

УТВЕРЖДЕНЫ
Генеральным директором ООО «КП Ритейл»
Приказ № 24-ПС/21 от 31.08.2021 г.
Вступают в силу с 01.09.2021 г.

Правила платежной системы «КП Ритейл»

Редакция 5

Москва

2021

Оглавление

1. Введение	5
2. Термины и определения.....	5
3. Субъекты Системы и их функции.....	8
4. Права и обязанности Субъектов Системы	9
4.1. Обязанности Оператора	9
4.2. Права Оператора.....	10
4.3. Обязанности Участников	11
4.4. Права Участников.....	12
4.5. Обязанности Операционного центра	12
4.6. Права Операционного центра.....	12
4.7. Обязанности Платежного клирингового центра.....	12
4.8. Права Платежного клирингового центра	13
4.9. Обязанности Расчетного центра.....	13
4.10. Права Расчетного центра	14
5. Порядок привлечения ОУПИ, ведение перечня ОУПИ, требования к ОУПИ.....	14
5.1. Порядок привлечения ОУПИ, ведение перечня ОУПИ.....	14
5.2. Требования к Операторам услуг платежной инфраструктуры.....	15
6. Порядок взаимодействия между Субъектами Системы	16
6.1. Организация взаимодействия Субъектов Системы.....	16
6.2. Взаимодействие Оператора с Участниками.....	16
6.3. Критерии участия в Системе	17
6.4. Порядок присвоения идентификационного номера	18
6.5. Критерии и порядок приостановления и/или прекращения участия в Системе.....	18
6.6. Взаимодействие между Оператором и привлеченными ОУПИ.....	20
6.7. Взаимодействие между ОУПИ.....	21
6.8. Взаимодействие между ОУПИ и Участниками	21
6.9. Контроль соблюдения Правил, ответственность за их несоблюдение.....	22
6.10. Порядок предоставления Участниками и привлеченными Операторами услуг платежной инфраструктуры информации о своей деятельности Оператору.....	23
6.11. Порядок изменения Правил	24
6.12. Порядок взаимодействия в рамках Системы в чрезвычайных и спорных ситуациях.....	24
6.13. Порядок взаимодействия с платежными системами	26
6.14. Порядок досудебного разрешения споров между Субъектами Системы.....	26
6.15. Ответственность за несоблюдение Правил	29
7. Порядок осуществления платежного клиринга и расчетов.....	30
7.1. Общий порядок осуществления Операций в Системе и применяемые формы безналичных расчетов	30
7.2. Платежный клиринг	31
7.3. Расчеты	33
7.4. Временной регламент функционирования Системы.....	34
8. Порядок осуществления перевода денежных средств, включая моменты наступления безотзывности, безусловности и окончательности	36
8.1. Порядок осуществления перевода денежных средств	36
8.2. Эмиссия и обслуживание ЭСП.....	37
8.3. Моменты наступления безотзывности, безусловности и окончательности Перевода.....	38
8.4. Порядок сопровождения перевода денежных средств сведениями о Плательщике.....	38
8.5. Порядок оформления, формирования и отправки запроса на изменение реквизитов ранее отправленного Перевода	39
8.6. Отзыв, возврат (аннулирование) Переводов	40

9. Порядок оплаты услуг по переводу денежных средств и услуг платежной инфраструктуры, услуг Оператора.....	40
9.1. Порядок оплаты услуг	40
10. Управления рисками в Системе	42
10.1. Система управления рисками	42
10.2. Организационная модель управления рисками	43
10.3. Порядок обмена информацией, необходимой для управления рисками.....	44
10.4. Мероприятия по управлению рисками	45
10.5. Способы управления рисками	46
10.6. Виды рисков, присущих деятельности Системы	47
10.7. Методики анализа рисков в Системе	48
10.8. Порядок проведения оценки рисков и мониторинг рисков в Системе.....	50
10.9. Организационная структура системы управления рисками	50
10.10. Доведение до органов управления Оператора информации о рисках	53
11. Управление непрерывностью и порядок обеспечения бесперебойности функционирования Системы	53
11.1. Общие положения по обеспечению бесперебойности функционирования Системы.....	53
11.2. Управление непрерывностью и порядок осуществления деятельности по обеспечению бесперебойности	54
11.3. Показатели бесперебойности функционирования Системы	59
11.4. Требования к содержанию деятельности по обеспечению БФПС, осуществляемой Субъектами Системы	65
11.5. Порядок оценки качества функционирования операционных и технологических средств, информационных систем	67
11.6. Порядок изменения операционных и технологических средств и процедур.....	68
11.7. Порядок информационного взаимодействия Субъектов платежной системы и документационного обеспечения их деятельности по обеспечению БФПС.....	69
11.8. Обеспечение БФПС Субъектами Системы	70
11.9. Порядок и формы контроля соблюдения Участниками, привлеченными ОУПИ порядка обеспечения БФПС	72
11.10. Обязанности ОУПИ по обеспечению бесперебойности оказания услуг платежной инфраструктуры.....	73
11.11. Права и обязанности Оператора по обеспечению БФПС	73
11.12. Права и обязанности Участников по обеспечению БФПС	75
11.13. Права и обязанности привлеченных Операторов УПИ по обеспечению БФПС	75
12. Порядок информационного взаимодействия Субъектов Системы и документационного обеспечения их деятельности по обеспечению БФПС	76
12.1. Документы, используемых Субъектами Системы при осуществлении деятельности по обеспечению БФПС.....	76
12.2. Контроль за соблюдением операторами УПИ и участниками платежной системы порядка обеспечения БФПС	77
13. Обеспечение защиты информации в Системе	79
13.1. Общие правила осуществления защиты информации	79
13.2. Требования к обеспечению защиты информации	80
13.3. Порядок обеспечения защиты информации в Системе.....	81
13.4. Использование средств криптографической защиты информации	83
13.5. Требования к обеспечению защиты информации от воздействия вредоносного кода на инфраструктуру Системы	84
13.6. Обеспечение защиты персональных данных в Системе	85
13.7. Обеспечение банковской и коммерческой тайны в Системе	85
13.8. Порядок реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия Клиента Участника.....	85

13.9. Порядок информационного взаимодействия при выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	86
13.10. Порядок информационного взаимодействия для целей анализа обеспечения в Системе защиты информации.....	88
14. Приложения, являющиеся неотъемлемой частью Правил:	88
Приложение № 1 к Правилам. Тарифы	89
Приложение № 2 к Правилам. Регламент электронного документооборота	90

1. Введение

Платежная система «КП Ритейл» (далее – Система) представляет собой сообщество организаций (оператор платежной системы, операторы услуг платежной инфраструктуры, участники), объединенных единым информационным пространством и взаимодействующих в соответствии с настоящими Правилами в целях осуществления переводов денежных средств.

Полное официальное наименование платежной системы – Платежная система «КП Ритейл».

Сокращенное официальное наименование платежной системы – ПС «КП Ритейл».

Наименование на английском языке - Payment system «CP Retail».

Настоящие Правила Платежной системы «КП Ритейл» (далее – Правила) определяют порядок и условия участия в Системе, взаимодействия субъектов Системы, осуществления перевода денежных средств, использования электронных средств платежа при оказании услуг платежной инфраструктуры и иные положения, необходимые для функционирования Системы, определяемые оператором платежной системы, в том числе в соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее – Закон о НПС) и нормативными актами Банка России.

Правила разрабатывает и вводит в действие оператор платежной системы (далее – Оператор). Оператор вправе устанавливать требования к участникам и операторам услуг платежной инфраструктуры, к организации системы управления рисками и защиты информации в Системе, обеспечения бесперебойного функционирования в рамках Системы.

Правила, а также тарифы, являющиеся частью Правил, публикуются в открытом доступе на официальном сайте Оператора в информационно-телекоммуникационной сети «Интернет» по адресу: <https://cpetail.ru/>

2. Термины и определения

Для целей Правил используются следующие термины и определения:

Авторизация – разрешение, предоставляемое Участником–эмитентом Банковской карты на осуществление операций с использованием ЭСП.

Авторизационный запрос – запрос Плательщика на осуществление Авторизации.

Аннулирование перевода — отмена перевода, не выплаченного Получателю, производимая по инициативе Отправителя или Участника-отправителя.

Аутентификация – комплекс мер по проверке подлинности и принадлежности идентификационных данных Плательщику/Пользователю ЭСП.

Банковская карта – электронное средство платежа, эмитированное Участником для Плательщика, в том числе таможенная карта, карта в электронном виде, или её реквизиты, используемые для составления расчетных и иных документов к счету Плательщика, открытому у Участника, подлежащих оплате за счет Плательщика.

БФПС – бесперебойность функционирования Платежной системы «КП Ритейл».

Инцидент – событие, которое привело к нарушению оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, в том числе связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.

Комиссия за перевод – денежное вознаграждение субъектов Системы за осуществление Перевода, уплачиваемое Клиентом через Участника при осуществлении Перевода дополнительно к Сумме перевода.

Клиент – юридическое или физическое лицо, имеющее счет, открытый у Участника,

Конфигурация Участника – регистрация Участника в перечне Участников, заведение сведений об Участнике в базы данных ПК «КП РИТЕЙЛ», установление параметров Участника для целей оказания операционных услуг и услуг платежного клиринга, присвоение идентификационного кода.

