

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Оказание услуг по информационному и технологическому взаимодействию при осуществлении переводов денежных средств (платежей) при реализации товаров (работ, услуг) с использованием банковских карт, топливных карт и системы быстрых платежей (СПБ) через сеть Интернет и других системах Заказчика

Термины и сокращения

№	Термин	Сокращение	Определение
1	АРМ		Автоматизированное рабочее место
2	Банк, банк-эквайер		Кредитная организация, обеспечивающая расчёты с МПС/НПС по проведённым операциям с использованием банковских платёжных карт.
3	Личный кабинет	ЛК	ИС Заказчика, предназначенная для предоставления Плательщикам информации и выполнения операций по управлению Лицевым счетом по принципу самообслуживания посредством сети Интернет
4	Мобильное приложение	МП	Мобильное приложение (Мобильное приложение «Автодор»), предназначенное для предоставления Плательщикам информации и выполнения операций по управлению Лицевым счетом посредством средств мобильной связи / мобильных устройств
5	Многофункциональный шлюз	МФШ	Программно-аппаратный комплекс Заказчика, предназначенный для взаимодействия с Платежным шлюзом Исполнителя с целью обеспечения процесса приемки Платежей.
6	МПС		Международные платежные системы VISA International и MasterCard International, UnionPay International
7	ПВП		Пункты взимания платы
8	НПС		Национальная платежная система МИР
9	ППШ агента	ППШ Агента	Платёжный шлюз агента. Могут быть ППШ как Банков-агентов, так и Организаций-агентов
10	Платёжный шлюз Исполнителя	ППШ Исполнителя	Программно-аппаратный комплекс Исполнителя, функционирующий на оборудовании Исполнителя в ЦОД Исполнителя, позволяющий автоматизировать процесс приёма платежей
11	Программное обеспечение	ПО	
12	Процессинговый центр Банка	ПЦ	Структурное подразделение Банка обеспечивающее проведение операций по приёму платежей с использованием банковских платёжных карт
13	Российская Федерация	РФ	
14	Система Быстрых Платежей	СБП	Сервис Банка России, позволяющий физическим лицам производить оплату товаров и услуг в розничных точках продаж (пунктах взимания платы за проезд по платным участкам автомобильных дорог) и сети Интернет по идентификатору получателя (QR-коду).
15	Система взимания платы	СВП	Распределенный аппаратно-программный комплекс, предназначенный для автоматизации взимания платы на платных дорогах Государственной компании «Автодор».
16	Топливные карты	ТК	Карта, используемая для автоматизации оплаты топлива на АГНКС, АГЗС или АЗС
17	Транспортное средство	ТС	
18	Центральный Банк Российской Федерации	ЦБ	
19	Центр обработки данных	ЦОД	
20	Сбер Pay		Метод оплаты с банковской карты сервисом ПАО Сбербанк
21	МТС Pay		Метод оплаты с банковской карты сервисом ПАО МТС Банк
22	T-Pay		Метод оплаты с банковской карты сервисом АО «ТБанк»
22	QR-код		Прочие методы оплаты с банковской карты при использовании QR-кода

Исполнитель оказывает услуги по информационному и технологическому взаимодействию при осуществлении переводов денежных средств (Платежей) при реализации товаров (работ, услуг) с использованием банковских карт (эквайринг в том числе с использованием Сбер Pay, МТС Pay, T-Pay, QR-кода), топливных карт и системы быстрых платежей через сеть Интернет и других системах Заказчика.

Основной целью оказания Услуг является обеспечение возможности проведения расчётов Заказчика с участниками взаиморасчётов.

Для целей надлежащего оказания Услуги Исполнителем осуществляется:

– Выполнение процессов приёма Платежей, в том числе на Лицевые счета Плательщиков, в качестве оплаты услуг организации платного проезда, в качестве оплаты иных товаров и услуг с использованием банковских карт (эквайринг платежей, в том числе с использованием Сбер Pay, МТС Pay, Т-Pay, QR-кода), топливных карт и СБП через сеть Интернет (интернет-эквайринг), на пунктах взимания платы (ПВП).

– Формирование перечня Банков для проведения Платежей, с которыми у Заказчика заключен договор (соглашение) на основании лучших стоимостных параметров для Заказчика и требований Заказчика в части технически бесперебойного сервиса по приему платежей.

– Определение угроз безопасности информации в связи с изменениями в информационной системе Заказчика, разработка модели угроз безопасности информации, разработка технического задания, технического проекта на систему защиты информации информационной системы, обрабатывающей данные платежей, а также проведение контроля защищенности в соответствии с проектной документацией.

