Приложение №3
к Операционным правилам Оператора взаимодействия
по обеспечению технического взаимодействия
и проведению расчетов по платежам и переводам
с использованием двухмерного символа штрихкода (QR кода)

ТЕХНИЧЕСКИЙ РЕГЛАМЕНТ ОПЕРАТОРА ВЗАИМОДЕЙСТВИЯ

ЗАО «Демир Кыргыз Интернэшнл Банк»
г. Бишкек, 2022

Оглавление

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аббревиатура	Описание
ДКИБ	Закрытое акционерное общество «Демир Кыргыз Интернэшнл Банк»
НБКР	Национальный банк Кыргызской Республики
API	Application Programming Interface - это определенный набор компонентов, который позволяет одной программе обмениваться данными с другой программой. Также под термином API может пониматься и описание способов обмена ПО (константы, классы, структуры, функции, процедуры и другие элементы).
Платежная система (PSP)	Поставщик платежных услуг - Косвенный участник, который предоставляет услуги продавцам / Плательщикам для получения/отправки финансовых услуг (Платежное приложение).
JSON	JavaScript Object Notation - это открытый стандартный формат файлов и формат обмена данными, который использует текст, читаемый человеком, для хранения и передачи объектов данных, состоящих из пар атрибут-значение и массивов (или других сериализуемых значений). Это распространенный формат данных, который находит разнообразное применение в электронном обмене данными, в том числе при взаимодействии веб-приложений с серверами.
REST	Representational State Transfer - архитектурный стиль для разработки веб-сервисов.
WAF	Web Application Firewall – межсетевой экран для веб-приложений. Это инструмент для фильтрации трафика, работающий на прикладном уровне и защищающий веб-приложения методом анализа трафика HTTP/HTTPS и семантики XML/SOAP. WAF может устанавливаться на физический или виртуальный сервер и выявляет самые разнообразные виды атак.
Оператор взаимодействия / ОВ / ОВ ДКИБ	Оператор платежной системы, обеспечивающий техническое взаимодействие с участниками платежных систем и формирование клиринговых файлов для окончательных расчетов по Платежам с использованием QR-кода, имеющий лицензию НБКР на оказание услуг по приему, обработке и выдаче финансовой информации (Процессинг, Клиринг) по платежам и расчетам третьих лиц участникам платежной системы, данного процессингового, клирингового центра, а также имеющий регистрацию в реестре НБКР в качестве Оператора взаимодействия по проведению платежей с использованием двумерных символов штрих кода (QR-кода). Оператором взаимодействия является Закрытое акционерное общество «Демир Кыргыз Интернэшнл Банк».
PSP Отправитель	Платежное приложение - инициатор Платежа, т.е. Платежное приложение, через которое оплачиваются финансовые услуги.
PSP Получатель	Платежное приложение - QR-эквайринг, т.е. Платежное приложение, через которое поступают финансовые услуги.

Режим реального времени	Режим обработки платежных документов, информации, который обеспечивает немедленное взаимодействие системы с внешними процессами.
Хост	Программная или аппаратная компьютерная система, подключённая к коммуникационной сети и имеющая уникальный сетевой адрес; узел сети Прямого участника
Операционный день	Период времени с 00:00 (включительно) календарного дня D до 00:00 (не включительно) следующего календарного дня D+1, установленный Оператором взаимодействия для формирования электронной базы данных по проведенным QR Платежам в рамках Платежных приложений. Операции, совершенные после окончания Операционного дня, учитываются как операции следующего Операционного дня.
Мерчант	Торгово-сервисное предприятие, которое принимает Платежи для оплаты за товары/услуги посредством QR-кода.
Участник	под участником понимается Прямой участник и/или Косвенный участник
Эквайер	Прямой участник и/или Косвенный участник, который генерирует QR-код
Frontend	Пользовательский интерфейс, видимая пользователям часть сайта или приложения.
Backend / Бекэнд	Бэкэнд (англ. back-end) — ядро сайта или приложения, скрытое от пользователя. Бэкендом называют программно-аппаратную часть сервиса, которая работает на сервере.

2. ВВЕДЕНИЕ

2.1. Технический регламент Оператора взаимодействия (далее по тексту – Регламент) является регулирующим документом, который определяет технические требования к Платёжным приложениям, устанавливает порядок Закрытия операционного дня, Клиринга и взаимодействия Прямых участников / Косвенных частников системы Оператора взаимодействия, а также архитектуру системы Оператора взаимодействия и схему ее функционирования.
2.2. Регламент является обязательным для исполнения всеми субъектами настоящих Правил. Неисполнение Регламента Прямым участником / Косвенным участником влечет ответственность вплоть до исключения из системы Оператора взаимодействия.

3. АРХИТЕКТУРА СИСТЕМЫ И СХЕМА ЕЕ РАБОТЫ

3.1. Система Оператора взаимодействия является масштабируемой и имеет распределение вычислений и данных. Архитектура подразумевает разделение ролей и включает frontend, backend, базу данных и хранилище файлов.
3.2. Архитектура системы Оператора взаимодействия включает основной и резервный сайт.
3.3. Основа системы Оператора взаимодействия – это программное обеспечение, обеспечивающее исполнение основных процессов Платежа посредством QR-кода/Платежных ссылок, Закрытия операционного дня, сверку и взаиморасчеты между Прямыми участниками.
Основа системы состоит из нижеследующих компонентов:

- Прямой участник / Косвенный участник;

- Платежная система (PSP) – инициатор/получатель QR Платежа, Платежное приложение, которое взаимодействует с Оператором взаимодействия, имеет счет в расчетном Банке, в системе заводится под этим банком;
- Лимит – представляет собой количественное ограничение, накладываемое на QR Платежи Прямых участников / Косвенных участников;
- Транзакция – процесс проведения Платежа с одного счета/кошелька в пользу другого счета/кошелька с помощью использования Платежной системы; Полное описание спецификации по протоколу (API) взаимодействия в Режиме реального времени в Приложении Д к Регламенту.
- Закрытие дня – это процесс Закрытия операционного дня: прием и обработка пакета всех QR Транзакций за предыдущий Операционный день.
- Клиринг - процесс проведения Банком безналичных расчетов по взаимным требованиям и обязательствам Прямых участников с Банком и/или с другими Прямыми участниками Оператора взаимодействия по проведенным Платежам с помощью QR кодов.

3.4. Информационное взаимодействие между Прямыми участниками / Косвенными участниками, предполагает следующую схему взаимодействия:

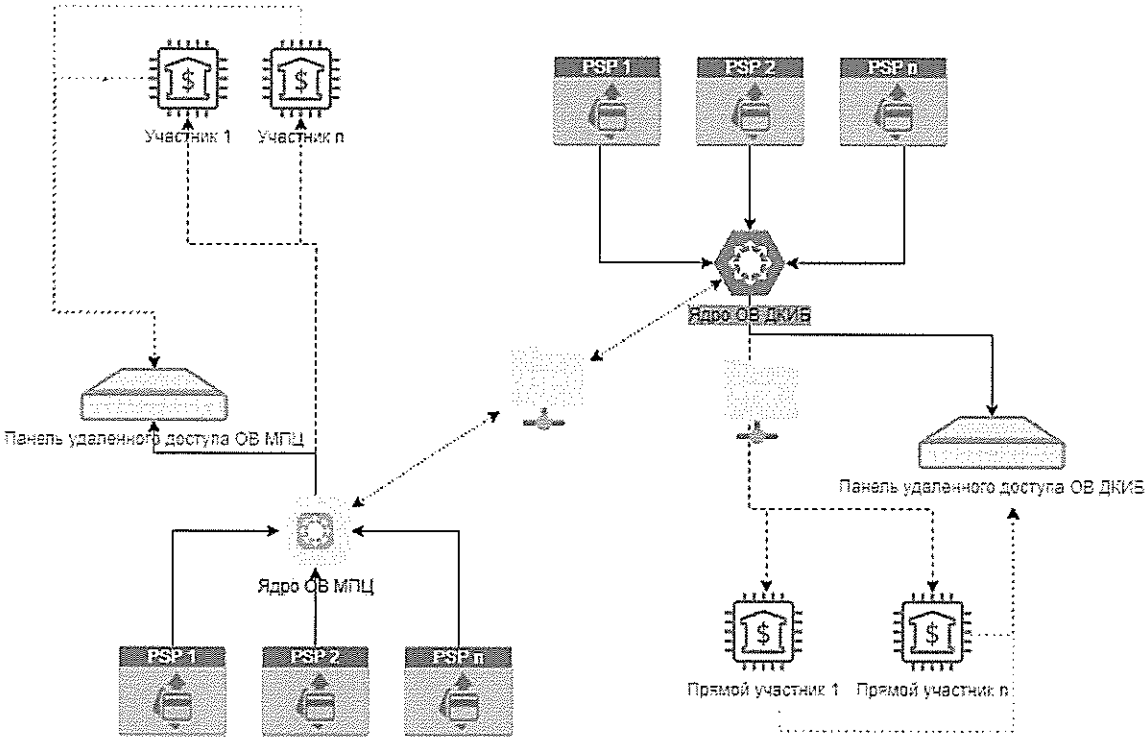

Рисунок 1. Общая схема Оператора взаимодействия

4. СЕТЕВОЕ ВЗАИМОДЕЙСТВИЕ

4.1. Онлайн сообщения

- Взаимодействие с API, Панелью удаленного доступа осуществляется посредством HTTPS;
- Обмен оффлайн-сообщениями осуществляется посредством SFTP;
- Все программные интерфейсы используют JSON/REST API.