Лимит по Банковской карте/ Лимит ЭСП – максимальная сумма Операций, которые могут быть совершены с использованием Банковской карты (ЭСП). Лимит по Банковской карте/ Лимит ЭСП устанавливается Участником по согласованию с Оператором на основании заявления Плательщика. Лимит по Банковской карте/ Лимит ЭСП может быть установлен, в том числе, на календарный день и/или календарный месяц.

Личный кабинет (ЛК) – интерфейс для информационного обмена между Оператором и другими Субъектами Системы. Доступ к ЛК организован на официальном сайте Оператора в информационно-телекоммуникационной сети «Интернет» с использованием индивидуального логина и пароля.

Оператор платежной системы (Оператор) – оператор Платежной системы «КП Ритейл» – Общество с ограниченной ответственностью «КП Ритейл», ОГРН 1137746774791, ИНН 7702821709, – определяющий правила Системы, а также выполняющий иные функции и обязанности, предусмотренные Правилами и законодательством Российской Федерации.

Оператор по переводу денежных средств - организация, которая в соответствии с законодательством Российской Федерации вправе осуществлять перевод денежных средств.

Операторы услуг платежной инфраструктуры (Операторы УПИ, ОУПИ) – операционные центры, платежные клиринговые центры и расчетные центры.

Операционный центр (ОЦ) – организация, обеспечивающая в рамках Системы для Участников и их клиентов доступ к услугам по переводу денежных средств, в том числе с использованием электронных средств платежа, а также обмен электронными сообщениями (далее - операционные услуги).

Операция - операция по переводу денежных средств или иная операция, в том числе совершенная посредством устройства приема платежей.

Официальный сайт Оператора в сети интернет – официальный сайт Оператора в информационно-телекоммуникационной сети «Интернет» (далее – сеть интернет), расположенный по адресу: <https://cpretail.ru/>.

Перевод денежных средств (Перевод) – действия Оператора по переводу денежных средств в рамках применяемых форм безналичных расчетов по предоставлению Получателю средств денежных средств Плательщика.

Платежный клиринговый центр (ПКЦ) – организация, созданная в соответствии с законодательством Российской Федерации, обеспечивающая в рамках Системы прием к исполнению распоряжений Участников об осуществлении перевода денежных средств и выполнение иных действий, предусмотренных настоящим Федеральным законом (далее - услуги платежного клиринга).

Плательщик (Отправитель) – физическое или юридическое лицо, клиент Участника, осуществляющее в рамках Системы операции для целей перевода денежных средств.

Получатель – юридическое лицо, для перевода денежных средств которому совершена операция по переводу денежных средств.

Пользователь ЭСП – Клиент-физическое лицо, а также уполномоченный представитель Клиента-юридического лица, имеющий доступ к ЭСП.

Предельный размер (лимит) обязательств Участника – установленная в соответствии с Правилами максимальная сумма денежных средств, которой может воспользоваться Участник для перевода денежных средств в рамках Системы, превышающий размер остатка денежных средств на Счете Участника в данный момент времени.

Программный комплекс «КП РИТЕЙЛ» (ПК «КП РИТЕЙЛ») – интеграционная технологическая платформа, включая программное обеспечение Системы (клиентский WEB-интерфейс), обеспечивающее взаимодействие с Системой, доступ Участников к Системе.

Пункт обслуживания - подразделения Участников, осуществляющие обслуживание Клиентов.

Расчетный центр (РЦ) – кредитная организация, созданная в соответствии с законодательством Российской Федерации, заключившая договор с Оператором на осуществление функций расчетного центра, предусмотренных Правилами, и удовлетворяющая требованиям, предъявляемым к ней Правилами.

Реестр ПКЦ - формируемый Оператором, выполняющим функции Платежного клирингового центра и направляемый Участнику документ в электронной форме, содержащий информацию по принятым к исполнению распоряжениям на проведение Операций, а также корректирующим операциям и возвратам платежей, операциям оплаты комиссий и штрафов и прочим переводам денежных средств.

Реестр распоряжений – составляемые Оператором, выполняющим функции Платежного клирингового центра, и направляемые в Расчетный центр реестры в виде электронных сообщений, включающие платежные клиринговые позиции Участников, определенные Оператором, выполняющим функции Платежного клирингового центра, а также комиссии, рассчитанные в соответствии с Тарифами.

Реестр Участника – формируемый Участником и направляемый в Платежный клиринговый центр документ в электронной форме, содержащий информацию по установленным Лимитам по Банковским картам, эмитированным Участником, Переводам, а также корректирующим операциям и возвратам платежей.

Согласованный канал связи – средства и способы, определенные Оператором, Участником и/или привлеченным ОУПИ для информационного обмена и расчетов, указанный в заключенных между ними договорах и/или Правилах.

Субъекты Системы – Оператор, Операторы услуг платежной инфраструктуры и Участники.

Счет Участника – банковский счет Участника, открытый в Расчетном центре, используемый для перевода денежных средств и/или расчетов в рамках Системы.

Тарифы – Система ставок и размеров вознаграждения, установленная Оператором. (Приложение № 1 к Правилам). Тарифы подлежат опубликованию на Официальном сайте Оператора в сети интернет.

Требования к оказанию услуг – требования, применяемые к Оператору при обеспечении бесперебойности функционирования Системы, которая достигается при условии оказания Участникам услуг платежной инфраструктуры согласно требованиям Закона о НПС и принятых в соответствии с ним нормативных актов Банка России, а также положениям Правил, договоров об оказании услуг платежной инфраструктуры, документов Оператора и привлеченных им Операторов услуг платежной инфраструктуры.

Управление непрерывностью функционирования Системы – выявление оказания услуг платежной инфраструктуры, не соответствующих требованиям к оказанию услуг, обеспечению функционирования Системы в случае нарушения оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, и восстановлению оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, включая восстановление оказания услуг платежной инфраструктуры в случае

приостановления их оказания в течение периодов времени, установленных Оператором в Правилах.

Управление рисками в Системе – осуществление деятельности по организации системы управления рисками в Системе, оценке и управлению рисками в Системе.

Услуги Системы - осуществление перевода денежных средств, в том числе с использованием Электронных средств платежа в рамках Системы.

Устройство приема платежей – программное и/или аппаратно-программное устройство, осуществляющее информационное взаимодействие с Операционным центром и предназначенное для совершения Операций с использованием Электронных средств платежа, без возможности приема (выдачи) наличных денежных средств (далее - электронные терминалы), а также платежные терминалы и банкоматы.

Участники – Операторы по переводу денежных средств, иностранные кредитные организации, присоединившиеся к Правилам платежной системы, в целях оказания услуг по переводу денежных средств.

Участник-исполнитель – Участник, осуществляющий зачисление денежных средств Получателю.

Участник-отправитель – Участник, принимающий от Отправителя/Плательщика распоряжение, обслуживающий банковский счет Отправителя/Плательщика и/или принимающий денежные средства на осуществление Перевода.

Электронное средство платежа (ЭСП) - средство и (или) способ, позволяющие клиенту Оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

Настоящие термины имеют то же значение при использовании их во множественном числе и написании строчными буквами. Иные термины, предусмотренные настоящими Правилами, применяются в значениях, установленных Законом о НПС, иными законодательными актами Российской Федерации, нормативными актами Банка России и настоящими Правилами.

3. Субъекты Системы и их функции

Функции Оператора Платежной системы (Оператор): определение Правил Системы, а также выполнение иных обязанностей, предусмотренных Законом о НПС, в том числе привлечение Участников, Операторов услуг платежной инфраструктуры, контроль соблюдения Правил Системы Участниками, Операторами услуг платежной инфраструктуры.

Функции Операционного центра (ОЦ): обеспечение в рамках Системы Участникам, их клиентам доступа к Услугам по переводу денежных средств, Системы, в т.ч. с использованием Электронных средств платежа, а также обмен электронными сообщениями.

Функции Платежного клирингового центра (ПКЦ): обеспечение в рамках Системы приема к исполнению распоряжений Участников об осуществлении перевода денежных средств и выполнении иных действий, предусмотренных Законом о НПС, в т.ч. дальнейшей передачи подлежащих исполнению распоряжений Расчетному центру для осуществления его функций.

Функции Расчетного центра (РЦ): обеспечение в рамках Системы исполнения поступивших от ПКЦ распоряжений Участников посредством списания и зачисления

денежных средств по банковским счетам Участников, направление подтверждений, касающихся исполнения распоряжений Участников (далее – расчетные услуги).

В Системе действует единственный расчетный центр.

Функции Участников – предоставление Услуг Системы Клиентам.

Субъекты Системы при оказании платежных услуг в рамках Системы обязаны руководствоваться Правилами, а в части, не урегулированной Правилами, действующим законодательством Российской Федерации, нормативными правовыми актами Банка России, иными ведомственными нормативными правовыми актами.

Оператор выполняет функции Операционного и Платежного клирингового центра Системы. Полный перечень Операторов УПИ доступен для ознакомления на Официальном сайте Оператора в сети интернет.

4. Права и обязанности Субъектов Системы

4.1. Обязанности Оператора

4.1.1. Создать единую концептуальную основу взаимодействий в Системе и обеспечивать организационную и технологическую целостность Системы, а также равноправный доступ Операторов услуг платежной инфраструктуры и Участников в Систему.