– Определение на основании банковского идентификационного номера банковских карт в платежных сервисах Заказчика Банка-эмитента (банка, выпустившего карту) банковской карты, по которой производится платеж.

– Определение на основании банковского идентификационного номера принадлежность банковских карт в платежных сервисах Заказчика конкретной МПС или НПС.

– Обеспечение возможности направления платежей по банковским картам в следующие банки-эквайеры в рамках предоставленного алгоритма Заказчика в целях обеспечения бесперебойности предоставляемых сервисов:

- ПАО Сбербанк (ИНН 7707083893)
- ПАО Банк ВТБ (ИНН 7702070139)
- ПАО «АК БАРС» БАНК (ИНН 1653001805)
- АО «Банк Русский Стандарт» (ИНН 7707056547)
- Акционерное общество «ТБанк» (ИНН 7710140679)
- АО Банк ГПБ (ИНН 7744001497)
- Публичное акционерное общество "Банк Псб" (ИНН 7744000912)
- АО «Почта Банк» (ИНН 3232005484)
- АО «АЛЬФА-БАНК» (ИНН 7728168971)
- ПАО «Банк «Санкт-Петербург» (ИНН 7831000027)
- РНКБ Банк (ПАО) (ИНН 7701105460)
- ПАО «Банк Зенит» (ИНН 7729405872)
- АО «АБ «РОССИЯ» (ИНН 7831000122)
- И другие банки-эквайеры при наличии у Заказчика договора с ними и у Исполнителя технической интеграции с банком-эквайером.

– Осуществление направления на основании алгоритма, предоставленного Заказчиком, платежей по банковским картам определенных Заказчиком банков-эмитентов конкретных МПС/НПС в конкретные банки (на основании банковских идентификационных номеров карт), с которыми у Заказчика заключен договор (соглашение) в целях предоставления технически бесперебойного сервиса по приему платежей и снижения конечной суммы вознаграждения, уплачиваемого Заказчиком банкам. Алгоритм и последующие изменения алгоритма формируются Заказчиком и передаются Исполнителю в письменном виде за подписью уполномоченного представителя Заказчика по форме заявки, установленной в Приложении № 1.2 к Договору. Алгоритм описывает направление (маршрутизацию) платежей по банковским картам на основании принадлежности карты к той или иной МПС/НПС и/или банку-эмитенту в определенный Алгоритмом банк-эквайер.

– Осуществление перевода платежей по банковским картам и СБП из одного Банка в другой при условии наличия заключенного договора (соглашения) у Заказчика с этим Банком по указанию Заказчика в целях обеспечения бесперебойности сервиса приема платежей и снижения конечной суммы вознаграждения, уплачиваемого Заказчику банкам.

1. Технические требования к Платежному шлюзу

• 1.1. Требования к структуре и функционированию Платежного шлюза Исполнителя

1.1.1. Требования к структуре Платежного шлюза

Платежный шлюз должен обеспечивать операции, приведённые в таблице 1.

Таблица 1 – Подсистемы ПШ

№	Подсистема ПШ	Назначение
1	Модуль проведения расчётов с кредитными организациями	– осуществление информационного сопровождения расчётов с кредитными организациями.
2	Модуль Управления ПШ	– Бизнес-администрирование ПШ.

3	Платежный сервис	– Поддержка интеграционных решений с Процессинговыми центрами банков при проведении платежных операций с использованием
№	Подсистема ПШ	Назначение
		банковских карт в личном кабинете Пользователя на интернет-сайте и мобильном приложении.

1.1.2. Требования к характеристикам взаимосвязей Платежного шлюза со смежными системами

В ходе своего функционирования Платёжный шлюз должен осуществлять взаимодействие со следующими смежными системами:

1) Внутренние информационные системы Заказчика:

- МФШ;
- Битрикс 24;
- сайт и мобильное приложение «Автодор»;
- иные внутренние системы и системы контрагентов Заказчика, по согласованию с Заказчиком.

2) Карточные процессинговые центры Банков;

Связь со смежными подсистемами должна обеспечиваться согласно протоколам взаимодействия с каждой конкретной смежной системой.

ПШ должен обеспечивать:

- взаимодействие с МФШ;
- взаимодействие с внутренними платёжными компонентами;
- взаимодействие с ПЦ Банков;
- взаимодействие с системой отчетности ПО МФШ в части выгрузки данных из ПО ПШ (при условии наличия этих данных в ПО ПШ).