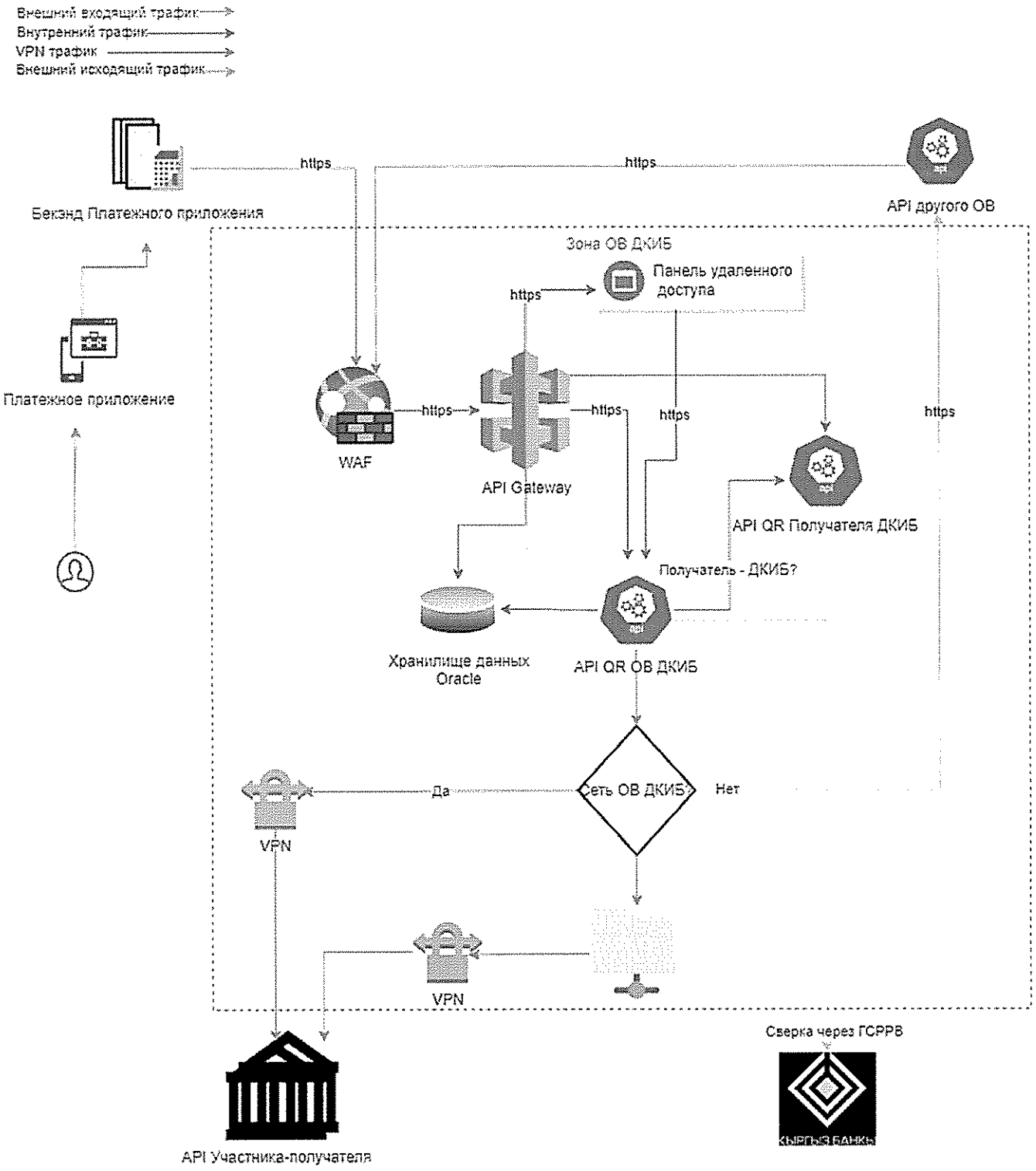

Рисунок 2. Схема сетевых потоков данных Оператора взаимодействия

4.2. Оффлайн сообщения

- К оффлайн сообщениям относятся процессы осуществляемые в процессе закрытия дня;
- Обмен файлам осуществляется посредством SFTP;
- Система поддерживает следующие оффлайн сообщения:

4.3. Interbank Settlement file - ГРОСС-файл (внутренний формат системы ГСРРВ)

Файл формирует: Система Оператора взаимодействия
Файл принимает: ГСРРВ НБКР
Частота выполнения: один раз в рабочий день
Назначение: Файл двусторонних чистых позиций для проведения окончательного расчета между Прямыми участниками за проведенные Транзакции.

4.4. Файл установки резервов - ГРОСС-файл (внутренний формат системы ГСРРВ)
Файл формирует: Система Оператора взаимодействия
Файл принимает: ГСРРВ НБКР
Частота выполнения: один раз в рабочий день
Назначение: Файл установки резерва Прямого участника в ГСРРВ для Системы.

4.5. Клиринг файл - JSON-файл (внутренний формат Системы) согласно Приложению А к Регламенту.
Файл формирует: Система Оператора взаимодействия
Файл принимает: Прямой участник
Частота выполнения: один раз в рабочий день
Назначение: Файл, содержащий список Платежей, успешно принятых и попавших в закрытие дня.

5. ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Закрытое акционерное общество «Демир Кыргыз Интернэшнл Банк» как Оператор взаимодействия по проведению Платежей с использованием двухмерных символов штрихкода (QR-код), Прямые участники / Косвенные участники обязаны обеспечить защиту информации в соответствии с:

- Положением Национального банка Кыргызской Республики «О требованиях по обеспечению информационной безопасности в коммерческих банках Кыргызской Республики»;
- Положением Национального банка Кыргызской Республики «О нештатных ситуациях в платежной системе»;
- Стандартом по обеспечению информационной безопасности учреждений банковской системы Кыргызской Республики;
- Правилами проведения платежей и переводов с использованием двухмерных символов штрихкода (QR-код);
- Требования Национального банка Кыргызской Республики в области защиты информации;
- Требованиями законодательства Кыргызской Республики в области защиты информации.

5.2. Платежные приложения должны обеспечить безопасное сканирование/обработку QR- кода/Платежных ссылок, исключающее возможность реализации угрозы внедрения вредоносных программных обеспечений, вирусов и других угроз, а также обеспечить обработку только тех Платежных ссылок, которые санкционированы в системе Оператора взаимодействия.

5.3. Защита веб-приложения от несанкционированного доступа и атак строится на основе Web Application Firewall (WAF).

5.4. WAF должен обнаруживать и блокировать атаки, включая атаки из списка OWASP Top 10 (Open Web Application Security Project) и классификации WASC, L7 DDoS и атаки нулевого дня. Обеспечивать непрерывную защиту приложения, пользователей и инфраструктуру.

5.5. Прямые участники / Косвенные участники должны предоставить заполненную Анкету – опросник по информационной безопасности согласно Приложения Б к Регламенту.

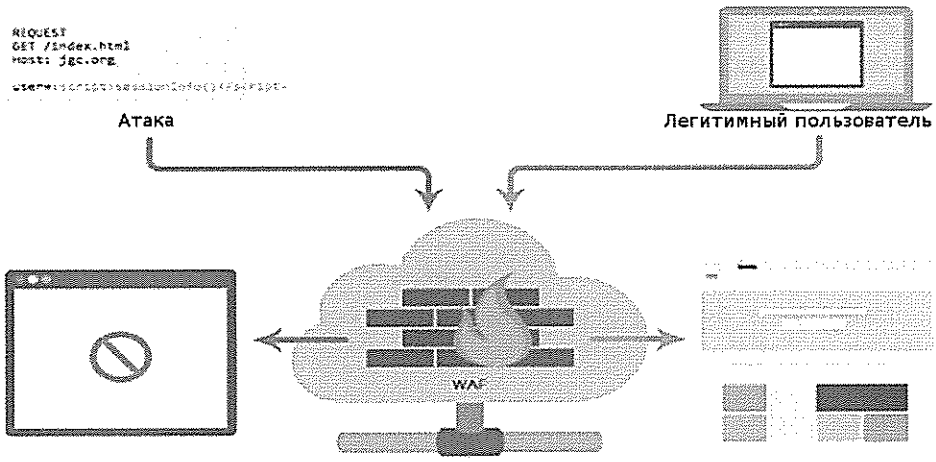

Рисунок 3. Принцип работы WAF

6. ТРЕБОВАНИЕ К ПРЯМОМУ УЧАСТНИКУ

6.1. Контроль Лимитов своего PSP (Косвенных участников) через Панель удаленного доступа.
6.2. Возможность читать и поддерживать клиринговые отчеты от Оператора взаимодействия.
6.3. Обеспечить ежедневное наличие на Корреспондентском счете в НБКР денежной суммы, необходимой для проведения расчетов.
6.4. Оплачивать счета, выставленные ДКИБ за Услуги Оператора взаимодействия (если Услуги ДКИБ будут оплачиваться).
6.5. Прямые участники должны разработать внутренние правила или процедуры для обеспечения бесперебойного функционирования своей информационной системы и безопасности для проведения Платежей с использованием QR-кода. Программные и технические средства, применяемые в системах для проведения Платежей с использованием QR-кода, должны соответствовать требованиям НБКР по обеспечению информационной безопасности.
6.6. Хранить данные и копии квитанций, а также другую информацию, связанную с QR Платежами, в течение 6 лет со дня Платежа.

7. ТРЕБОВАНИЯ К PSP

7.1. Иметь автоматизированное информационное программное обеспечение, способное подключаться к системе Оператора Взаимодействия.
7.2. Иметь Платежное приложение, способное считывать QR-код и размещенное в открытом доступе для скачивания на платформах мобильных приложений (Play Store, App Store и т.п.).
7.3. Генерация/создание стандартизированного QR-кода/Платежной ссылки, отвечающей всем требованиям НБКР.
7.4. Платежные приложения должны иметь защиту доступа в виде аутентификации при входе Клиента в систему (PIN-код, Face ID, Touch ID и т.п.).
7.5. Обеспечение интеграции API с системой Оператора взаимодействия в Режиме реального времени.
7.6. Предоставление ответа на онлайн запрос API в течение 2 (двух) секунд.