4.1.2. Определять Правила Системы, организовывать и осуществлять контроль за их соблюдением Участниками и Операторами услуг платежной инфраструктуры.

4.1.3. Осуществлять привлечение Операторов услуг платежной инфраструктуры (за исключением случаев, когда Оператор совмещает функции Оператора с функциями Оператора услуг платежной инфраструктуры), которые находятся на территории Российской Федерации и соответствуют требованиям, установленным законодательством Российской Федерации и Правилами, обеспечивать контроль оказания услуг платежной инфраструктуры, вести перечень Операторов услуг платежной инфраструктуры (при их привлечении).

4.1.4. Устанавливать требования к Операторам услуг платежной инфраструктуры, с которыми могут заключаться договоры при их привлечении Оператором, в т.ч. в части их финансового состояния, технологического обеспечения.

4.1.5. При наличии в Системе двух и более расчетных центров обеспечивать взаимозаменяемость Расчетных центров и (или) возможность для Участников Системы осуществить переход в течение не более 20 (двадцати) рабочих дней на обслуживание к другому (резервному) Расчетному центру, в случае нарушения обслуживающим их Расчетным центром требований к БФПС, в том числе приостановления (прекращения) оказания услуг платежной инфраструктуры.

4.1.6. Организовать систему управления рисками в Системе, осуществлять мониторинг, анализ, оценку и управление рисками в Системе в соответствии с требованиями законодательства Российской Федерации, нормативных актов Банка России и Правил.

4.1.7. Обеспечить прием и обработку обращений Участников платежной системы по вопросам бесперебойности работы платежной системы.

4.1.8. Обеспечить возможность досудебного рассмотрения споров с Участниками и Операторами услуг платежной инфраструктуры в соответствии с Правилами.

4.1.9. Обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, в соответствии с требованиями к защите указанной информации, установленными Правительством Российской Федерации.

4.1.10. Обеспечивать защиту информации при осуществлении переводов денежных средств в соответствии с требованиями, установленными законодательством Российской Федерации, Правительством Российской Федерации и Банком России.

4.1.11. Гарантировать банковскую и коммерческую тайну в соответствии с законодательством Российской Федерации о банках и банковской деятельности.

4.1.12. Обеспечивать бесперебойность оказания услуг платежной инфраструктуры Участникам и управление непрерывностью функционирования Системы.

4.1.13. Организовывать взаимодействие Оператора, привлеченных Операторов УПИ и Участников Системы по обеспечению БФПС и контроль за соблюдением Операторами УПИ и Участниками Системы порядка обеспечения БФПС.

4.1.14. Обеспечивать, в случае выполнения функций операционного центра Системы, обмен электронными сообщениями, в случаях, когда такой обмен предусмотрен Правилами, между Субъектами Системы. Оператор может осуществлять иные действия, связанные с использованием информационно-коммуникационных технологий, необходимые для функционирования Системы и предусмотренные Правилами.

4.1.15. Нести ответственность, в случае выполнения функций Оператора услуг платежной инфраструктуры, за реальный ущерб, причиненный Участникам вследствие неоказания (ненадлежащего оказания) услуг платежной инфраструктуры (за исключением услуг расчетного центра), при этом ответственность Оператора за реальный ущерб ограничена размером неустойки, за исключением случаев умышленного неоказания (ненадлежащего оказания) услуг платежной инфраструктуры (за исключением услуг расчетного центра). Размер неустойки определяется как наименьшая из величин:

- размер реального ущерба, причиненного Участнику,
- размер вознаграждения, подлежащего уплате Участником Оператору, за оказание услуг Оператором за календарный месяц, в котором причинен ущерб Участнику.

4.1.16. Соблюдать требования, предусмотренные законодательством Российской Федерации к указанному виду деятельности, в течение всего времени осуществления деятельности Оператора.

4.1.17. Информировать Участников о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры в день такого приостановления (прекращения) любым из указанных ниже способов:

- размещение информации на Официальном сайте Оператора в сети интернет;
- размещение информации в Личных кабинетах Участников;
- направление уведомления по согласованным каналам связи.

4.2. Права Оператора

4.2.1. В одностороннем порядке вносить изменения в Правила с соблюдением условий, установленных Законом о НПС, в порядке, определенном в Правилах.

4.2.2. Заключать договоры о взаимодействии с другими платежными системами при условии отражения порядка такого взаимодействия в Правилах путем внесения соответствующих изменений в порядке, определенном Законом о НПС и настоящими Правилами.

4.2.3. Совмещать свою деятельность с деятельностью Оператора услуг платежной инфраструктуры (за исключением Расчетного центра) и с иной деятельностью, если это не противоречит законодательству Российской Федерации.

4.2.4. Размещать в публичном доступе перечень Участников Системы.

4.2.5. Приостанавливать и прекращать участие в Системе в порядке и по основаниям, установленным настоящими Правилами.

4.2.6. Уведомлять Участников Системы о необходимости смены Расчетного центра в более сокращенные сроки, чем установлены в Правилах, в случае наличия объективной информации о наличии риска невыполнения Расчетным центром своих обязательств по бесперебойности функционирования.

4.2.7. Устанавливать, изменять Предельные размеры (лимиты) обязательств Участников Системы и Лимиты ЭСП.

4.2.8. Организовывать продвижение Услуг Системы.

4.2.9. Вводить дополнительную плату за выполнение функций, не связанных с выполнением функций Оператора и Оператора УПИ Системы.

4.2.10. Устанавливать обменный курс, применяемый при осуществлении расчетов в Системе. Курс фиксируется в ПК «КП РИТЕЙЛ», доводится до сведения Клиентов и Участников до момента инициирования соответствующей Операции.

4.2.11. Запрашивать у Участников и привлеченных Операторов УПИ, разработанные ими документы по обеспечению БФПС в пределах выполняемого функционала в целях управления рисками и управления непрерывностью функционирования Системы.

4.3. Обязанности Участников

4.3.1. Соблюдать Правила Системы.

4.3.2. Соблюдать порядок обеспечения БФПС в рамках выполняемого функционала.

4.3.3. Открыть счет в Расчетном центре Системы. Контролировать достаточность денежных средств на счете в Расчетном центре для бесперебойности расчетов и выполнения своих обязательств.

4.3.4. Предоставлять услуги по переводу денежных средств в строгом соответствии с требованиями законодательства Российской Федерации и Правилами.

4.3.5. Своевременно направлять Оператору Реестр Участника.

4.3.6. Обеспечивать своевременную оплату Операций, в том числе совершенных с использованием эмитированных/предоставленных им Электронных средств платежа, в рамках Лимитов ЭСП, установленных в соответствии с Правилами. Участник несет финансовую ответственность перед Оператором за несвоевременную оплату данных операций и обязуется возместить убытки, понесенные Оператором в случае неосуществления в срок, определенный Правилами и/или Договором участия в Системе действий, предусмотренных Правилами и/или Договором участия в Системе, для оплаты совершенных операций.

4.3.7. Обеспечивать техническое взаимодействие с Субъектами Системы, необходимое для бесперебойного оказания Услуг Системы.

4.3.8. Оплачивать услуги, предоставляемые Оператором и привлеченными Операторами услуг платежной инфраструктуры в сроки и в порядке, определенные Правилами, договорами, заключенными в рамках Системы.

4.3.9. Незамедлительно информировать Оператора о любых обстоятельствах, которые могут повлиять на исполнение Участником своих обязательств.

4.3.10. Сообщать Оператору о всех инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, инцидентах безопасности.

4.3.11. Обеспечить получение согласия на обработку (включая автоматизированную обработку) данных физических лиц (Отправителей и Получателей переводов денежных средств) всеми Субъектами Системы, участвующими в обработке данных.

4.3.12. Выполнять требования по обеспечению информационной безопасности в Платежной системе в соответствии с Правилами и действующим законодательством Российской Федерации.

4.3.13. Самостоятельно нести ответственность за соблюдение требований применимого законодательства, в т.ч. валютного законодательства, законодательства о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма, о защите персональных данных.

4.3.14. Гарантировать банковскую и коммерческую тайну в соответствии с законодательством Российской Федерации о банках и банковской деятельности.

4.3.15. Обеспечивать защиту информации при осуществлении переводов денежных средств, в т.ч. в соответствии с требованиями, установленными Банком России.

4.3.16. Обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации.

4.3.17. Направлять по запросу Оператора (поступившему в том числе с почтового ящика ответственного подразделения Оператора) копии, а при необходимости - оригиналы или должным образом заверенные копии документов, подтверждающих осуществление Клиентами операций в Системе и/или согласие клиентов на обработку их персональных данных Участниками и Оператором, а также связываться с Отправителем/Получателем Перевода для получения дополнительной информации и/или копии удостоверяющего личность Отправителя документа при получении соответствующего запроса от Оператора.

4.3.18. Предоставлять по требованию Оператора внутренние документы по обеспечению БФПС на контроль Оператору Системы.

4.3.19. Выполнять другие обязательства в соответствии с настоящими Правилами.

4.3.20. Разрабатывать внутренние документы по обеспечению БФПС в пределах выполняемого функционала в целях управления рисками и управления непрерывностью функционирования Системы.

4.4. Права Участников

4.4.1. Участвовать в других платежных системах.