1.1.3. Требования к взаимодействию с ПО МФШ

Взаимодействие ПШ с ПО МФШ происходит при выполнении операций Внесения платежа в собственной платёжной инфраструктуре.

Должна быть реализована поддержка следующих операций:

- проверка правильности идентификационных реквизитов Плательщика, валидность реквизитов;
- учёт Платежа в Системе учета и контроля, подтверждение приёма платежа с суммой зачисления;
- поддержка механизма подключения, отключения, параметризации и проведения рекуррентных платежей (автоплатежей) с возможностью переключения между Банками эквайерами без необходимости перепривязки банковских карт;
- поддержка привязки и хранение HASH-PAN банковских карт, а также возможность оплаты по привязанным банковским картам без ввода дополнительной информации ввода CVV кода;
- поддержка механизма автоматизированных возвратов платежей.

В течение 1 (одного) рабочего дня со дня заключения договора Исполнитель обязан предоставить Заказчику описание открытых программных интерфейсов (API) для интеграции МФШ Заказчика с ПШ Исполнителя. Исполнитель обязан присоединиться к МФШ Заказчика посредством данного интерфейса (API). Исполнитель не позднее чем в течение 20 (двадцати) рабочих дней со дня заключения договора должен обеспечить поддержку и проведение мероприятий по внедрению и тестированию открытого программного интерфейса.

Состав тестовых мероприятий:

1. Подключение многофункционального шлюза Заказчика к ПШ Исполнителя и проверка корректности подключения.
3. Проверка корректности регистрации платежа в ПШ Исполнителя.
4. Проверка финансовой авторизации (ввода карточных данных).
5. Проверка вовлеченности карты в 3DSecure (SecureCode/двухфакторная аутентификация Пользователя).
6. Проверка корректности списания средств с карты клиента.
7. Проверка корректности получения статуса оплаты от ПШ Исполнителя. 8. Проверка корректности данных "Реестра переводов денежных средств";
9. Проверка корректности проведения рекуррентных платежей (автоплатежей).

1.1.4. Требования к взаимодействию с внутренними платёжными компонентами

Взаимодействие с внутренними платёжными компонентами предназначено для организации процесса приёма платежей с использованием банковских пластиковых карт (эквайринг, в том числе с использованием Сбер Pay, МТС Pay, Т-Pay, QR-кода) и СБП в собственной платёжной инфраструктуре Заказчика.

В течение 1 (одного) рабочего дня со дня заключения договора, Заказчик обязан предоставить Исполнителю описание открытых программных интерфейсов (API) для интеграции интернет-ресурсов Заказчика с ПШ Исполнителя. Исполнитель обязан присоединиться к платежным страницам интернет-ресурсов Заказчика посредством данного интерфейса (API). Исполнитель в течение 20 (двадцати) рабочих дней со дня заключения договора по согласованию с Заказчиком должен обеспечить поддержку и проведение мероприятий по внедрению и тестированию открытого программного интерфейса со стороны Заказчика для интеграции платежных страниц Заказчика с системами Исполнителя.

1.1.5. Требования к взаимодействию с ПЦ Банка

Взаимодействие с ПЦ Банка предназначено для организации приёма платежей с ПЦ Банков, выбранных Исполнителем для приема платежей, с использованием банковских пластиковых карт.

1.2. Требования к надёжности

1.2.1. Устойчивое функционирование должно быть обеспечено в режиме 24/7/365 (24 часа 7 дней в неделю 365 дней в году).

• 1.3. Требования к функциям, выполняемым Платежным шлюзом

1.3.1. Требования к функциям Модуля проведения операций с Плательщиком

Модуль проведения операций с Плательщиком должен обеспечивать выполнение функций:

- приём платежей с использованием банковских карт (эквайринг, в том числе с использованием Сбер Pay, МТС Pay, Т-Pay, QR-кода), систем мобильных платежей MIR Pay и иных платежных систем, действующих на рынке (через сеть Интернет и на ПВП в режиме онлайн и отложенного платежа);
- прием платежей через СБП (онлайн и на ПВП);
- прием платежей с использованием топливных карт.

1) Приём платежей с использованием банковских карт

ПШ при приёме платежей с использованием банковских карт должен обеспечивать выполнение операций:

- внесение Плательщиком денежных средств;
- возврат и частичный возврат Плательщикам карточных платежей;
- осуществление операций рекуррентных платежей (автоплатежей) с банковских карт при наступлении условий, определяемых Плательщиком по параметрам.