8. ТРЕБОВАНИЯ К ГЕНЕРАЦИИ QR-КОДОВ

8.1. Для приема Платежей через систему Оператора взаимодействия, необходимо реализовать поддержку дополнительных полей, в соответствии со стандартом НБКР:

Стандартизированный QR НБКР	**ID – макс длина**	**Обязательные поля**
Стандарт версия	00 - 02	Обязательно
Тип Платежной ссылки	01 - 02	Обязательно
Информация продавца торговой точки:	32 - 99	Обязательно
- уникальный идентификатор	00 - 32	Обязательно
- Спецификация платежной сети	01 - 10	Условно
- Уникальный идентификатор плательщика в рамках услуги (лицевой счет)	10 - 32	Не обязательно
- ID Транзакции	11 - 32	Условно
- Возможность редактирования суммы Платежа	12 - 02	Условно
- Возможность редактирования идентификатора плательщика (лицевой счет)	13 - 02	Условно
Дополнительная информация о Платеже	33 - 99	Условно
- Уникальный идентификатор компании	00 - 32	Условно
- Наименование услуги	01 - 32	Не обязательно
Описание Платежа	34 -	Не обязательно
Дополнительные поля продавца/торговой точки	35, 36, 37, 38, 39	Не обязательно
Код поставщика услуг (MCC)	52 - 04	Обязательно
Код валюты	53 - 03	Обязательно
Сумма к оплате	54 - 13	Условно
Имя поставщика услуг (на латинице)	59 - 25	Обязательно
Контрольная сумма данных	63 - 04	Обязательно

Таблица 1. Стандартизированный QR НБКР

8.2. Поддержка дополнений, указанных в Таблице 1, обязательно для всех подключаемых Косвенных участников / PSP, которые принимают Платежи по QR- коду/Платежным ссылкам.

8.3. Полное описание Спецификации по QR-коду содержится в Приложении В к Регламенту.

9. ТИПЫ ФИНАНСОВЫХ ТРАНЗАКЦИЙ

Код	**Описание**
10	Перевод по QR-коду/Платежной ссылке для оплаты. C2C
20	Покупка через QR-код/Платежной ссылке для оплаты. C2B
30	Государственный платеж (физического лица) по QR-коду/Платежной ссылке на оплату. C2G
40	Денежный перевод/вывод/возврат по QR-коду/Платежной ссылке для оплаты. B2C
50	Оплата/перевод по QR-коду/Платежной ссылке для оплаты. B2B
60	Электронное сообщение по установке резерва Прямому участнику.
70	Государственный платеж (юридическое лицо) по QR-коду/Платежной ссылке на оплату. B2G

Таблица 2. Типы финансовых Транзакций

10. ПАНЕЛЬ УДАЛЕННОГО ДОСТУПА

10.1. Панель удаленного доступа предоставляется Прямым участникам/Косвенным участникам Оператора взаимодействия по Платежам с помощью QR-кода.

10.2. Роли:

- Оператор взаимодействия;
- Прямой участник;
- Косвенный участник.

10.3. Панель удаленного доступа предоставляет следующие основные возможности:

Для Оператора взаимодействия будут доступны следующие функции:

1) Управление пользователями Панели удаленного доступа и их доступом к системе;
2) Управление Лимитами Прямых участников;
3) Доступ к информации о Платежах в Режиме реального времени;
4) Мониторинг Платежей;
5) Загрузка отчетов о Транзакциях;
6) Заполнение списка выходных и праздничных дней.

Для Прямых участников в Панели удаленного доступа будут следующие возможности:

1) Установка Лимитов для своих Косвенных участников (будут установлены на следующий рабочий день);
2) Доступ к информации о Платежах в Режиме реального времени;
3) Загрузка отчетов о Платежах.

Для косвенных участников будут доступны следующие функции:

1) Доступ к информации о Платежах в режиме реального времени;
2) Выгрузка отчетов о Транзакциях.

10.4. Полное описание Панели удаленного доступа содержится в Приложении Г к Регламенту.

11. ПОРЯДОК ПРОВЕДЕНИЯ ПЛАТЕЖА

Оператор взаимодействия ДКИБ

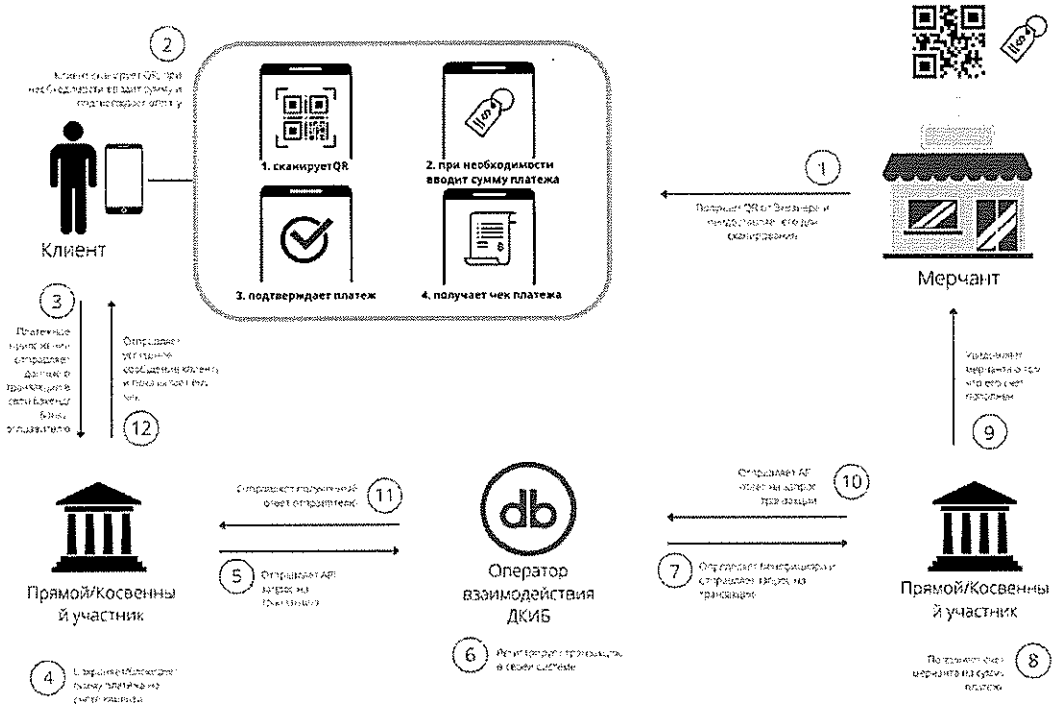

Рисунок 4. Схема проведения Платежа внутри Оператора взаимодействия

1. Платежное приложение - PSP Получателя генерирует QR-код и предоставляет его PSP Отправителю.
2. Платежное приложение - PSP Отправителя сканирует QR-код и передает данные на Хост.
3. Прямой участник / Косвенный участник - PSP Отправителя авторизовывает Платеж и отправляет запрос Оператору взаимодействия.
4. Оператор взаимодействия сохраняет данные о Платежах и направляет запрос на авторизацию соответствующему Прямому участнику / Косвенному участнику - PSP Получателя.
5. Прямой участник / Косвенный участник - PSP Получателя - получает запрос, авторизовывает Платеж и отправляет ответ Оператору взаимодействия.
6. Прямой участник / Косвенный участник - PSP Получателя уведомляет продавца по средствам Платёжного приложения о статусе Платежа.

6.1. В случае успешной оплаты Платежное приложение предоставляет квитанцию о Платеже.

7. Оператор взаимодействия направляет ответ со статусом Платежа Прямого участника / Косвенного участника - PSP Получателя Прямому участнику / Косвенному участнику - PSP Отправителя
8. Платежное приложение - PSP Отправителя показывает Клиенту статус Платежа.

8.1. В случае успешной оплаты Платежное приложение предоставляет квитанцию о Платеже.

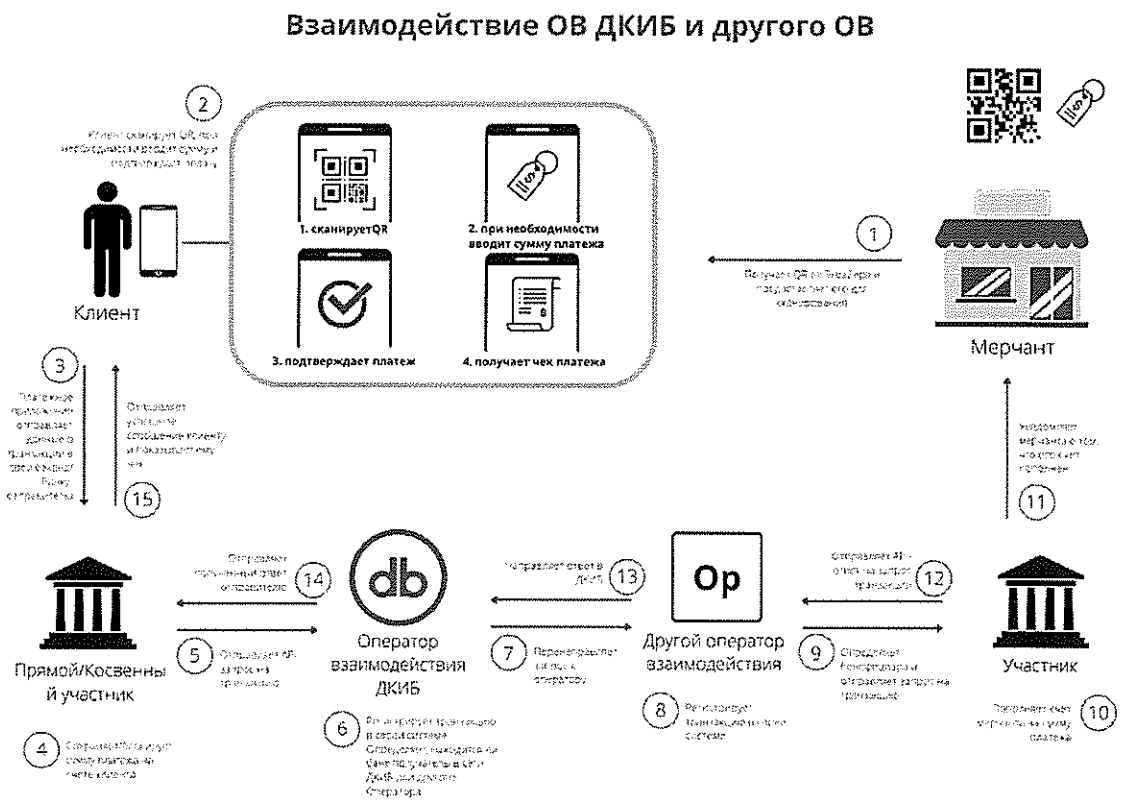

Рисунок 5. Схема проведения Платежа с другим оператором взаимодействия

1. Платежное приложение - PSP Получателя генерирует QR-код и предоставляет его PSP Отправителю.