4.4.2. Привлекать третьих лиц в целях предоставления Услуг Системы в соответствии с законодательством страны своего месторасположения, в т.ч. банковских платежных агентов (далее – БПА) в соответствии с законодательством Российской Федерации. При этом Участник несет ответственность перед Субъектами Системы за действия указанных третьих лиц.

4.4.3. Полностью или частично приостановить участие в Системе.

4.5. Обязанности Операционного центра

4.5.1. Обеспечивать регистрацию Участников в Системе и доступ к Услугам Системы.

4.5.2. Обеспечивать обмен электронными сообщениями.

4.5.3. Обеспечивать защиту обрабатываемой в соответствии с выполняемыми функциями Операционного центра информации.

4.5.4. Гарантировать банковскую и коммерческую тайну в соответствии с законодательством Российской Федерации о банках и банковской деятельности.

4.5.5. Не раскрывать третьим лицам сведения об операциях и о Счетах Участников и их клиентов, полученные при оказании операционных услуг, за исключением передачи информации в рамках Системы, а также случаев, предусмотренных федеральными законами.

4.5.6. Информировать Субъектов Системы об изменении технических условий функционирования Системы.

4.5.7. Соблюдать порядок обеспечения БФПС в рамках выполняемого функционала.

4.5.8. Выполнять иные обязательства в соответствии с настоящими Правилами.

4.6. Права Операционного центра

4.6.1. Определять и вносить изменения в технические условия подключения и функционирования Системы.

4.7. Обязанности Платежного клирингового центра

4.7.1. Выполнять процедуры приема к исполнению платежных распоряжений, переданных Участниками, включая проверку соответствия платежных распоряжений установленным требованиям.

4.7.2. Определять достаточность денежных средств для исполнения распоряжений Участников.

4.7.3. Определять платежные клиринговые позиции Участников на нетто-основе.

4.7.4. Направлять Участнику Реестры ПКЦ, а также извещения, относящиеся к исполнению распоряжений Участников в сроки и в порядке, определенные Правилами.

4.7.5. Передавать Расчетному центру от имени Участников подлежащие исполнению распоряжения Участников.

4.7.6. Гарантировать банковскую и коммерческую тайну в соответствии с законодательством Российской Федерации о банках и банковской деятельности.

4.7.7. Не раскрывать третьим лицам сведения об операциях и о Счетах Участников и их клиентов, полученные при оказании услуг платежного клиринга, за исключением передачи информации в рамках Системы, а также случаев, предусмотренных федеральными законами.

4.7.8. Соблюдать порядок обеспечения БФПС в рамках выполняемого функционала.

4.7.9. Выполнять иные обязательства в соответствии с настоящими Правилами.

4.8. Права Платежного клирингового центра

4.8.1. Отказать в приеме платежного распоряжения Участника в случае, если платежное распоряжение не прошло проверку на соответствие установленным требованиям, определенным Правилами и законодательством Российской Федерации.

4.9. Обязанности Расчетного центра

4.9.1. Уведомлять Оператора об открытии/закрытии Счетов Участников в течение трех рабочих дней с момента их открытия/закрытия.

4.9.2. Не изменять без согласования с Оператором положения, определяющие порядок, условия и сроки предоставления расчетных услуг в рамках Системы.

4.9.3. Уведомлять Оператора, а также Участников о намерении изменения тарифов предоставления услуг по ведению банковского счета, не менее чем за 15 (пятнадцать) календарных дней до даты вступления в силу таких изменений.

4.9.4. Обеспечивать в рамках Системы своевременное и полное исполнение Реестра распоряжений, полученного от Оператора, выполняющего функции Платежного клирингового центра, распоряжений Участников посредством списания и зачисления денежных средств по Счетам Участников.

4.9.5. Обеспечивать направление Оператору, выполняющему функции Платежного клирингового центра, подтверждений, касающихся исполнения его Реестра распоряжений.

4.9.6. Передавать Оператору, выполняющему функции Платежного клирингового центра, сведения об остатках на Счетах Участников и проведенных по Счетам Участников платежах, связанных с осуществлением расчетов по операциям, совершенным в рамках Системы, в сроки, определенные договором между Оператором, выполняющим функции Платежного клирингового центра и Расчетным центром.

4.9.7. Обеспечивать бесперебойность оказания расчетных услуг, самостоятельно организовывать управление рисками, присущими деятельности Расчетного центра – кредитной организации.

4.9.8. Соответствовать требованиям финансовой устойчивости, установленным Банком России.

4.9.9. Обеспечить выполнение требований законодательства Российской Федерации, нормативных актов Правительства Российской Федерации и Банка России в части обеспечения защиты информации в собственных информационных системах, а также при взаимодействии с субъектами платежной системы.

4.9.10. Самостоятельно нести ответственность за соблюдение требований применимого законодательства, в т.ч. валютного законодательства, законодательства о

противодействию легализации доходов, полученных преступным путем, и финансированию терроризма, о защите персональных данных.

4.9.11. При фиксации в течение календарного года 2 (двух) и более событий оказания Расчетным центром услуг платежной инфраструктуры, не соответствующих требованиям к оказанию услуг по причине ненадлежащего функционирования операционных и технологических средств и информационных систем, для проведения оценки качества функционирования операционных и технологических средств и информационных систем Расчетного центра по требованию Оператора следует привлечь независимую экспертную организацию. Привлекаемая сторонняя независимая экспертная организация должна соответствовать требованиям, иметь лицензии (разрешения), необходимые для осуществления соответствующей деятельности (в случае, если такие требования, лицензии (разрешения) предусмотрены законодательством Российской Федерации). Оценка качества функционирования операционных и технологических средств, информационных систем осуществляется сторонней независимой экспертной организацией в соответствии со стандартами и правилами привлекаемой организации, стандартами и правилами, установленными законодательством Российской Федерации (при их наличии), в сроки, согласованные с Оператором и обеспечивающие качественное выполнение поставленной задачи. Результаты оценки, проведенной независимой экспертной организацией качества функционирования операционных и технологических средств и информационных систем Расчетного центра предоставляются Оператору.

4.9.12. Соблюдать порядок обеспечения БФПС в рамках выполняемого функционала.

4.9.13. Незамедлительно информировать Оператора о всех событиях, которые привели к нарушению оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, в том числе об инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, а также инцидентах безопасности в порядке, установленном в пп. 6.12.1 Правил.

4.9.14. Предоставлять по запросу Оператора внутренние документы по обеспечению БФПС.

4.9.15. Выполнять иные обязательства в соответствии с настоящими Правилами.

4.10. Права Расчетного центра

4.10.1. Совмещать свою деятельность с деятельностью Участника.

4.10.2. Самостоятельно определять и контролировать условия, порядок открытия и ведения Счетов Участников, учитывая положения Правил.

4.10.3. Вводить плату за предоставление услуг по ведению банковского счета.

4.10.4. Самостоятельно разрабатывать внутренние документы по обеспечению БФПС в пределах выполняемого функционала в целях управления рисками и управления непрерывностью функционирования Системы.

5. Порядок привлечения ОУПИ, ведение перечня ОУПИ, требования к ОУПИ

5.1. Порядок привлечения ОУПИ, ведение перечня ОУПИ

5.1.1. В Системе Оператор совмещает свою деятельность с деятельностью Операторов услуг платежной инфраструктуры, за исключением деятельности Расчетного центра.

5.1.2. Оператор, в т.ч. с целью обеспечения бесперебойности функционирования Системы, принимает решение о необходимости привлечения ОУПИ, об объеме выполняемых ими функциях.

5.1.3. Привлечение ОУПИ осуществляется Оператором на основании договора, заключаемого между Оператором и Оператором услуг платежной инфраструктуры.

5.1.4. Привлечение осуществляется на условиях обеспечения равноправного доступа ОУПИ в Систему и отсутствия условия об исключительном оказании услуг платежной инфраструктуры.

5.1.5. Ведение перечня ОУПИ осуществляется Оператором самостоятельно путем включения в него информации об Операторе услуг платежной инфраструктуры с указанием его типа.

5.1.6. Оператор поддерживает перечень ОУПИ в актуальном состоянии и публикует перечень на Официальном сайте Оператора в сети интернет.

5.2. Требования к Операторам услуг платежной инфраструктуры

5.2.1. Требования к Расчетному центру:

- Расчетным центром платежной системы может выступать кредитная организация, созданная в соответствии с законодательством Российской Федерации, в том числе небанковская кредитная организация.
- Кредитная организация не менее 1 (одного) года осуществляет перевод денежных средств по открытым в этой кредитной организации банковским счетам.
- Финансовая устойчивость (размер уставного капитала не ниже, установленного законодательством Российской Федерации).
- Расчетный центр выполняет обязательные требования Банка России, в том числе требования по обеспечению мер по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.
- Расчетный центр обеспечивает банковскую тайну, защиту информации при осуществлении переводов денежных средств и персональных данных Плательщиков (в случае их получения и обработки) в соответствии с законодательством Российской Федерации.

5.2.2. Требования к Операционному центру.

- Оператор самостоятельно осуществляет функции Операционного центра и не привлекает сторонние организации в качестве Операционных центров, за исключением случаев, указанных в пп. 11.4.3 Правил.
- Оператор обязан соответствовать требованиям, предъявляемым действующим законодательством Российской Федерации к организациям, осуществляющим деятельность в качестве операционного центра.

5.2.3. Требования к Платежному клиринговому центру.

