») подключения Участника к ОПКЦ НСПК с целью проверки технической готовности систем Участника и его операционного центра или ТРР к взаимодействию с ОПКЦ НСПК при осуществлении операций по российским картам в российских точках обслуживания.

Участнику необходимо проверить:

- для роли эквайрера:
  - БИН-таблицы, получаемые от ОПКЦ НСПК, обрабатываются корректно, маршрутизация осуществляется в соответствии с ними;
  - запросы на авторизацию операций и отмены авторизованных операций формируются корректно и получаются ожидаемые ответы от эмитента;
  - на основании ответов эмитента, получаемых от ОПКЦ НСПК, генерируются правильные инструкции устройству - инициатору операции (банкомату, терминалу самообслуживания, POS-терминалу);
  - клиринговые файлы корректно формируются и направляются в ОПКЦ НСПК;
  - получаемые от ОПКЦ НСПК клиринговые файлы и файлы отчётов обрабатываются корректно;
  - исключительные ситуации обрабатываются корректно.
- в роли эмитента:
  - сообщения, получаемые от ОПКЦ НСПК, обрабатываются корректно;
  - авторизация и отмена операций работает корректно;
  - ответные сообщения формируются корректно и направляются в ОПКЦ НСПК;

- клиринговые файлы корректно формируются и направляются в ОПКЦ НСПК;
- получаемые от ОПКЦ НСПК клиринговые файлы и файлы отчётов обрабатываются корректно;
- исключительные ситуации обрабатываются корректно.

6.2. Сертификация ТРР

Участники являются Заказчиками сертификации для своих операционных центров или ТРР.

Участники, использующие процессинговые услуги ТРР, самостоятельно согласуют со своими ТРР требуемые объемы участия в тестах и делегируют ТРР ведение проектов сертификации, исходя из количества используемых Участниками сервисов и особенностей взаимодействия Участников и ТРР.

ТРР, успешно прошедшие тестирование с ОПКЦ НСПК в рамках сертификации одного из Участников (Заказчиков), могут не проходить повторное тестирование в рамках сертификации последующих Участников, если объем выполненных тестов полностью покрывает перечень сервисов, используемых последующими Участниками. Техническое и организационное взаимодействие при подключении последующих Участников к ОПКЦ НСПК берет на себя ТРР. Участник вправе запросить у АО «НСПК» и своего ТРР проведение сертификационного тестирования.

6.3. Порядок подключения и проведения сертификации

Для подключения к сертификационной среде ОПКЦ НСПК и проведения тестирования операционному центру Участника или его ТРР необходимо выполнить следующие шаги:

- успешно пройти проверку пакета документов в АО «НСПК»;
- получить от АО «НСПК»:
  - параметры для подключения к среде сертификации;
  - инструкцию по подключению к среде сертификации ОПКЦ НСПК;
  - процедуру проведения сертификации;
  - план-график сертификации и подключения Участника;
  - набор тестовых карт;
- согласовать с АО «НСПК» объем сертификационного тестирования (сертификационные тесты);
- передать в АО «НСПК» свои тестовые карты;
- подключиться к среде сертификации ОПКЦ НСПК;
- провести сертификационные тесты;

- подписать акт прохождения сертификационных тестов.

6.4. Конфигурация подключения к среде сертификации

На основании полученных параметров подключения Участник конфигурирует тестовую среду на своей стороне для подключения к среде сертификации ОПКЦ НСПК.

6.5. Обмен тестовыми картами

Согласно «Процедуре проведения сертификации Участника» представитель Участника получает от АО «НСПК» комплект карт для тестирования эквайринга.

Для тестирования операций эмитента участник подготавливает тестовые карты и предоставляет в АО «НСПК» их параметры в формате, определяемом в «Процедуре проведения сертификации Участника».

6.6. Согласование набора тестов

Участник выбирает набор тестовых испытаний, который соответствует его текущей функциональности в рамках соответствующей МПС (MasterCard, Visa).

6.7. Заведение параметров Участника в ОПКЦ НСПК

На основании полученной информации, АО «НСПК» выполняет настройки среды сертификации ОПКЦ НСПК и уведомляет Участника о готовности к началу тестирования.

Участник выполняет настройки тестовой среды согласно полученным от АО «НСПК» настроечным параметрам и со своей стороны уведомляет АО «НСПК» о готовности к началу тестирования.