2. Платежное приложение - PSP Отправителя сканирует QR-код и передает данные на хост.
3. Прямой участник / Косвенный участник - PSP Отправителя авторизовывает Платеж и отправляет запрос Оператору взаимодействия (ОВ1).
4. Оператор взаимодействия (ОВ1) сохраняет данные о Транзакции и направляет запрос на авторизацию другому оператору взаимодействия (ОВ2).
5. ОВ2 сохраняет данные о Платеже и направляет запрос на авторизацию соответствующему Прямому участнику / Косвенному участнику - PSP Получателя.
6. Прямой участник / Косвенный участник - PSP Получателя - получает запрос, авторизовывает Платеж и отправляет ответ ОВ2.
7. Прямой участник / Косвенный участник - PSP Получателя уведомляет продавца по средствам Платёжного приложения о статусе Платежа.
7.1. В случае успешной оплаты Платежное приложение предоставляет квитанцию о Платеже.
8. ОВ2 направляет ответ со статусом Платежа ОВ1
9. ОВ1 направляет ответ со статусом Платежа Прямого участника / Косвенного участника - PSP Получателя Прямому участнику / Косвенному участнику - PSP Отправителя.
10. Платежное приложение - PSP Отправителя показывает Клиенту статус Платежа.
10.1. В случае успешной оплаты Платежное приложение предоставляет квитанцию о Платеже.

12. ЗАКРЫТИЕ ОПЕРАЦИОННОГО ДНЯ / КЛИРИНГ

12.1. Процедура Закрытия операционного дня - включает все операции, совершенные в течение Операционного дня, и выполняются следующие группы процессов в период с 00:00 до 00:30.
12.2. Формируются сводные данные по прошедшим Платежам, по каждому Прямому участнику и по каждому Косвенному участнику.
12.3. Формируются Файлы чистых позиций и резервов по каждому Прямому участнику.
12.4. Обработка пакетов Транзакций, проведённых в выходные дни и, в установленные действующим законодательством КР, праздничные дни, осуществляется Оператором взаимодействия в первый рабочий день, следующий за выходными и праздничными днями.

Прямая интеграция с ГСРРВ

1. После открытия сессии файлы установки резервов по каждому Прямому участнику отправляются в ГСРРВ.
2. После получения успешного ответа от ГСРРВ, в ГСРРВ отправляются Файлы чистых позиций.
3. Формируются клиринговые файлы по каждому Прямому частнику и Косвенному участнику согласно установленному формату и направляются Прямым участникам для дальнейших расчетов с Косвенными участниками по проведенным Платежам.

Взаиморасчеты между участниками ОВ ДКИБ и другим ОВ

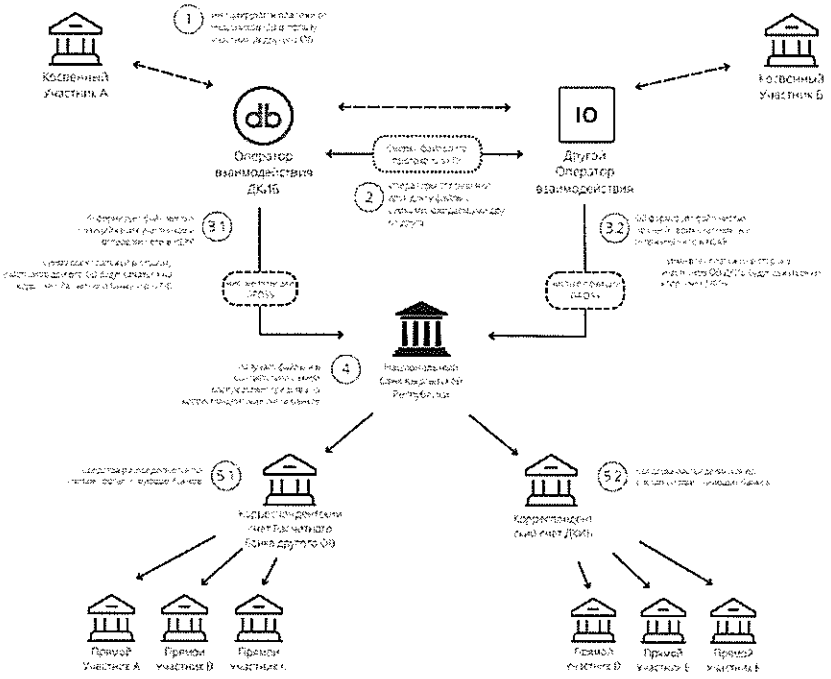

Рисунок 7. Схема файлового обмена (информационного потока) между Прямыми участниками, а также между другим оператором взаимодействия и Оператором взаимодействия

Согласно схеме выше, операторы взаимодействия будут вести взаиморасчёты с участием расчётных банков, через которые будут проходить взаиморасчёты по всем Прямым участникам и Косвенным участникам. Так каждый оператор взаимодействия регистрирует другого оператора взаимодействия в своей системе как Косвенного участника с указанием расчетного банка, через который будут происходить взаиморасчеты при закрытии дня.

В схеме приведен пример совершения Платежа от Косвенного участника ОВ «ДКИБ» в сторону участника другого оператора взаимодействия, которая актуальна также и для Платежей, совершаемых участниками другого оператора взаимодействия в сторону Прямого участника/Косвенного участника ОВ «ДКИБ».

1. Прямой участник / Косвенный участник ОВ «ДКИБ» инициирует QR платежи в сторону участников-получателей другого оператора взаимодействия.

2. При закрытии дня ОВ «ДКИБ» и другой оператор взаимодействия через SFTP-протокол обмениваются файлами в согласованном формате двумя операторами взаимодействия для сверки всех Платежей.

3. Также каждый оператор взаимодействия формирует свой Файл чистых позиций по тем же инициируемым Платежам и высылает его в ГСРРВ. Другими словами, Файлы чистых позиций будут формироваться в соответствии со схемой, сумма всех Платежей, принятых в сторону другого оператора взаимодействия – в данном случае от Косвенного участника ОВ «ДКИБ» в сторону участника другого оператора взаимодействия - будет дебетоваться **с корреспондентских счетов** участников-

отправителей и кредитоваться на **корреспондентский счет расчетного банка** оператора взаимодействия-получателя. Пример ниже:

	ОВ «ДКИБ» отправитель	Сумма дебета	другой оператор взаимодействия получатель	Сумма кредита
1	Корр. Счет участника "А" ОВ «ДКИБ»	100	Корр. Счет расчетного банка другого оператора взаимодействия	300
2	Корр. Счет участника "Б" ОВ «ДКИБ»	200		
	итого	**0**		

Такой же процесс в обратную сторону, когда другой оператор взаимодействия - инициатор Платежа, а ОВ «ДКИБ» - получатель:

	Другой оператора взаимодействия отправитель	Сумма дебета	ОВ «ДКИБ» получатель	Сумма кредита
1	Корр. Счет Участника "А" другого оператора взаимодействия	100	Корр. Счет расчетного банка ОВ «ДКИБ»	300
2	Корр. Счет Участника "Б" другого оператора взаимодействия	200		
	итого	**0**		

4. На основе Файла чистых позиций, полученных от другого оператора взаимодействия и ОВ, Национальный банк в ГСРРВ обрабатывает полученный файл.

5. После получения денежных средств на корреспондентский счет, каждый оператор взаимодействия распределяет их по своим Участникам-получателям.

	оператор взаимодействия отправитель	Сумма ЧП	Участники–получатели	Распределение сумм
1	Корр. счет расчетного банка ОВ	300	Банк "С"	200
			Банк "D"	100
	итого		**0**	

В данной схеме, каждый оператор взаимодействия, самостоятельно формирует Файлы чистых позиций и направляет на обработку в ГСРРВ, соответственно ответственность за проведение окончательных взаиморасчетов по своим Участникам несет каждый оператор взаимодействия.