- Оператор самостоятельно осуществляет функции Платежного клирингового центра и не привлекает сторонние организации в качестве Платежных клиринговых центров, за исключением случаев, указанных в пп. 11.4.3 Правил.
- Оператор обязан соответствовать требованиям, предъявляемым действующим законодательством Российской Федерации к организациям, осуществляющим деятельность в качестве платежного клирингового центра.
- Оператор, оказывая услуги платежного клиринга, обязуется передавать Расчетному центру от имени Участников подлежащие исполнению распоряжения Участников.

5.2.4. Операторы услуг платежной инфраструктуры не вправе в одностороннем порядке приостанавливать (прекращать) оказание услуг платежной инфраструктуры Участникам Системы.

5.2.5. Оператор в отношении привлеченных ОУПИ самостоятельно, в том числе используя общедоступную информацию, а также при необходимости запрашивая от привлеченных ОУПИ дополнительную информацию о текущей деятельности, осуществляет мониторинг деятельности привлеченных ОУПИ на соответствия требованиям, перечисленным в пп.5.2.1-5.2.3 Правил. Мониторинг деятельности привлеченных ОУПИ осуществляет

структурное подразделение (работник) Оператора, ответственное за управление рисками, присущими деятельности Системы. Результаты мониторинга ежегодно оформляются в виде отчета и направляются не позднее последнего числа первого месяца года, следующего за отчетным, на рассмотрение единоличному исполнительному органу Оператора.

6. Порядок взаимодействия между Субъектами Системы

6.1. Организация взаимодействия Субъектов Системы

6.1.1. Операции по переводу денежных средств в Системе совершаются Плательщиками, в том числе, с использованием устройств приема платежей. Для проведения перевода денежных средств в Системе могут использоваться Электронные средства платежа.

6.1.2. Участники вправе осуществлять эмиссию Электронных средств платежа в порядке и на условиях, предусмотренных Правилами и договором, заключаемым с Оператором с соблюдением законодательства Российской Федерации.

6.1.3. Расчеты по переводам денежных средств в Системе осуществляются через Счета Участников.

6.2. Взаимодействие Оператора с Участниками

6.2.1. Взаимодействие Оператора с Участниками осуществляется на основании Правил и договора участия в Системе. Договор участия может быть подписан Оператором и Участником, может быть направлен в форме публичной оферты или оферты, адресованной конкретному юридическому лицу.

6.2.2. Взаимодействие между Оператором и Участником осуществляется с момента выражения намерения юридического лица присоединиться к Системе в качестве Участника, и в дальнейшем в процессе осуществления им функций Участника вплоть до момента прекращения участия в Системе.

6.2.3. Юридическое лицо, отвечающее требованиям, установленным Правилами для Участника, информирует Оператора в письменной или устной форме о своем намерении присоединиться к Системе. Оператор направляет на рассмотрение юридическому лицу Правила и договор, содержащий в том числе положения о присоединении к Правилам, иные условия, согласование которых предусмотрено в договоре (далее – Договор участия).

6.2.4. После подписания Договора участия Оператор в срок, не превышающий две недели, осуществляет конфигурацию Участника в Системе.

6.2.5. Оператор, в соответствии с Правилами:

- вправе инициировать предложение об участии в Системе;
- принимает решение о соответствии юридического лица критериям участия в Системе;
- контролирует выполнение Правил и условий договора участия Участником;
- предпринимает меры воздействия к Участникам, нарушившим Правила;
- принимает решение о приостановлении, прекращении участия в Системе Участника;
- принимает обращения Участника, касающиеся вопросов функционирования Системы;
- принимает обращения Участника о приостановлении или прекращении участия в Системе.

6.2.6. Для обеспечения взаимодействия Оператор и Участники используют следующие Согласованные каналы связи:

- Официальный сайт Оператора в сети интернет.
- Личный кабинет Участника.

- Адреса электронной почты Оператора, принадлежащие домену @cpretail.ru, или доведенные до привлеченных ОУПИ уполномоченными должностными лицами Оператора. Информационные рассылки, осуществляемые с таких адресов, являются официальными сообщениями Оператора.
- Обмен сообщениями на бумажных носителях, направляемых сторонами друг другу с привлечением организаций почтовой связи, компаний экспресс-доставки документов, курьеров, а также осуществляемый уполномоченными представителями сторон.
- Электронный адрес Участника:
 - указанный в Договоре участия;
 - указанный в Личном кабинете Участника;
 - указанный в официальном сообщении Участника, направленном Оператору на бумажном носителе или отправленном на электронный адрес Оператора.

6.2.7. В целях минимизации финансовых рисков в Системе Оператор вправе устанавливать Предельные размеры (лимиты) обязательств Участника с учетом уровня риска.

При установлении Предельного размера (лимита) обязательств Участника, Оператор направляет Участнику по согласованному каналу связи уведомление в срок не позднее рабочего дня, следующего за днем установления такого Предельного размера (лимита) обязательств Участника.

Предельный размер (лимит) обязательств Участника устанавливается в соответствии с внутренними процедурами Оператора на основании комплексной оценки Участника и анализа его финансовой устойчивости с учетом рейтинга кредитоспособности по классификации рейтинговых агентств, а также, в случае принятия Оператором соответствующего решения, с учетом предоставленных Участником всех видов обеспечения для надлежащего исполнения его обязательств в рамках Системы, согласованных с Оператором.

Оператор осуществляет постоянный мониторинг Операций по Банковским картам, эмитированным Участником, в сети Устройств приема платежей других Участников и Операций с использованием Банковских карт других Участников в сети Устройств приема платежей Участника с тем, чтобы объем финансовых обязательств Участника не превышал Предельный размер (лимит) обязательств Участника, установленный Оператором данному Участнику.

Оператор блокирует осуществление Операций с использованием Банковских карт, эмитированных Участником, в сети Устройств приема платежей Участника и других Участников, в случае, если объем финансовых обязательств Участника превысит Предельный размер (лимит) обязательств Участника.

6.3. Критерии участия в Системе

6.3.1. Взаимодействие в рамках Системы возможно только при условии присоединения Участника к Правилам. Участник может присоединиться к Системе при соответствии следующим критериям:

- финансовая устойчивость юридического лица;
- наличие действующей лицензии на осуществление банковских операций или иного разрешения, необходимого для осуществления переводов денежных средств в соответствии с законодательством страны своей юрисдикции;
- организация не находится в стадии ликвидации, банкротства;
- наличие технической возможности интеграции в Систему.

6.3.2. Участник считается присоединившимся к Системе после подписания с Оператором Договора участия. Присоединение к Системе является бесплатным для Участника.

6.3.3. Соответствие критериям, указанным в абзаце 4 подпункта 6.3.1 Правил, проверяется в процессе открытия Счета Участника в Расчетном центре.

6.3.4. Подписывая Договор участия, Участник гарантирует выполнением им мер по защите информации, соблюдение требований применимого законодательства.

6.3.5. Датой начала участия в Системе в целях уведомления об этом уполномоченного органа является дата заключения Договора участия в Системе.

6.3.6. Оператор устанавливает виды участия в Системе:

- прямое участие, предусматривающее обязательное открытие счетов в Расчетном центре.

6.3.7. Присоединяясь к Правилам, Участник принимает их в целом без каких-либо изъятий и исключений.

6.4. Порядок присвоения идентификационного номера

6.4.1. Участнику присваивается идентификационный цифровой, буквенный или буквенно-цифровой номер – четырехразрядный код, позволяющий однозначно идентифицировать Участника.

6.4.2. Идентификационный код присваивается Операционным центром автоматически в процессе конфигурации Участника.

6.5. Критерии и порядок приостановления и/или прекращения участия в Системе

6.5.1. Критериями приостановления и/или прекращения участия в Системе являются:

- случаи несоблюдения Участником своих обязательств, установленных Правилами;
- зафиксированные случаи утраты соответствия критериям участия;
- случаи приостановления государственным органом операций Участника, включая отзыв лицензии, или наложения ареста на денежные средства Участника, находящиеся на счете в Расчетном центре;
- случаи, когда любые компетентные органы власти приостанавливают или отменяют полномочия Участника или выпускают уведомление о своем намерении поступить таким образом;
- случаи принятия решения Участником о приостановлении или прекращении участия в Системе, в т.ч. в связи с отзывом у Участника необходимых для его деятельности лицензий или иных разрешений либо приостановления их действия, если Участник объявляет о своей ликвидации, либо в отношении него инициирована процедура банкротства.

6.5.2. В случае несоблюдения Участником своих обязательств, условий осуществления расчетов, установленных Правилами, а также в иных случаях, установленных в Правилах, Оператор вправе до дня устранения Участником допущенного нарушения в одностороннем порядке приостановить его участие в Системе, а именно: приостановить возможность совершения операций для целей перевода денежных средств Клиентами Участника, а также ограничить в иных правах и не оказывать иные услуги, предусмотренные Правилами и Договором участия. Оператор производит на регулярной основе мониторинг соответствия Участников критериям, установленным пп. 6.3.1 Правил, и возникновения оснований приостановления и/или прекращения участия в Системе, указанных в пп. 6.5.1 Правил. При установлении факта невыполнения одного или нескольких критериев соответствия Участников и/или при возникновении оснований приостановления и/или прекращения участия в Системе, Оператор осуществляет документальное оформление результатов мониторинга Участников. Ответственное подразделение Оператора доводит

соответствующую информацию до органов управления Оператора для принятия решения о приостановлении/прекращении участия в Системе.