Стороны убеждаются в подключении тестовой системы Участника к сертификационной системе ОПКЦ НСПК путём успешного (согласно условиям тестового скрипта) выполнения одной любой операции.

6.8. Согласование графика сертификации и переключения на ОПКЦ НСПК

Между Участником и АО «НСПК» будет согласован и подписан график проведения сертификационных тестов и переключения на ОПКЦ НСПК.

В графике фиксируются следующие основные даты:

- дата проведения сертификационных тестов;
- резервная дата для проведения сертификационных тестов (в случае неуспеха);
- даты переключения БИНов Участника на ОПКЦ НСПК.

6.9. Проведение сертификационных тестов

Сертификационное тестирование проводится в согласованные даты в соответствии с Процедурой проведения сертификации Участника.

По результатам тестирования Участнику направляется протокол выполнения тестовых сценариев.

В случае успешного прохождения сертификационных тестов оформляется акт, содержащий:

- перечень выполненных тестов;
- уточненный график переключения БИНов Участника на ОПКЦ НСПК.

В случае участия в тестировании Участника его ТРР акт подписывается тремя сторонами (Участник, АО «НСПК», ТРР).

7. Процедура переключения на ОПКЦ НСПК

7.1. Общие положения

График переключения составляется по принципу «BIN by BIN», то есть:

- НСПК, согласно графику переключения, включает БИНы Участника в БИН-таблицы ОПКЦ НСПК;
- БИН-таблицы ОПКЦ НСПК рассылаются Участникам в рамках регламентной процедуры;
- эквайреры, регулярно получая и обрабатывая БИН-таблицы ОПКЦ НСПК, самостоятельно «переключают» эквайрерный трафик на ОПКЦ НСПК по БИНам, перечисленным в БИН-таблице;
- в период переключения Участков на ОПКЦ НСПК эквайреры должны обеспечить оперативную загрузку БИН-таблиц ОПКЦ НСПК и соответствующее изменения маршрутизации не позднее двух часов с момента получения БИН-таблиц.

В день обработки эквайрерами направленных им БИН-таблиц часть трафика по одному и тому же БИНу Участника может проходить как через сеть МПС, так и через сеть ОПКЦ НСПК.

7.2. Конфигурация систем Участника

В период между датой оформления акта прохождения Участником сертификации и датой переключения на ОПКЦ НСПК:

- АО «НСПК» предоставляет Участнику БИН-таблицы для маршрутизации операций в ОПКЦ НСПК;
- Участник загружает и обрабатывает БИН-таблицы для маршрутизации операций в ОПКЦ НСПК;
- Участник подготавливает конфигурацию своей промышленной системы для ее активации в согласованную дату и сообщает АО «НСПК» о готовности к переключению (не менее чем за два календарных дня до согласованной даты);
- АО «НСПК» сообщает Участнику о технической готовности к переключению (не позднее, чем за один календарный день до переключения).

7.3. Переключение маршрутизации

В назначенную дату уполномоченные представители АО «НСПК» и Участника координированно дают команду на переключение (ввод в действие подготовленных конфигураций с двух сторон).

При условии успешного переключения всех БИНов Участника на ОПКЦ НСПК оформляется акт о подключении Участника к ОПКЦ НСПК.

8. Контактная информация

По вопросам, связанным с подключением к ОПКЦ НСПК, Участники и их уполномоченные ТРР могут обратиться к выделенным кураторам со стороны АО «НСПК» (контакты будут предоставлены дополнительно), а также:

На электронную почту:

По организационным и техническим вопросам — **css24@nspk.ru**

Указав в теме письма направление вопроса (организационно-правовой вопрос, каналы связи, безопасность, доступ к порталу **support.nspk.ru**[1], операционно-технологическое взаимодействие).

В контактный центр по телефону[2] — **8 800 500 0005**

[1] портал инцидент-менеджмента **support.nspk.ru** будет доступен с 12 января 2015.

Схема голосового меню (IVR) контактного центра:

1 Организационно-правовые вопросы

8 800 500 0005 — **В тональном**

2 Организация каналов связи, установка и настройка оборудования

8 800 500 0005 — **В тональном**

3 Информационная безопасность

8 800 500 0005 — **В тональном**

4 Сертификационное тестирование

8 800 500 0005 — **В тональном**

5 Операционное взаимодействие с НСПК

8 800 500 0005 — **В тональном**

[2] телефонный номер 8 800 500 0005 будет доступен с 25 декабря 2014.