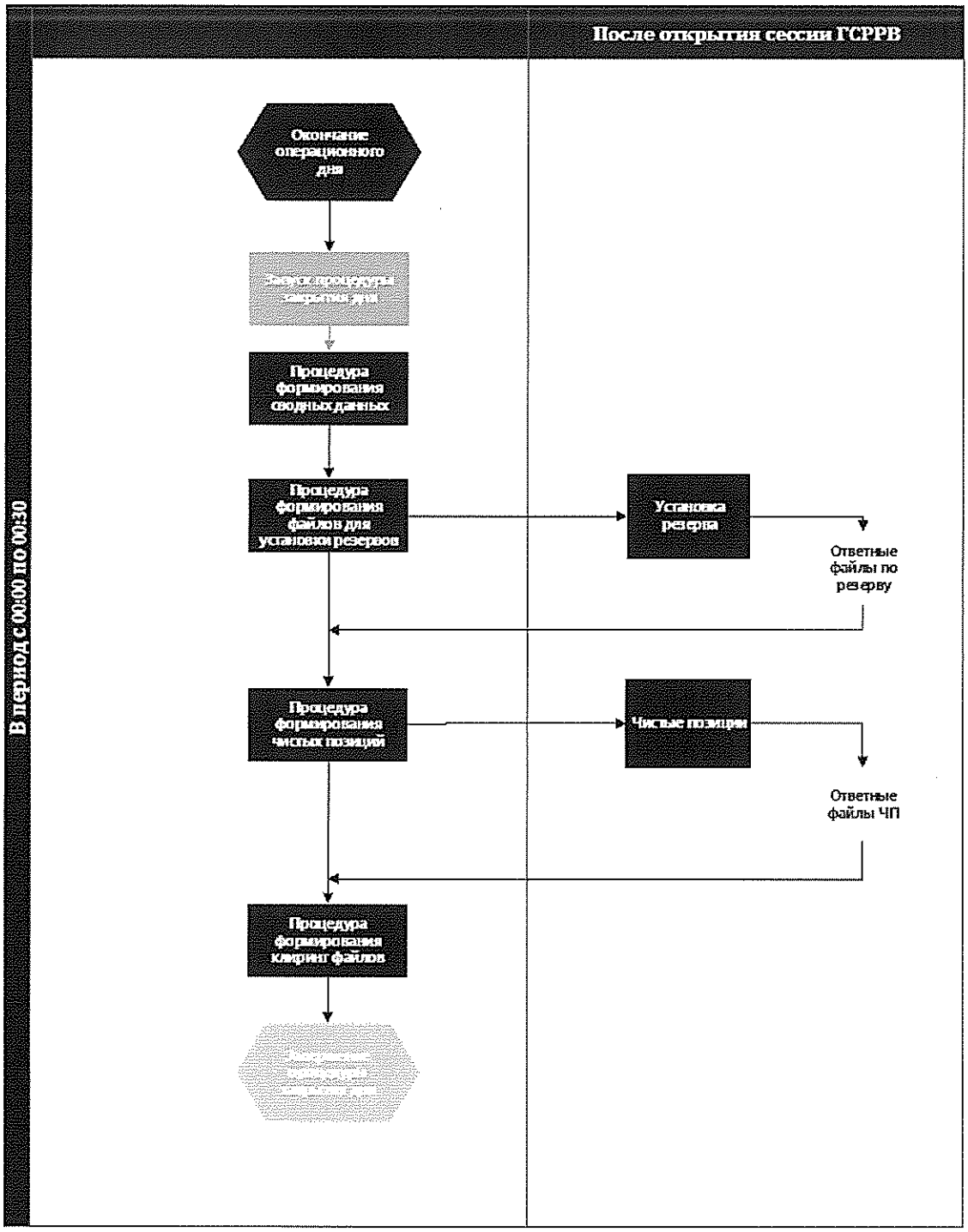

Рисунок 8. Процесс Закрытия операционного дня Оператора взаимодействия

Приложение А
к Техническому регламенту Оператора взаимодействия

Описание полей:
transaction_no- уникальный номер транзакции
dtcr_flag -'D'дебетовый/'C'кредитный флаг транзакции (1 символ)
amount - сумма транзакции (разделитель .00)
commission - сумма комиссии транзакции
curr - валюта сделки (iso 4217 - 3 цифры)
transaction_type - из приведенного ниже списка кодов операций
bic - БИК банка (8 символов)
bank_account - внешний счет (16 символов)
psp_id - идентификатор платежного приложения
bank_id - идентификатор банка
created_time - DD/MM/YYYY hh:mm:ss
executed_time - DD/MM/YYYY hh:mm:ss

Типы транзакций:
10 - перевод по QR-коду/ссылке на оплату.

20 - Покупка по QR-коду/платежной ссылке.

30 - Государственный платеж (физическое лицо) по QR-коду/платежной ссылке.

40 - Перевод/выдача денег/возврат по QR-коду/платежной ссылке

50 - Оплата/перевод по QR-коду/ссылке на оплату

60 - Электронное сообщение о создании резерва в банк

70 - Государственный платеж (юридическое лицо) по QR-коду/платежной ссылке.


```
{
    "transactions": [
      {
        "transaction_no": "1234569467",
        "dtcr_flag": "'D'",
         "amount": 50000,
         "commission": 0,
         "curr": 417,
         "transaction_type": 50,
         "bic": 11800002,
         "bank_account": 1180000000000000,
         "psp_id": 1,
         "bank_id": 1,
         "created_time": "26/11/2022 23:13:42",
         "executed_time": "26/11/2022 23:13:56"
      }
    ],
```

```
    "checksum": {
      "total_count": 1,
      "total_sum": 50000
    }
  }
],
  {
    "transactions": [
      {

        "transaction_no": "1234569465",
        "dtcr_flag": "'C'",
        "amount": 70000,
        "commission": 0,
        "curr": 417,
        "transaction_type": 10,
        "bic": 11800000,
        "bank_account": 1180000000000000,
        "psp_id": 1,
        "bank_id": 1,
        "created_time": "26/11/2022 23:13:42",
        "executed_time": "26/11/2022 23:13:56"
      }
    ],
    "checksum": {
      "total_count": 1,
      "total_sum": 70000
    }
  }
```

DemirBank
банк для вашей жизни

Приложение Б
к Техническому регламенту
Оператора взаимодействия

Анкета – опросник
по информационной безопасности
для Прямых участников и Косвенных участников/PSP

Закрытое акционерное общество
«Демир Кыргыз Интернэшнл Банк»
Версия 1.0

Введение

Анкета – опросник предназначен для всех Прямых участников и поставщиков платежных услуг, определенных Оператором взаимодействия как организации, имеющие право по проведению Платежей с использованием двухмерных символов штрихкода (QR-код).

Порядок заполнения анкеты – опросника

1. Идентифицируйте себя как Прямого участника или поставщика платежных услуг.
2. Подтвердите, что ваша среда настроена должным образом.
3. Оцените соответствие вашей среды необходимым требованиям по информационной безопасности (ИБ).
4. Заполните все разделы настоящего документа.
5. Отправьте заполненную Анкету – опросник, а также любые другие требуемые документы Оператору взаимодействия.

Заполнение анкеты – опросника

- При ответе на каждый вопрос воспользуйтесь предложенными вариантами ответов, чтобы обозначить текущий статус.

- Ответы должны быть понятными и отображать текущее положение «как есть».

- Если какое-либо из требований неприменимо к вашей среде, укажите об этом и дайте свои комментарии.

Раздел 1: Информация об организации

Часть 1. Информация об организации			
Наименование организации:		Коммерческое обозначение (DBA):	
ФИО контактного лица по информационной безопасности		Должность:	
Номер телефона:		E-mail:	
Адрес компании:		Город:	
Регион/Область:		Страна:	

Часть 2. Описание среды	
Тип предоставляемых платежных сервисов и услуг (например, интернет-банкинг, мобильные приложения, терминалы и другое)	
Как и в каком объеме ваша организация хранит, обрабатывает и / или передает ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА?	
Перечислите типы объектов, где хранятся, обрабатываются, передаются ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА (например, корпоративные офисы, центры обработки данных, центры обработки вызовов и т. д.) и краткую информацию о местах.	

Раздел 2: Поддержка защищенной сети и систем

1. Установка и поддержание конфигурации межсетевых экранов для защиты информации, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА		Ответ	Комментарии
1.1	Использует ли ваша организация сегментацию сети, для отделения среды, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА от остальных сетей? *Если ответ "ДА ", то необходимо в графе "Комментарии" предоставить соответствующую информацию с кратким описанием.*		
1.2	Разработана и внедрена ли в организации локальный нормативный акт по безопасной конфигурации межсетевых экранов и маршрутизаторов? *Если ответ "ДА ", то необходимо в графе "Комментарии" указать перечень наименований локальных нормативных актов.*		
1.3	Ограничены ли соединения между не доверенными сетями и любыми системными компонентами в информационной среде, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА в конфигурациях межсетевых экранов и маршрутизаторов? Если *ответ "ДА ", то необходимо в графе "Комментарии" предоставить соответствующую информацию с кратким описанием.*		
1.4	Запрещен ли прямой публичный доступ между сетью Интернет и любым системным компонентом в информационной среде, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА? *Если ответ "ДА ", то необходимо в графе "Комментарии" предоставить соответствующую информацию с кратким описанием.*		
1.5	Используются ли программные межсетевые экраны или подобные решения на портативных устройствах (например, ноутбуки), которые при нахождении вне корпоративной сети подключены к сети Интернет и которые используются для подключения к среде, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА? *Если да, то регламентировано ли использование подобных решений? В графе "Комментарии" необходимо указать перечень наименований ВНД.*		