6.5.3. Оператор также вправе приостановить участие в Системе Участника, если имеющиеся в распоряжении Оператора сведения или документы позволяют сделать вывод о высокой вероятности возникновения рисков, ведущих к невозможности осуществления расчетов по операциям, совершенным Клиентами Участника для целей перевода денежных средств, в том числе неисполнения обязанности по обеспечению достаточности денежных средств на Счете Участника в сроки и порядке, установленные Правилами.

6.5.4. Оператор не позднее двух рабочих дней, следующих за днем приостановления участия, уведомляет Участника по согласованным каналам связи о причинах приостановления участия и о необходимости устранения Участником допущенных нарушений. После устранения Участником допущенных нарушений и их последствий участие в Системе возобновляется автоматически либо по заявлению Участника с приложением документов, подтверждающих устранение допущенных нарушений и их последствий (прилагаются при необходимости подтверждения), направленного по согласованным каналам связи.

6.5.5. Участие в Системе Участника прекращается в следующих случаях и порядке:

- по заявлению о прекращении участия Участника в Системе, составленному в письменной форме на бумажном носителе, подписанному уполномоченным лицом Участника и скрепленного печатью Участника, поданному Оператору. Со дня получения заявления о прекращении участия Оператор приостанавливает участие Участника в Системе. Оператор предпринимает меры по прекращению обработки Операционным центром операций с использованием Электронных средств платежа, выпущенных Участником и в сети устройств приема платежей Участника в день получения заявления о прекращении участия в Системе. Не позднее, чем на второй рабочий день после получения заявления о прекращении участия, Оператор уведомляет Участника об объеме неисполненных обязательств Участника, связанных с участием в Системе, включая обязательства по осуществлению расчетов по операциям, совершенным Клиентами Участника для целей перевода денежных средств, и оплаты оказанных Участнику услуг. Участник обязан в срок, не превышающий трех рабочих дней, с даты получения уведомления от Оператора осуществить расчеты по всем своим обязательствам, после чего его участие в Системе прекращается, о чем Оператор уведомляет Участника в письменной форме. Оператор вправе направить уведомление, содержащее информацию о дате прекращения участия в Системе как на бумажном носителе, так и в электронном виде (по используемому сторонами при обмене в рамках Системы электронному каналу связи). В случае, если в срок, не превышающий трех рабочих дней, с даты получения уведомления от Оператора Участник не осуществит расчеты по всем своим обязательствам, то Оператор, в соответствии с заявлением Участника о прекращении участия в Системе, лишает Участника статуса Участника и уведомляет об этом Участника в письменной форме. Урегулирование финансовых отношений в этом случае может быть осуществлено за счет гарантийного взноса Участника, а также в ином порядке, предусмотренном законодательством Российской Федерации;

- по решению Оператора в случаях, предусмотренных в Правилах. При этом участие Участника приостанавливается, Оператор уведомляет Участника о приостановлении с последующим прекращением участия Участника в Системе, об объеме неисполненных обязательств Участника, связанных с участием в Системе, включая обязательства по осуществлению расчетов по операциям, совершенным Клиентами Участника для целей перевода денежных средств, и оплаты оказанных Участнику услуг. Оператор предпринимает меры по прекращению обработки Операционным центром операций с использованием Электронных средств платежа, выпущенных Участником и в сети устройств приема платежей Участника в день уведомления Участника о приостановлении с последующим прекращением участия в Системе. Участник обязан в срок, не превышающий трех рабочих дней, с даты получения уведомления от Оператора осуществить расчеты по всем своим обязательствам,

после чего его участие в Системе прекращается, о чем Оператор уведомляет Участника в письменной форме. Оператор вправе направить уведомление, содержащее информацию о дате прекращения участия в Системе как на бумажном носителе, так и в электронном виде (по используемому сторонами при обмене в рамках Системы электронному каналу связи). В случае, если в срок, не превышающий трех рабочих дней, с даты получения уведомления от Оператора Участник не осуществит расчеты по всем своим обязательствам, то Оператор лишает Участника статуса Участника и уведомляет об этом Участника в письменной форме. Урегулирование финансовых отношений в этом случае может быть осуществлено за счет гарантийного взноса Участника, а также в ином порядке, предусмотренном законодательством Российской Федерации;

- в случаях, предусмотренных законодательством Российской Федерации, в том числе, когда Участник лишается права осуществлять деятельность по переводу денежных средств, включая отзыв (аннулирование) лицензии на осуществление банковских операций. Со дня, когда Оператору стало известно об указанных обстоятельствах, участие Участника в Системе приостанавливается, Оператор уведомляет Участника о приостановлении с последующим прекращением участия Участника в Системе, об объеме неисполненных обязательств Участника, связанных с участием в Системе, включая обязательства по осуществлению расчетов по операциям, совершенным Клиентами Участника для целей перевода денежных средств, и оплаты оказанных Участнику услуг. по всем своим обязательствам, после чего его участие в Системе прекращается. Оператор предпринимает меры по прекращению обработки Операционным центром операций с использованием Электронных средств платежа, выпущенных Участником и в сети устройств приема платежей Участника в день отзыва лицензии. Участник обязан в срок, не превышающий трех рабочих дней, с даты получения уведомления от Оператора осуществить расчеты по всем своим обязательствам, после чего его участие в Системе прекращается, о чем Оператор уведомляет Участника в письменной форме. Оператор вправе направить уведомление, содержащее информацию о дате прекращения участия в Системе как на бумажном носителе, так и в электронном виде (по используемому сторонами при обмене в рамках платежной системы электронному каналу связи). В случае, если в срок, не превышающий трех рабочих дней, с даты получения уведомления от Оператора Участник не осуществит расчеты по всем своим обязательствам, то Оператор лишает Участника статуса Участника и уведомляет об этом Участника в письменной форме. Урегулирование финансовых отношений в этом случае может быть осуществлено за счет гарантийного взноса Участника, а также в ином порядке, предусмотренном законодательством Российской Федерации.

6.5.6. Услуги, предусмотренные Правилами, оказываются Участникам, участие которых в Системе не приостановлено и не прекращено.

6.6. Взаимодействие между Оператором и привлеченными ОУПИ

6.6.1. Взаимодействие Оператора с привлеченными ОУПИ осуществляется в соответствии с Правилами и на условиях договора, заключаемого между привлеченным ОУПИ и Оператором.

6.6.2. Основные функции ОУПИ, требования к ОУПИ, их права и обязанности, ответственность устанавливаются Правилами. Договор, заключаемый между привлеченным ОУПИ и Оператором, содержит положения, необходимые для реализации взаимодействия.

6.6.3. Взаимодействие между Оператором и привлеченным ОУПИ по вопросам защиты информации, обеспечения бесперебойности функционирования Системы, управления рисками, а также по иным вопросам осуществляется в порядке, определенном в соответствующих разделах Правил.

6.6.4. Для обеспечения взаимодействия Оператор и привлеченный ОУПИ используют следующие Согласованные каналы связи:

- Официальный сайт Оператора в сети интернет.

- Личный кабинет ОУПИ.
- Адреса электронной почты Оператора, принадлежащие домену @cpretail.ru, или доведенные до привлеченного ОУПИ уполномоченными должностными лицами Оператора. Информационные рассылки, осуществляемые с таких адресов, являются официальными сообщениями Оператора.
- Обмен сообщениями на бумажных носителях, направляемых сторонами друг другу с привлечением организаций почтовой связи, компаний экспресс-доставки документов, курьеров, а также осуществляемый уполномоченными представителями сторон.
- Адреса электронной почты привлеченного ОУПИ:
 - указанный в договоре с Оператором;
 - указанный в Личном кабинете привлеченного ОУПИ;
 - указанный в официальном сообщении привлеченного ОУПИ, направленном Оператору на бумажном носителе или отправленном на электронный адрес Оператора.

6.6.5. Оператор информирует привлеченных ОУПИ о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры в день такого приостановления (прекращения) любым из указанных ниже способов:

- размещение информации на Официальном сайте Оператора в сети интернет;
- направление уведомления по согласованным каналам связи.

6.7. Взаимодействие между ОУПИ

6.7.1. Взаимодействие Оператора, выполняющего функции Операционного центра, Платежного клирингового центра с Расчетным центром осуществляется в соответствии с Правилами и на условиях договора, заключаемого между Оператором и Расчетным центром.

6.7.2. Расчетный центр обязан принимать и соответствующим образом обрабатывать полученные от Оператора, выполняющего функции Операционного центра, Платежного клирингового центра, Реестры распоряжений.

6.7.3. Оператор, выполняющий функции Операционного центра, Платежного клирингового центра, обязан принимать и соответствующим образом обрабатывать полученные от Расчетного центра уведомления и подтверждения исполнения Реестра распоряжений.

6.8. Взаимодействие между ОУПИ и Участниками

6.8.1. Взаимодействие ОУПИ с Участниками осуществляется в соответствии с Правилами, а также предусматривается условиями договоров, заключаемых между ОУПИ и Участником.