Для обеспечения функциональности внесения Плательщиком денежных средств Заказчику, Платёжный шлюз должен предоставлять возможность в том числе:

- проведение платежей с преавторизацией – платежей с предварительной проверкой возможности проведения операции;
- поддержка рекуррентных платежей – регулярных платежей, не требующих подтверждения, с возможностью продолжения использования оплат при подключении/отключении новых банков эквайеров без необходимости перепривязки карт;
- регистрация банковских карт для упрощения повторных платежей;
- вывод Плательщику по факту совершенной оплаты электронного и фискального чека с информацией о совершенном платеже. При необходимости, по соглашению с Заказчиком, Исполнитель обязан предоставить Заказчику возможность самостоятельной фискализации платежей через облачные кассы Заказчика в соответствии с требованиями Федерального закона № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении расчетов в Российской Федерации» от 22.05.2003г. (с изм.);
- возможность переключения между поставщиками ОФД без остановки сервиса фискализации платежей;
- уведомление Плательщика по факту совершенной оплаты письмом по электронной почте, содержащим информацию о совершенном платеже;
- взаимодействие с процессинговыми системами Банка-эквайера и третьего процессора для осуществления операций по банковским картам следующих платёжных систем:
 - МИР;
 - MasterCard;
 - Visa.
 - Union Pay

ПШ должен обеспечивать осуществление операций рекуррентных платежей (автоплатежей) с банковских карт при наступлении условий, определяемых Плательщиком по параметрам:

- сумма достижения заданного порога баланса Лицевого счета Плательщика;
- величина (сумма) рекуррентного платежа (автопополнения);
- выбранная зарегистрированная банковская карта.

Исполнитель обязан обеспечить возможность получения сохраненных у текущего банка-эквайера Заказчика банковских карт и параметров рекуррентных платежей (с соблюдением стандарта безопасности PCI DSS) и организовать проведение рекуррентных платежей по ним в соответствии с этими параметрами. Исполнитель обязан предоставить возможность функционирования рекуррентных платежей при смене банка эквайера без необходимости перепривязки иницирующей транзакции рекуррентного платежа.

Исполнитель обязан обеспечить возможность одновременной работы не менее двух банков эквайеров для обеспечения отказоустойчивости проведения платежей.

Исполнитель в течение 14 (четырнадцати) календарных дней со дня окончания срока действия договора по согласованию с Заказчиком обязан обеспечить возможность передачи сохраненных у Исполнителя или данных банковских карт (с соблюдением стандарта безопасности PCI DSS) и при необходимости, по требованию Заказчика, осуществить такую передачу.

Исполнитель обязан обеспечить возможность осуществления платежей Mir Pay посредством программного интерфейса (API).

1.3.2. Требования к функциям Модуля проведения расчётов с КО

Модуль проведения расчётов с кредитными организациями должен обеспечивать возможность выполнения операций: – осуществление взаиморасчётов с кредитными организациями;

- осуществление информационного сопровождения расчётов с кредитными организациями при осуществлении платёжных операций, в том числе:
 1. за операционный день;
 2. за отчётный период;

1.3.3. Требования к функциям Модуля Управления ПШ

Модуль Управления ПШ должен обеспечивать выполнение операций:

- отмена операций с использованием платёжных карт; – контроль статусов платежей.

Персонал Заказчика должен иметь доступ к ПШ посредством АРМ ПШ.

В составе Модуля Управления ПШ должны быть реализован доступ к следующим АРМам:

- Личный кабинет администратора ПШ;
- Личный кабинет администратора платежей.
- Личный кабинет плательщика

Работа во всех АРМ должна быть обеспечена на основе веб-интерфейсов и должна поддерживать следующие популярные браузеры: Mozilla Firefox, Opera, Google Chrome, Яндекс-Браузер (версии, поддерживаемые производителем).

1.3.3.1. Личный кабинет администратора ПШ

Личный кабинет администратора ПШ должен отвечать следующим требованиям:

- иметь систему разграничения прав доступа пользователей ЛК администратора платежа на выполняемые операции и элементы интерфейса ЛК администратора платежа, поддерживающую индивидуальную и групповую настройку прав;
- предоставлять администратору ПШ следующие функциональные возможности:
 1. подключение новых пользователей ЛК администратора платежа, их учёт и администрирование;
 2. создание и администрирование групп пользователей ЛК администратора платежа;
 3. управление индивидуальными и групповыми правами подключённых пользователей ЛК администратора платежа.