2. Запрет использования паролей к системам и других параметров безопасности, заданных производителем по умолчанию		Ответ	Комментарии
2.1	Изменяются или отключаются заданные производителем параметры по умолчанию, включая неиспользуемые предустановленные учётные записи системных компонентов и проводится ли регулярная проверка изменения параметров, заданных производителем? *Если ответ "ДА", то в графе "Комментарий" необходимо предоставить соответствующую информацию с кратким описанием и периодичностью мероприятия.*		
2.2	Разработаны ли стандарты конфигурации для всех системных компонентов и соответствуют ли такие стандарты принятым в отрасли стандартам усиления защиты систем? *Если ответ "ДА ", то необходимо в графе "Комментарий" предоставить информацию по наименованию стандартов конфигурации.* Например, к источникам общепринятых отраслевых стандартов по безопасной настройке систем относятся, среди прочих: Центр Интернет- безопасности (CIS); Международная организация по стандартизации (ISO); Институт системного администрирования, аудита, сетевых технологий и проблем безопасности (SANS); Национальный институт стандартов и технологий (NIST), DoD Cyber Exhange Public (STIG).		
2.3	Защищен ли любой не консольный административный доступ к компонентам среды содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА с использованием одного или нескольких способов ниже: 1) с помощью надежной криптографии и вызовом надежного метода шифрования до запроса пароля администратора. 2) Запрет на использование небезопасных команд удаленного входа (например, Telnet). 3) Шифрование доступа администратора к веб- интерфейсам управления с помощью надежной криптографии 4) Эффективная криптография для используемых технологий в соответствии с передовыми отраслевыми практиками? 5) Другой. *Если ответ "ДА ", то необходимо в графе "Комментарий" предоставить соответствующую информацию с кратким описанием по каждому пункту, в частности, с указанием используемых*		
2.4	Ведется ли инвентаризация для системных компонентов, которые входят в среду обработки, хранения, передачи информации, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА, включая список аппаратных и программных компонентов и описание функций / использования для каждого из них? *Если ответ "ДА ", то необходимо в графе "Комментарий" предоставить соответствующую информацию с кратким описанием и указанием периодичности проведения инвентаризации.*		

3. Защита информации, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА		Ответ	Комментарии
3.1	Сведено ли хранение информации, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА к минимуму с помощью локальных нормативных актов, регламентирующих процессы хранения и уничтожения данных, в которые включены, как минимум, следующие пункты для всех хранилищ с информацией содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА: - Ограничение количества хранимых данных и сроки хранения до значений, необходимых для выполнения законодательных, нормативных и (или) служебных требований; - Процессы безопасного удаления данных, когда в них уже нет необходимости; - Ежеквартальный процесс обнаружения и безопасного удаления информации, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА, по которой превышены сроки хранения, установленные требованиями. *Если ответ "ДА ", то необходимо в графе "Комментарий" предоставить соответствующую информацию с указанием перечня наименований локальных нормативных актов по хранению и уничтожению информации, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА*		
3.2	Используются ли секретные и закрытые криптографические ключи для шифрования/дешифрования данных по платежам. *Если ответ "ДА ", то необходимо в графе "Комментарий" предоставить соответствующую информацию по длине ключа, срокам действия, тип шифрования.*		
3.3	Используется ли стойкая криптография, безопасные протоколы или иные меры, чтобы защитить информацию, содержащую ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА при их передаче через открытые общедоступные сети, такие как Интернет, беспроводная связь, спутниковые средства связи и т.п., в частности, учетом исполнения следующего списка мер: - принимаются только доверенные ключи и сертификаты; - используемый протокол поддерживает только безопасные версии и конфигурации; - стойкость шифрования соответствует используемой методологии шифрования. *Если ответ "ДА ", то необходимо в графе "Комментарий" предоставить соответствующую информацию с кратким описанием по каждому пункту.*		
3.4	Являются ли политики безопасности и рабочие процедуры защиты хранимых данных по платежам: - задокументированными и утвержденными; - используемыми; - известным всем вовлеченным лицам? Если *ответ "ДА ", то необходимо в графе "Комментарий" предоставить соответствующую информацию, в частности, с указанием перечня ВНД.*		

4. Защита всех систем от вредоносного ПО и регулярное обновление антивирусных ПО или программ		Ответ	Комментарии
4.1	Установлено ли антивирусное программное обеспечение на всех системах, предусмотренных технологическим процессом, которые подвержены воздействию вредоносного ПО (в частности, на персональных компьютерах и серверах)?		
4.2	Защищены ли конфигурации антивирусных механизмов от действий пользователей (изменение настроек, отключение защиты и т.п.)?		
4.3	Все ли антивирусные механизмы поддерживаются в актуальном состоянии? *Если ответ "ДА ", то необходимо в графе "Комментарий" предоставить соответствующую информацию с указанием периодичности обновления антивирусного ПО (включая базы данных сигнатур), периодичности проведения антивирусных сканирований и сроков хранения журналов регистрации событий антивирусного ПО (по всем мероприятиям необходимо перечислить типы системных компонент, в которых данные мероприятия проводятся).*		
4.4	Являются ли политики безопасности и рабочие процедуры защиты систем от вредоносного ПО: - задокументированными и утвержденными; - используемыми; - известные всем вовлеченным лицам? *Если ответ "ДА", то необходимо в графе "Комментарий" указать перечень наименований ВНД.*		
5. Разработка и поддержание безопасных систем и приложений, содержащих ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА			
5.1	Безопасно ли разрабатываются внутренние и внешние приложения (включая административный доступ к приложениям через веб-интерфейс), в частности, с учетом следующих пунктов: на основе безопасной аутентификации и ведению журналов регистрации событий на основе отраслевых стандартов и рекомендаций с учетом обеспечения информационной безопасности в течение всего цикла разработки ПО В графе "Комментарии" необходимо предоставить ответ по каждому пункту. Примечание: в частности, включая любое ПО собственной разработки и заказное ПО, разработанное третьим лицом.		

5.2	Производится ли управление распространенными уязвимостями программного кода в процессе разработки ПО следующим образом: обучение разработчиков ПО не реже одного раза в год актуальным методикам безопасного программирования, включая информацию о том, как избежать распространенных программных уязвимостей? разработка ПО в соответствии с основными принципами безопасного программирования? В графе "Комментарии" необходимо предоставить ответ по каждому пункту, в частности: периодичность обучения разработчиков перечень используемых отраслевых стандартов, рекомендаций и лучших практик по управлению уязвимостями Примечание: Примеры отраслевых рекомендаций по управлению уязвимостями - Руководство OWASP, Список SANS CWE Top 25, CERT Secure Coding.		
5.3	Производится ли постоянное управление новыми угрозами и уязвимостями общедоступных веб- приложений и обеспечивается ли этим приложениям защита от известных атак в соответствии со следующими методами: проверка общедоступных веб-приложений на наличие уязвимостей, используя методы или инструменты ручного или автоматизированного анализа защищенности приложений не реже одного раза в год, а также после внесения любых изменений установка автоматизированного технического средства (например, межсетевой экран уровня веб- приложений) перед общедоступными веб- приложениями для непрерывной проверки всего трафика, в целях обнаружения, предупреждения и предотвращения веб-атак В графе "Комментарии" необходимо предоставить ответ по каждому пункту, в частности, с указанием метода защиты от известных атак.		
5.4	Документированы\используются\известны ли всем заинтересованным лицам локальные нормативные акты по безопасности и операционным процессам разработки и поддержки безопасных систем и приложений? *Если ответ "ДА ", то необходимо в графе "Комментарии" предоставить соответствующую информацию с развернутым ответом, в частности с указанием перечня наименований локальных нормативных актов.*		
6. Ограничение доступа к ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА в соответствии со служебной необходимостью			
6.1	Ограничен ли доступ к системным компонентам и ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА, доступ предоставляется только тем лицами, которым такой доступ требуется в соответствии с их служебными обязанностями? *Если ответ "ДА", то необходимо в графе "Комментарии" указать методы и подходы ограничения доступа к системным*		

	компонентам и ДАННЫЕ ПО ПЛА ТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА.		
6.2	Установлена ли система (или системы) контроля доступа к системным компонентам и информации, содержащие ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА, которая ограничивает доступ в соответствии со служебной необходимостью пользователя, и которая настроена запрещать все, что явным образом не разрешено? *Если ответ "ДА", то необходимо в графе "Комментарии" указать каким образом реализована система контроля доступа к системным компонентам.*		
6.3	Документированы\используются и известны ли всем заинтересованным лицам локальные нормативные акты по безопасности и операционным процессам ограничения доступа к информации, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА? *Если ответ "ДА", то необходимо в графе "Комментарии" указать перечень наименований локальных нормативных актов по безопасности и операционным процессам.*		
7. Идентификация и аутентификация доступа к системным компонентам и информации, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА			
7.1	Помимо назначения уникального идентификатора, обеспечивается ли надлежащее управление аутентификацией пользователей и администраторов на уровне всех системных компонентов, применяя один из следующих методов аутентификации: 1) обладание информацией (например, паролем или парольной фразой) обладание предметом (например, аппаратным токеном или смарт-картой) обладание параметрами (например, биометрическими) *Если ответ «ДА», в графе "Комментарии" необходимо указать используемые методы аутентификации.*		
7.2	Защищены ли все индивидуальные не консольные административные доступы и все удаленные доступы в информационную среду, содержащую ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА - с использованием мультифакторной аутентификации? *Если ответ "ДА ", то необходимо в графе "Комментарии" указать используемые способы двухфакторной аутентификации.*		

7.3	Используются ли общие учетные записи и стандартные учетные записи пользователей для системного администрирования любых системных компонент и иных критичных функций? *Если ответ "ДА", то необходимо в графе "Комментарии" предоставить соответствующую информацию с кратким ответом.*		
7.4	Ограничивается ли любой доступ к базе данных, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА (включая доступ со стороны программных приложений, администраторов и любых других пользователей) в соответствии со следующими пунктами: осуществление доступа, запросов и операций с базами данных только при помощи программных методов разрешение запросов и прямого доступа к базам данных только администраторам баз данных разрешение использования учетных записей программных приложений для доступа к базам данных только программным приложениям (а не отдельным пользователям или иным процессам) В графе "Комментарии" необходимо предоставить ответ по каждому пункту.		
7.5	Документированы и внедрены ли локальные нормативные акты, обеспечивающие надлежащее управление аутентификацией и идентификацией, и доведены ли данные локальные нормативные акты до сведения всех пользователей, включая: рекомендации по выбору надежных учетных данных для аутентификации? рекомендации для пользователей по защите учетных данных для аутентификации? указания не использовать ранее использованные пароли? указания по смене пароля в случае подозрения на его компрометацию? *Если ответ «ДА», то необходимо в графе "Комментарии" указать перечень наименований локальных нормативных актов по аутентификации.*		
8. Ограничение физического доступа к информации, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА			
8.1	Используются ли средства управления доступом на территории организации, чтобы ограничивать и отслеживать физический доступ к системам среды, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА? *Если ответ "ДА", то необходимо в графе "Комментарии" необходимо указать способы контроля и отслеживания физического доступа к системам среды, содержащей ДАННЫЕ ПО ПЛА ТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА.*		