6.8.2. Договор, заключаемый между Участником и Расчетным центром о порядке открытия и ведения банковского счета Участника (далее – Договор Счета) для осуществления расчетов в Системе, должен быть заключен в течение 30 дней с даты заключения Договора участия. Расчетный центр в соответствии с Договором Счета, открывает Участнику Счет Участника, предназначенный для осуществления расчетов в рамках Системы. Счет Участника открывается после предоставления копии Договора участия и документов, предоставление которых для открытия Счета Участника необходимо в соответствии с нормативными актами Банка России, в соответствии с требованиями иных нормативных актов, а также иных документов, предусмотренных Договором Счета. Взаимодействие между Расчетным центром и Участником по вопросам, связанным с ведением Счета Участника, осуществляется в общеустановленном для взаимодействия между кредитной организацией и ее клиентом порядке, предусмотренном банковскими правилами, нормативными актами и договором счета, с учетом требований, установленных Правилами.

6.8.3. Присоединяясь к Правилам, Участники соглашаются с оказанием Оператором операционных услуг и услуг платежного клиринга.

6.8.4. Списание и зачисление денежных средств по счетам Участников осуществляется Расчетным центром на основании полученного от Оператора, выполняющего функции Платежного клирингового центра, распоряжения или Реестра распоряжений. При этом получение дополнительного распоряжения Участников на списание денежных средств со Счета Участника не требуется. На основании распоряжений, включенных в Реестр распоряжений, Расчетный центр составляет распоряжения на перевод денежных средств со Счета Участника получателям. Расчетный центр не несет ответственности за правомерность и содержание включенных в состав Реестра распоряжений о переводе денежных средств и, указанных реквизитов.

6.8.5. Исполнение распоряжений по списанию денежных средств со Счетов Участников, полученных от Участников и не связанных с операциями в рамках Системы, осуществляется Расчетным центром только по согласованию с Оператором в пределах остатка денежных средств на Счете Участника, образовавшегося после исполнения Расчетным центром полученного от Оператора, выполняющего функции Платежного клирингового центра, Реестра распоряжений за операционный день, соответствующий дате получения Расчетным центром указанного распоряжения Участника. Списание денежных средств со Счета Участника осуществляется (в случае, если Договором Счета не предусмотрено иное) только для перевода денежных средств на другой банковский счет Участника, открытый в Расчетном центре или иной кредитной организации, не позднее рабочего дня, следующего за днем предоставления указанного распоряжения в Расчетный центр.

Прием распоряжений непосредственно от Участника по каналам связи, предусмотренным Договором Счета, осуществляется в соответствии с временным регламентом приема расчетных документов, установленным Расчетным центром в зависимости от используемого для передачи распоряжений канала связи.

6.8.6. Средства, поступающие в Расчетный центр в пользу Участника из других кредитных организаций, зачисляются на Счет Участника датой проведения платежа обслуживающим Расчетный центр подразделением расчетной сети Банка России, днем получения Расчетным центром выписок других кредитных организаций, реестров и распоряжений клиринговых центров либо, в случае отсутствия приложений к выписке, в день поступления этих документов в Расчетный центр. Средства, поступающие в пользу Участника со счетов, открытых в Расчетном центре, в котором открыт Счет Участника, зачисляются на Счет Участника датой списания средств со счета Плательщика.

6.9. Контроль соблюдения Правил, ответственность за их несоблюдение

6.9.1. Контроль соблюдения Правил Участниками и привлеченных ОУПИ осуществляет Оператор на постоянной основе путем мониторинга деятельности Участников в процессе оказания услуг в рамках Системы, анализа жалоб и обращений Клиентов, а также мониторинга деятельности привлеченных ОУПИ, анализа жалоб и обращений Субъектов Системы.

6.9.2. Оператор вправе для целей осуществления контроля за соблюдением Правил обязать Участников (как всех, так и любого в отдельности), привлеченных ОУПИ предоставлять отчет о соблюдении ими Правил, о спорных и конфликтных ситуациях между Участником и его Клиентами, связанных с оказанием услуг, предусмотренных Правилами, и иную информацию относительно деятельности в качестве Участника или привлеченного ОУПИ. Периодичность предоставления указанного отчета не может быть чаще, чем один раз в месяц.

6.9.3. Оператор регулярно анализирует поступающие жалобы и обращения. По результатам анализа Оператором может быть принято решение о разработке мероприятия по устранению имеющихся некорректных действий, в том числе обращение к Участнику, привлеченному ОУПИ в рабочем режиме (в т.ч. по согласованным каналам связи),

организация встреч с Участником, привлеченным ОУПИ, направление им официальных писем, в т.ч. содержащих требования об уплате неустойки в соответствии с Правилами и/или условиями заключенных договоров.

6.9.4. Участники, привлеченные ОУПИ несут ответственность за несоблюдение Правил в порядке, предусмотренных Правилами и законодательством РФ. Несоблюдение Правил может служить основанием принятия Оператором решения о прекращении участия Участника в Системе, а также критерием прекращения выполнения функций привлеченного Оператора услуг платежной инфраструктуры.

6.9.5. Оператор вправе приостановить либо ограничить деятельность Участника, ОУПИ, обеспечивая при этом бесперебойность функционирования Системы.

6.9.6. Контроль соблюдения Участниками, привлеченными ОУПИ требований применимого законодательства, в т.ч. валютного законодательства, законодательства о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма, о защите персональных данных, осуществляют соответствующие надзорные органы Российской Федерации или страны нахождения Участника.

6.10. Порядок предоставления Участниками и привлеченными Операторами услуг платежной инфраструктуры информации о своей деятельности Оператору

Участники и привлеченные Операторы УПИ ежегодно, не позднее последнего числа первого месяца года, предоставляют по согласованному каналу связи Оператору сводную информацию об имевших место в отчетном периоде (завершившийся календарный год) чрезвычайных и спорных ситуациях, выявленных инцидентах, случаях нарушения бесперебойности функционирования Системы, а также иную информацию о своей деятельности в рамках Системы, предусмотренную Правилами, в том числе:

- о результатах проведенных оценок соответствия установленным требованиям, когда в соответствии с Правилами такая оценка должна быть проведена или проводилась по собственной инициативе;

- о степени выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств;

- о реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств;

- о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;

- о выявленных угрозах и уязвимостях в обеспечении защиты информации.

Расчетный центр, в случае несоответствия осуществляемой в отчетном периоде (завершившийся календарный год) в рамках Системы деятельности контрольным показателям уровня оказания расчетных услуг, установленным в Правилах, предоставляет детализированную информацию о допущенных нарушениях указанных показателей, причинах, их повлекших, а также о мерах, предпринятых с целью недопущения выявленных нарушений в будущем.

Привлеченные Операторы УПИ информируют Оператора о нарушении оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, при котором превышено время восстановления оказания услуг платежной инфраструктуры в случае их приостановления и (или) время восстановления оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, в порядке, установленном для информирования в чрезвычайных ситуациях.

Дополнительно, по запросу Оператора Участники и привлеченные Операторы УПИ обязаны в срок, не превышающий пяти рабочих дней со дня получения указанного запроса, предоставлять Оператору информацию, связанную с выполнением возложенных на них функций и обязанностей в рамках Системы.

6.11. Порядок изменения Правил

6.11.1. Изменения и/или дополнения в Правила вносятся Оператором в одностороннем порядке.

6.11.2. Для внесения изменений в Правила Оператор обязан обеспечить Участникам возможность предварительного ознакомления с предлагаемыми изменениями и направления своего мнения Оператору в установленный им срок, который не может быть менее одного месяца. Возможность предварительного ознакомления с предлагаемыми изменениями обеспечивается путем размещения предлагаемых изменений на Официальном сайте Оператора в сети интернет.

6.11.3. Оператор размещает на Официальном сайте Оператора в сети интернет:

- Проект новой редакции Правил или предлагаемых изменений с указанием срока вступления изменений в силу;
- информацию о сроке, в течение которого Участники могут направить Оператору свое мнение о вносимых изменениях.

6.11.4. Участники после ознакомления с вносимыми изменениями вправе в установленный Оператором срок направить Оператору свое мнение.

6.11.5. По истечению срока, установленного пп. 6.11.2 Правил, единоличный исполнительный орган Оператора утверждает новую редакцию Правил с указанием срока начала действия изменений. Изменения в Правила вносятся в срок не менее одного месяца со дня окончания срока, указанного в пп. 6.11.2 Правил.

6.11.6. Внесение изменений в Правила не требует соблюдение сроков, установленных в пп. 6.11.2, 6.11.5 Правил в случае получения Оператором письменного согласия всех Участников на внесение предложенных изменений в Правила.

6.11.7. После получения Оператором письменного согласия всех Участников на внесение предложенных изменений в Правила, единоличный исполнительный орган Оператора утверждает новую редакцию Правил с указанием срока начала действия изменений.

6.11.8. Оператор размещает на Официальном сайте Оператора в сети интернет редакцию Правил, утвержденную в соответствии в пп. 6.11.5 или 6.11.7 Правил.

6.12. Порядок взаимодействия в рамках Системы в чрезвычайных и спорных ситуациях

6.12.1. В случае выявления в рамках Системы чрезвычайных ситуаций, в том числе, событий, вызвавших системные сбои, Субъекты Системы, выявившие указанные ситуации, незамедлительно предпринимают все зависящие от них действия, направленные на снижение вредных последствий, незамедлительно информируют Оператора и Субъекта Системы, в функциональной зоне ответственности которого находится область возникновения чрезвычайной/спорной ситуации или сбоя, по любому из доступных каналов связи, в том числе посредством телефонной связи, по факсу, по электронной почте, о возникшей ситуации, включая информирование о событиях, по их мнению, вызвавших чрезвычайную/спорную ситуацию, операционные сбои, об их причинах и последствиях.