1.3.3.2. Личный кабинет администратора платежей

Личный кабинет администратора платежей должен предоставлять следующие функциональные возможности:

- мониторинг финансовых транзакций, осуществлённых через ПШ, в разрезе операций по карте и поиск в них по следующим критериям: наименование услуги, результат (успешность) операции, клиент, банк-эквайер, торговая точка, период операций, тип банковской карты, фрагмент номера банковской карты, дата окончания действия банковской карты, код авторизации оплаты, RRN финансовой транзакции (Retrieval Reference Number), идентификатор заказа на оплату, сумма операции;
- мониторинг финансовых операций, осуществлённых через систему, в разрезе заказов на оплату и поиск в них по следующим критериям: наименование услуги, результат (успешность) операции, плательщик, точка приема платежей, период операций, заказ на оплату;
- получение сводной финансовой отчётности по финансовым операциям;
- возможность выгрузки отчётов в Excel;
- инициирование операции отмены платежа (возврата средств) с помощью интерфейса ЛК.

1.3.3.3. Страница для Личного кабинета Плательщика

Страница платежа для Личного кабинета Плательщика должна предоставлять следующие функциональные возможности:

- отображение формы для ввода данных карты;
- проверка корректности ввода данных и повторный ввод некорректно введённых данных;
- отображение результатов попытки оплаты;
- вывод на экран электронного чека при успешной оплате (при наличии технической возможности).

Страница автоплатежа для Личного кабинета Плательщика должна предоставлять следующие функциональные возможности:

- регистрация карты для автоплатежа;
- настройка параметров автоплатежа по зарегистрированной карте.

Страницы для мобильных устройств должны быть на основе веб-интерфейсов и поддерживать популярные мобильные платформы, в том числе iOS и Android.

По согласованию с Заказчиком Сторонами могут быть использованы страницы платежа и автоплатежа Заказчика с аналогичной функциональностью.

• 1.4. Требования к отчётности

1.4.1. ПШ должен предоставлять возможность получения Заказчиком следующих отчётов:

- отчёт по финансовым транзакциям;
- отчёт по операциям банковскими картами.

Для всех отчётов должна быть реализована возможность выгрузить данные отчёта в Excel.

При выборе диапазона для построения отчёта, интервал между датой начала и датой окончания не должен превышать 12 месяцев.

1.4.1.1. Отчёт по финансовым транзакциям

Отчёт по финансовым транзакциям должен обладать следующими возможностями:

- выбор статуса финансовых транзакций для построения отчёта, в том числе должна быть возможность построить отчёт одновременно по всем статусам;
- выбор диапазона дат для построения отчёта;
- выбор диапазона сумм.

1.4.1.2. Отчёт по операциям банковскими картами

Отчёт по операциям банковскими картами должен обладать следующими возможностями:

- выбор типа операции (оплата, отмена, все);
- выбор статуса операции (успех, неудача, все);
- выбор эквайера (или по всем эквайерам);
- выбор диапазона дат для построения отчёта;
- выбор диапазона сумм.

• 1.5. Порядок проведения, обработки и отмены платежей с участием платежной страницы Заказчика и ПШ Исполнителя

Этапы проведения и обработки платежа банковской картой	
1	Держатель карты обращается на платежную страницу, размещенную на Интернет – ресурсе Заказчика, и формирует заказ на оплату товара, работы, услуги, подтверждая условия оформления заказа (наименование товара, работы, услуги, способ доставки, выбор средства оплаты через банковскую карту Сбер Pay, МТС Pay, Т-Pay QR-код или по СБП, сумма платежа, а также, в случае необходимости, параметры порогового рекуррентного платежа).
2	Платежная страница (сервис оплаты), используя данные заказа и функции открытого программного интерфейса (API) предоставленного Исполнителем, создает запрос в системе проведения электронных платежей Исполнителя на регистрацию платежа (в теле запроса передается описание платежа, сумма платежа, обратные адреса, на которые необходимо возвращать пользователя в случае успешного и в случае неуспешного платежа, и др.
3	В случае выбора пользователем платежа по СБП сервис оплаты отображает QR код для оплаты. Пользователь сканирует QR код, выбирает необходимый банк для оплаты, и подтверждает платеж в банковском приложении. Если выбран платеж с помощью карты Платежная страница осуществляет переадресацию пользователя на платежную страницу ПШ, на которой отображаются параметры платежа, также предлагается ввести реквизиты карты. Держатель карты выбирает тип карты, которой он будет расплачиваться и вводит информацию о параметрах своей карты: • тип карты; • номер карты; • дату окончания срока действия карты; • имя и фамилию, как указано на карте; • значения CVC2 или CVV2; • подтверждает, в случае необходимости, согласие на сохранение данных авторизации карты; • подтверждает свое согласие оплатить заказ вводом специального пароля, направленного Держателю в смс-сообщении. Специальный пароль представляет собой цифровую/буквенно-цифровую последовательность, однозначно идентифицирующую клиента как Держателя карты. Проверка специального пароля обеспечивается банком-эмитентом.