8.2	Документированы, используются и известны всем заинтересованным лицам локальные нормативные акты по безопасности и операционным процедурам ограничения физического доступа к информации, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА? *Если ответ "ДА", то необходимо в графе "Комментарии" необходимо указать перечень наименований локальных нормативных актов.*		
9. Отслеживание и ведение мониторинга всего доступа к сетевым ресурсам и информации, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА			
9.1	Реализованы ли автоматизированные журналы регистрации событий на всех системных компонентах, чтобы можно было восстановить и отследить все события? *Если ответ "ДА ", то необходимо в графе "Комментарии" необходимо указать перечень типов системных компонент, для которых реализованы автоматизированные журналы регистрации событий*		
9.2	Записываются ли в журналах регистрации событий, для каждого события каждого системного компонента, как минимум, ID пользователя, тип события, дата и время, успешное или неуспешное завершение события, источник события, ID системного компонента или ресурса, на которые воздействовало событие?		
9.3	Синхронизируются ли все часы и системное время в критичных системах с помощью механизмов синхронизации времени?		
9.4	Защищаются ли журналы регистрации событий от изменений?		
9.5	Проверяются ли журналы и события безопасности всех системных компонентов, чтобы выявлять аномалии или подозрительную активность?		
9.6	Сохраняется ли история журналов регистрации событий не менее одного года, причем в оперативном доступе должна находиться история не менее чем, за последние три месяца (например, в прямом доступе, в архиве, либо с возможностью восстановления из резервной копии)?		
9.7	Внедрен ли процесс своевременного обнаружения и отчетности об ошибках в критичных системах контроля безопасности?		
9.8	Документирован ли процесс мониторинга доступа к системным компонентам и ресурсам, содержащим ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА, и доведены до сведения заинтересованных сотрудников? *Если ответ "ДА ", то необходимо в графе "Комментарии" необходимо указать перечень наименований локальных нормативных актов.*		

10. Регулярное тестирование систем и процессов безопасности			
10.1	Внедрены ли процессы ежеквартальной проверки на наличие беспроводных точек доступа (802.11), а также выявления и идентификации санкционированных и несанкционированных беспроводных точек доступа?		
10.2	Проводится ли внешнее и внутреннее сканирование сети на наличие уязвимостей, а также после значительных изменений в сети (в частности, установки новых системных компонентов, изменения топологии сети, изменения правил межсетевых		
10.3	Проводится ли тестирование на проникновение среды, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА и критичных систем: если ответ да, в графе "Комментарии" необходимо указать периодичность мероприятия.		
10.4	Осуществляется ли мониторинг всего сетевого трафика по периметру среды, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА и в критичных точках внутри среды, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА, и оповещаются ли работники о подозрениях на компрометацию? *Если ответ "ДА", то необходимо в графе "Комментарии" указать используемые механизмы и методы.*		
10.5	Поддерживаются ли в актуальном состоянии системы обнаружения и предотвращения вторжений, их сигнатуры и правила?		
10.6	Внедрено ли средство обнаружения изменений (например, мониторинг целостности файлов), чтобы уведомлять работников о несанкционированных изменениях (включая, изменения, добавления и удаления) критичных системных файлов, конфигурационных файлов или файлов данных?		
10.7	Документированы и известны ли всем заинтересованным лицам локальные нормативные акты по безопасности и операционным процессам мониторинга и проверки безопасности? *Если ответ "ДА ", то необходимо в графе "Комментарии" указать перечень наименований локальных нормативных актов.*		
11. Поддержание политики информационной безопасности для всех работников.		-	-
11.1	Регламентирован ли процесс управления и оценки ИТ/ИБ-рисков? *Если ответ «ДА», необходимо в графе "Комментарии" указать перечень наименований локальных нормативных актов.*		
11.2	Имеются ли локальные нормативные акты, описывающие процесс защиты информации, содержащий ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА, если да, то доведено ли до сведения соответствующего персонала?		

	Если ответ "ДА", то необходимо в графе "Комментарии" необходимо указать наименования локальных нормативных актов.		
11.3	Тщательно ли происходит проверка потенциальных работников до приема на работу, чтобы минимизировать риск внутренних атак?		
11.4	Внедрены и поддерживается ли локальные нормативные акты по управлению поставщиками услуг, у которых есть доступ к информации, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА или которые могут воздействовать на безопасность информации содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА? *Если ответ "ДА", то необходимо в графе "Комментарии" указать названия локальных нормативных актов.*		
11.5	Подтверждают ли письменно поставщики услуг или клиенты, имеющие доступ к информации, содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА, что они отвечают за безопасность информации содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR- КОДА, которую они хранят, обрабатывают или передают от имени клиента, или отвечают в той мере, в которой они могут воздействовать на безопасность среды содержащей ДАННЫЕ ПО ПЛАТЕЖАМ С ИСПОЛЬЗОВАНИЕМ QR-КОДА?		
11.6	Документированы и используется ли локальные нормативные акты по реагированию на инциденты? *Если ответ "ДА ", то необходимо в графе "Комментарии" необходимо указать перечень наименований нормативных документов по реагированию на инциденты.*		
11.7	Проводится ли ежеквартальная проверка на предмет соблюдения сотрудниками локальных нормативных актов по обеспечению безопасности и операционных процедур?		

Приложение В
к Техническому регламенту
Оператора взаимодействия

СТРУКТУРА
передаваемых данных

Иерархия стандарта позволяет стандартизировать и обеспечить операционную совместимость как международных, так и локальных платежных систем.

QR-код, использующийся для совершения платежей и переводов в рамках данной спецификации, содержит платежную ссылку, которая представляет собой URI (Uniform Resource Identifier (унифицированный идентификатор ресурса)) и имеет вид:

схема://хост_провайдера_платежей_и_переводов#фрагмент, где:

- имя схемы по умолчанию содержит https;

- имя хоста провайдера платежей и переводов по умолчанию содержит домен участника платежных систем (имя хоста провайдера платежей и переводов может быть любым), и должно иметь возможность последующего перехода на домен оператора взаимодействия, обеспечивающего операционную совместимость между платежными инструментами всех участников платежных систем;

- фрагмент содержит детали платежа.

СПЕЦИФИКАЦИЯ
платежного QR-кода

Введение

Спецификация платежного QR-кода предназначена стандартизировать взаимообмен на рынке платежных услуг с целью обеспечения операционной и взаимной совместимости имеющихся на рынке решений совершения платежей и переводов по QR-коду.

За основу взят стандарт QR-кода "EMV QR Code Specification for Payment Systems Merchant-Present Mode Requirements".

Сокращения и обозначения

QR-код	(англ. Quick Response Code - код быстрого реагирования) считываемая машиной оптическая метка, содержащая информацию об объекте, к которому она привязана
Поставщик услуг и/или Поставщик	юридическое лицо или индивидуальный предприниматель, получающий денежные средства клиента за реализуемые товары, выполняемые работы, услуги
Информационная система или ИС	автоматизированная система поставщика услуги для приема, обработки и учета платежей и переводов
Платежный шлюз	аппаратно-программный комплекс для проведения платежей и переводов в пользу поставщиков услуг (в рамках заключенных Договоров), включая проведение финальных взаиморасчетов

Описание принципа работы

QR-код, использующийся для совершения платежей и переводов в рамках данной спецификации, содержит платежную ссылку, которая представляет собой URI, и имеет вид:

схема://хост_провайдера платежей_и_переводов#фрагмент, где:

- имя схемы по умолчанию содержит https (имя схемы может быть любым);

- имя хоста провайдера платежей и переводов по умолчанию содержит домен участника платежных систем (имя хоста провайдера платежей и переводов может быть любым) и должно иметь возможность последующего перехода на домен оператора взаимодействия, обеспечивающего операционную совместимость между платежными инструментами всех участников платежных систем;

- фрагмент содержит детали платежа.

Примечание:

(1) Если у плательщика нет приложения, которое умеет обрабатывать фрагментную часть ссылки (детали платежа), он будет перенаправлен на хост провайдера платежей и переводов (по умолчанию на https://участника платежных систем), где ему будет предоставлен канал оплаты по QR-коду и также реализован переход на домен оператора взаимодействия, где размещен список приложений, которые могут осуществлять обработку фрагментной части ссылки.

(2) Если у плательщика есть приложение одного из участников оператора взаимодействия, которое умеет обрабатывать фрагментную часть ссылки (детали платежа), но при этом не является платежным приложением участника платежной системы, сформировавшего сканируемый QR-код, то он будет направлен на хост провайдера платежей и переводов (по умолчанию на https://участника платежных систем/владельца приложения), где ему будет предоставлен канал оплаты по QR-коду. При этом взаимодействие с участником платежной системы, сформировавшего сканируемый QR-код, осуществляется через оператора взаимодействия.

(3) Если у плательщика есть приложение, которое умеет обрабатывать фрагментную часть ссылки (детали платежа), и оно является приложением данного участника платежной системы (сформировавшего сканируемый QR код), ему будет предоставлен канал оплаты по QR-коду.

Структура данных фрагмента URI - деталей платежа

Данные деталей платежа организованы в виде последовательности объектов. Объект содержит идентификатор (ID), длину и собственно данные:

- ID закодирован двумя цифрами в диапазоне от "00" до "99";

- длина также закодирована двумя цифрами в диапазоне от "01" до "99";

- данные представлены последовательностью символов, минимальная последовательность равна одному символу, максимальная - 99 символов.

Данные деталей платежа имеют древовидную структуру. Начиная от корня, данные могут содержать примитивные объекты (элементы) или шаблоны. Шаблоны могут включать в себя другие шаблоны или примитивные объекты.

Пример:

- корневой объект;

- примитивный объект;

    - шаблон;

    - примитивный объект;

    - шаблон.

Объекты

Объекты, которые должны обязательно присутствовать в деталях платежа, обозначены символом "M", если присутствие объекта в коде зависит от неких условий, то такие объекты помечены символом "C", все необязательные объекты помечены символом "O".

Идентификатор - ID

Идентификатор кодируется двумя цифрами в диапазоне от "00" до "99".

Длина

Представлена двумя цифрами в диапазоне от "01" до "99" и должна равняться длине поля данных.

Данные

Данные могут быть:

- цифровыми (N);

- алфавитно-цифровыми с ограниченным набором символов (ans);

- строковыми (S).

Цифровые данные - это подмножество алфавитно-цифровых с ограниченным набором символов, а алфавитно-цифровые - это подмножество строковых.

Организация данных

Данные для формирования деталей платежа должны начинаться корневым элементом (корневые объекты) с идентификатором "00" и заканчиваться элементом с идентификатором "63".

Используемые символы

В случае если во фрагменте используются символы, выходящие за пределы кодировки ASCII, а именно: ":", "/", "?", "#", "[", "]", "@", "!", "$", "&", "'", " ", "(", ")", "*", "+", ",", ";", "=", ALPHA, DIGIT, HEXDIG, "-", ".", "_", "~", где:

- ALPHA - любая буква верхнего и нижнего регистров кодировки ASCII (в regExp [A-Za-z]);

- DIGIT - любая цифра (в regExp [0-9]);

- HEXDIG - шестнадцатиричная цифра (в regExp [0-9A-F])

используется механизм т.н. "процентного кодирования". Перечисленные выше символы не участвуют в процентном кодировании. Процентно-кодированный символ представляет из себя символьный триплет, состоящий из знака "%" и следующих за ним двух шестнадцатиричных чисел:

Таким образом, %20, например, означает пробел.

Корневые элементы

Перечень корневых объектов:

Наименование	ID	Формат	Длина	Признак	Комментарий
Версия стандарта	00	N	"02"	M	
Тип платежной ссылки	01	N	"02"	M	
Информация о поставщике услуг, услуге и т.д.	02-51	ans	до "99"	M	
MCC код производителя услуг	52	N	"04"	M	
Код валюты	53	N	"03"	M	по умолчанию 417
Сумма платежа	54	N	до "13"	C	
Наименование поставщика услуг (латиницей)	59	ans	до "25"	M	

Контрольная сумма данных	63	ans	"04"	M	

ID "00" - Версия стандарта - объект обязательный

Данное поле должно быть первым и содержать значение "01".

ID "01" - Тип платежной ссылки - объект обязательный

Если присутствует, то должен содержать значения:

11 - если детали платежа используются для совершения более чем одной транзакции, статические коды, обычно с оплатой, где сумму может вводить сам покупатель, например, для использования в такси, уличной торговле и других точках с невысокой скоростью обслуживания покупателей;

12 - если для каждой транзакции необходимы новые детали платежа, динамические детали платежа, которые могут использоваться в интернет-магазинах, объектами общественного питания.

IDs "02" до "51" - Информация об оплачиваемой услуге, поставщике услуг - объект обязательный

Структура поля содержит элементы шаблона информации об оплачиваемой услуге.

Элемент с идентификатором "32", обязательный для указания, содержит код услуги в Платежном шлюзе, идентификатор плательщика в пределах услуги в системе поставщика услуг (номер телефона, номер заказа, номер договора и т.д.).

Элементы с идентификаторами от "35" до "39" содержат набор доп. полей платежа.

ID "32" - Объект с информацией об оплачиваемой услуге, для всех поставщиков услуг - объект обязательный

Наименование	ID	Формат	Длина	Признак	Комментарий
Уникальный идентификатор	00	ans	до "32"	O	Объект по умолчанию содержит домен участника платежной системы и имеется возможность последующего перехода на домен оператора взаимодействия.
Спецификация платежной сети	01	N	От 6 до 10	M	Код услуги в платежном шлюзе
Уникальный идентификатор плательщика в пределах услуги	10	S	До 32	O	Уникальный идентификатор плательщика в пределах услуги в ИС поставщика услуг
Идентификатор транзакции	11	S	До 32		Идентификатор транзакции в ИС поставщика
Возможность редактирования суммы к оплате	12	N	2	C	11 - разрешить плательщику изменять сумму, переданную в объекте 54. 12 - не разрешать плательщику изменять сумму, переданную в объекте 54. По умолчанию плательщику редактирование суммы разрешено. Приоритетной возможностью редактирования суммы является

					опция, указанная поставщиком услуг.
Возможность редактирования идентификатора плательщика (ID - 10) к оплате	13	N	2	C	11 - разрешить плательщику изменять значение, переданное в объекте 10. 12 - не разрешать плательщику изменять значение, переданное в объекте 10. По умолчанию плательщику редактирование разрешено.

Если объект "10" пустой и объект "13" равен 12, то необходимо скрыть поле ввода уникального идентификатора плательщика.

ID "33" - Объект с информацией об оплачиваемой услуге, для всех поставщиков услуг - объект необязательный (резервный)

IDs "35" - "39" - объект с дополнительными полями поставщика услуг. Объект необязательный

Содержит последовательность, начинается с идентификатора "00" и заканчивается идентификатором "99". Если нужное количество дополнительных полей не вмещается в первый объект, необходимо использовать следующий, по порядку ("35", "36", ... "39").

Значение каждого дополнительного поля содержит строку в следующем формате, с уникальным разделителем ":":

Наименование	Комментарий
key	Идентификатор поля в ИС поставщика услуги
label	Название поля
value	Значение поля
title	Значение поля, выводимое пользователю
visible_state	"11" - отображается пользователю; "12" - не отображается пользователю

Признак "visible_state" указывает нужно ли отображать данное поле пользователю в интерфейсе. Как правило, данные дополнительного поля следует отправлять в используемый платежный шлюз, согласно его протоколу взаимодействия.

Если "visible_state" имеет признак "11", заполнено поле "value", то в интерфейсе пользователю необходимо вывести значение из поля "title".

ID "52" - MCC код поставщика услуг - объект обязательный

Содержит 4-х значный код, определяющий категории продавца при операциях с банковской картой. По MCC определяется категория финансовой операции. Поле содержит цифры от "0" до "9". MCC коды определены в ISO 18245.

ID "53" - Код валюты - объект обязательный

Код валюты (ISO 4217) должен содержать 3-значный код валюты. По умолчанию необходимо использовать код валюты 417 - кыргызский сом.

ID "54" - Сумма платежа - объект не обязательный, условный

Используется поставщиком услуг при генерации деталей платежа.

Если присутствует, то должен содержать значение отличное от нуля. Поле содержит цифры от "0" до "9" и указывается в тыйнах.

Если поле отсутствует, то покупатель в приложении должен задать сумму, которую он платит поставщику услуг.

ID "59" - Наименование поставщика услуг - объект обязательный

Используется поставщиком услуг при генерации деталей платежа. Поле содержит наименование продавца (производителя услуг) латинскими буквами.

ID "63" - Контрольная сумма - объект обязательный

Контрольная сумма данных используется для проверки целостности данных, указанных в деталях платежа.

Алгоритм формирования:

1. Все значения деталей платежа до объекта 63 (ID "00" - "90", за исключением ID 63) преобразуются в одну строку.

2. Строка данных переводится в массив байт с кодировкой UTF-8.

3. Вычисляется хеш массива, используя алгоритм SHA256.

4. Массив байт преобразуется в строку.

5. Удаляются все символы "-", если они есть.

6. Из строки берутся последние 4 символа.

Использование данных из платежной ссылки для осуществления информационного взаимодействия

При генерации динамической платежной ссылки Поставщиком услуги необходимо использовать код услуги в Платежном шлюзе для корректной обработки деталей платежа.

Дополнительное использование платежной ссылки

Платежная ссылка, которая используется для формирования QR-кода, может передаваться плательщикам дополнительными следующими способами:

1. Генерация на сайте (мобильном приложении) Поставщика услуг (в том числе в виде URI-кнопки).

2. Push-уведомление в приложении.

3. SMS.

4. Мессенджеры (в том числе в виде URI-кнопки).

5. E-mail.

6. NFC-технология, обеспечивающая обмен данными между поддерживающими данную технологию устройствами. Например, передача приложением на смартфоне поставщика услуг на смартфон плательщика, или считывание смартфоном плательщика URI, записанный на пассивной NFC-метке поставщика услуг.

7. И т.п.

Дополнительная информация для пунктов совершения платежей и переводов (далее - ПСП) расчетного агента

1. Мобильным приложениям участников платежных систем (на всех операционных системах) необходимо настроить связь с доменом https://оператора взаимодействия для обеспечения операционной совместимости между платежными инструментами всех участников платежных систем.

2. Аналогичную связь рекомендуется осуществить между мобильным платежным приложением и собственным сайтом владельца приложения (для предложения пользователю открыть страницу в приложении или установить приложение).

3. Мобильное платежное приложение и иной ПСП (например, интернет-банкинг), на который можно перейти по URI, должны быть готовы к обработке фрагментной части QR-кода (платежной ссылки).

4. На всех стадиях совершения платежа ПСП плательщику должны быть отображены все детали выбранных (в том числе автоматически используя платежную ссылку) действий:

- название поставщика услуг;
- лицевой счет, отправленный в запросе параметров услуги протокола;
- дополнительные поля;
- сумма.

Пронумеровано и прошнуровано
на 38 (тридцать восемь) листах