4	Исполнитель проверяет корректность формата вводимых параметров карты и осуществляет дополнительные процедуры аутентификации Держателя карты в соответствии с стандартом 3DSecure и передает запрос на авторизацию операции в Банк, выпустивший карту.
5	Исполнитель проверяет право Интернет – ресурса провести операцию и проводит авторизацию операций в установленном соответствующими международными платежными системами порядке.
6	При получении отрицательного результата уведомление об отказе отправляется в ПШ, который, в свою очередь, передает данную информацию на платежную страницу Интернет -ресурса и Держателю карты, с указанием причин отказа.
7	При получении положительного результата авторизации в ПШ передается подтверждение положительного результата авторизации операции. ПШ одновременно передает подтверждения положительного результата проводимой авторизации операции на платежной странице и Держателю карты.
8	После получения подтверждения о положительном результате авторизации платежная станция осуществляет регистрацию платежа в учетной системе Заказчика.
9	Обработка успешно авторизованных операций осуществляется автоматически не позднее следующего рабочего дня за днем совершения операции.
Этапы проведения и обработки платежа Mir Pay	
1	Плательщик обращается на платежную страницу, размещенную на Интернет – ресурсе Заказчика, и формирует заказ на оплату товара, работ, услуг, подтверждая условия оформления заказа (наименование товара, работы, услуги, способ доставки, выбор средства оплаты через Mir Pay, сумма платежа).
2	Платежная страница, используя данные заказа и функции открытого программного интерфейса (API) предоставленного Исполнителем, создает запрос в системе проведения электронных платежей Банка на регистрацию платежа.
3	Исполнитель проверяет возможность совершения платежа указанным способом и формирует токен платежа в соответствии с протоколом платежной системы.
4	Платежная страница, используя полученный токен, инициирует оплату на стороне устройства Плательщика.
5	Плательщик подтверждает свое согласие оплатить заказ с помощью встроенных средств аутентификации устройства.
6	Исполнитель проверяет корректность формата вводимых параметров, осуществляет дополнительные процедуры аутентификации и передает запрос на авторизацию операции в Банк.
7	Исполнитель проверяет право Интернет – ресурса провести операцию и проводит авторизацию операций в установленном соответствующими международными платежными системами порядке.
8	При получении отрицательного результата уведомление об отказе отправляется в ПШ, который, в свою очередь, передает данную информацию на платежную страницу Интернет -ресурса и Плательщику, с указанием причин отказа.
9	При получении положительного результата авторизации в ПШ передается подтверждение положительного результата авторизации операции. ПШ одновременно передает подтверждения положительного результата проводимой авторизации операции на платежной странице и Плательщику.
10	После получения подтверждения о положительном результате авторизации платежная станция осуществляет регистрацию платежа в учетной системе Заказчика.

11	Обработка успешно авторизованных операций осуществляется автоматически не позднее следующего рабочего дня за днем совершения операции.
Этапы автоматизированной отмены платежа	
1	Платежная страница, используя данные заказа и функции открытого программного интерфейса (API) предоставленного Исполнителем, создает запрос в системе проведения электронных платежей Исполнителя на отмену платежа. (Запрос может быть инициирован как до момента запуска Исполнителем процедуры закрытия дня, так и после запуска Исполнителем такой процедуры).
2	Исполнитель проверяет возможность возврата денежных средств и производит отмену банковской транзакции в ПШ.
3	Исполнитель передает результат выполнения заявки на отмену операции Платежной странице Заказчика.
Этапы ручной отмены платежа	
1	Для отмены операции после проведения Исполнителем процедуры закрытия дня необходимо заполнить заявку на отмену операции и предоставить ее Исполнителю.
2	В случае если Держатель карты отменяет операцию оплаты, Заказчик проверяет наличие данного заказа в своей учетной системе и оформляет заявку на отмену операции и предоставляет ее Исполнителю. Заявка должна быть подписана уполномоченным лицом и скреплена оттиском печати Заказчика.