6.12.2. Оператор незамедлительно после получения информации о возникновении чрезвычайной/спорной ситуации предпринимает действия, направленные на снижение вредных последствий, а также, путем взаимодействия с Субъектом Системы, в функциональной зоне ответственности которого находится область возникновения чрезвычайной/спорной ситуации, действия, направленные на выявление и устранение причин возникновения чрезвычайной/нестандартной ситуации, на восстановление нормального режима функционирования Системы, ликвидации негативных последствий.

6.12.3. После восстановления нормального функционирования Системы Оператор по согласованным каналам связи информирует заинтересованных Субъектов Системы о предпринятых действиях и достигнутых результатах.

6.12.4. Оператор вправе приостановить все операции, относящиеся к Субъекту Системы, в функциональной зоне ответственности которого находится область возникновения чрезвычайной/спорной ситуации.

6.12.5. Оператор разрабатывает, тестирует и пересматривает план действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности в случае возникновения нестандартных и чрезвычайных ситуаций (далее - план ОНиВД) Оператора с периодичностью не реже одного раза в два года.

Оператор разрабатывает и включает в план ОНиВД мероприятия, направленные на управление непрерывностью функционирования Системы в случае возникновения инцидентов, связанных с приостановлением оказания услуг платежной инфраструктуры или нарушением установленных уровней оказания услуг платежной инфраструктуры, в том числе:

а. при наличии в Системе двух и более Расчетных центров - мероприятия по обеспечению взаимозаменяемости данных ОУПИ;

б. при выполнении Оператором функций Операционного центра, Платежного клирингового центра и при наличии в Системе одного Расчетного центра - мероприятия по привлечению ОУПИ и по переходу Участников Платежной системы на обслуживание к вновь привлеченному ОУПИ в течение 20 (двадцати) рабочих дней после привлечения в случаях:

- превышения времени восстановления оказания услуг платежной инфраструктуры при приостановлении их оказания более двух раз в течение трех месяцев подряд;

- нарушения Правил, выразившего в отказе привлеченного ОУПИ в одностороннем порядке от оказания услуг Участнику (Участникам) Системы, не связанного с приостановлением (прекращением) участия в Системе в случаях, предусмотренных настоящими Правилами.

6.12.6. Оператор обеспечивает реализацию указанных выше мероприятий. В случае, когда Оператор выполняет функции Операционного и Платежного клирингового центра, а также при условии наличия в Системе одного Расчетного центра, Оператор осуществляет мероприятия, указанные в части б. подпункта 6.12.5 Правил в соответствии с порядком, изложенном в пп. 11.4.3 Правил.

6.12.7. Оператор организует, при необходимости, разработку и контролирует наличие планов ОНиВД у привлеченных ОУПИ, проведение ими тестирования и пересмотра планов ОНиВД с периодичностью не реже одного раза в два года.

В случае, если привлеченный ОУПИ является кредитной организацией, разработка, тестирование и пересмотр плана ОНиВД осуществляется в порядке, предусмотренном нормативными документами Банка России.

Оператор передает часть функций по реализации мероприятий по управлению рисками и непрерывностью функционирования Системы привлеченным ОУПИ и Участникам.

6.12.8. Привлеченные Операторы УПИ обязаны разработать, реализовывать, пересматривать, а также проводить проверку (тестирование) плана ОНиВД. План ОНиВД должен определять порядок, способы и сроки осуществления комплекса мероприятий по предотвращению или своевременной ликвидации последствий возможного нарушения режима повседневного функционирования привлеченного Оператора УПИ, вызванного непредвиденными обстоятельствами (возникновением чрезвычайной ситуации или иным событием, наступление которого возможно, но трудно предсказуемо и связано с угрозой существенных материальных потерь или иных последствий, препятствующих выполнению Оператором УПИ принятых на себя обязательств).

6.12.9. В целях контроля за выполнением указанной обязанности Оператор с периодичностью не реже одного раза в два года направляет в адрес привлеченных Операторов УПИ запрос о предоставлении:

- копии плана ОНиВД Расчетного центра;

- информации о проведении Расчетным центром проверки (тестирования) и/или ее сроках/результатах, а также о периодичности пересмотра плана ОНиВД.

6.13. Порядок взаимодействия с платежными системами

6.13.1. Оператор вправе заключать с операторами платежных систем договоры/соглашения о взаимодействии платежных систем в целях осуществления межсистемных Операций. Под межсистемной Операцией понимается Операция, в осуществлении которой участвуют Субъекты и/или Устройство приема платежа разных платежных систем.

6.13.2. Оператор после заключения договора/соглашения о взаимодействии Системы с иной платежной системой отражает порядок взаимодействия в Правилах. Платежный клиринг и расчеты между Системой и другой платежной системой, с оператором которой заключен взаимный договор/соглашение, осуществляются в порядке, предусмотренном данным соглашением о взаимодействии платежных систем.

6.13.3. Оператор ведет перечень платежных систем, с которыми осуществляется взаимодействие, поддерживает его в актуальном состоянии и размещает указанный перечень на Официальном сайте Оператора в сети интернет, доводит перечень до сведения Банка России в случаях и в порядке, определенных законодательством Российской Федерации и нормативными актами Банка России.

6.14. Порядок досудебного разрешения споров между Субъектами Системы

6.14.1. Спорные ситуации, включая системные сбои, между Оператором и Участниками, между Оператором и привлеченными ОУПИ, между Участниками и привлеченными ОУПИ разрешаются (урегулируются) в досудебном порядке: в рабочем порядке и/или по итогам работы комиссии по разрешению спорной ситуации, возникшей при применении электронного документооборота (далее – комиссия).

6.14.2. В случае невозможности разрешения спорной ситуации в рабочем порядке и/или по итогам работы комиссии, споры разрешаются в претензионном порядке, а в случае не удовлетворения претензии, споры направляются на рассмотрение суда в порядке, установленном законодательством Российской Федерации.

6.14.3. В случае возникновения обстоятельств, свидетельствующих, по мнению одного из Субъектов системы, о возникновении и/или наличии спорной ситуации, данный Субъект (далее – инициатор) незамедлительно извещает другую заинтересованную сторону о возможном возникновении и/или наличии спорной ситуации, обстоятельствах, свидетельствующих о ее возникновении или наличии, а также ее предполагаемых причинах.

6.14.4. Субъекты Системы, которым было направлено извещение о спорной ситуации, и, участвующие в разрешении спорной ситуации (далее – ответчики), обязаны не позднее чем в течение следующих двух рабочих дней проверить наличие указанных в извещении обстоятельств, и по необходимости принять меры по разрешению спорной ситуации со своей стороны. В тот же срок ответчики извещают доступными способами инициатора о результатах проверки и, при необходимости, о мерах, принятых для разрешения спорной ситуации.

6.14.5. Спорная ситуация признается разрешенной в рабочем порядке в случае, если инициатор удовлетворен информацией, полученной в извещениях участников спора, и не имеет к ним претензий в связи со спорной ситуацией.

6.14.6. В случае, если инициатор не удовлетворен информацией, полученной от ответчиков, для рассмотрения спорной ситуации формируется комиссия.

Если спорная ситуация не была разрешена в рабочем порядке, инициатор должен не позднее чем в течение трех рабочих дней после возникновения спорной ситуации направить уведомление о спорной ситуации (далее - уведомление) и предложение о создании комиссии по разрешению спорной ситуации ответчику и Оператору (если Оператор не является инициатором или ответчиком). Уведомление, подписанное уполномоченным представителем инициатора, направляется по согласованному каналу связи.

Уведомление должно содержать информацию о предмете и существе спорной ситуации, обстоятельствах, по мнению инициатора, свидетельствующих о наличии спорной ситуации, возможных причинах и последствиях ее возникновения. Уведомление должно содержать информацию с указанием фамилий, имен, отчеств, должностей и контактной информации должностных лиц инициатора, уполномоченных участвовать в разрешении спорной ситуации.

6.14.7. Организацию формирования и деятельности комиссии осуществляет Оператор. Расходы, связанные с формированием и обеспечением деятельности комиссии для разрешения спорной ситуации, несет сторона инициатор, если по итогам рассмотрения спорной ситуации комиссией не будет установлено иное. По результатам рассмотрения комиссией спорной ситуации, расходы, связанные с формированием и обеспечением деятельности комиссии для разрешения спорной ситуации, могут быть отнесены на счет ответчиков либо распределены между инициатором и ответчиками в определенной в решении комиссии пропорции.

6.14.8. Оператор не позднее чем в течение двух рабочих дней после получения от инициатора уведомления направляет по согласованному каналу связи инициатору и ответчику информацию о предлагаемом месте, дате и времени сбора комиссии, список предлагаемых для участия в работе комиссии представителей Оператора с указанием фамилий, имен, отчеств, должностей, их контактной информации (телефон, факс, электронная почта), а также предлагает инициатору и ответчикам не позднее чем в течение двух рабочих дней после получения указанной информации сообщить список предлагаемых для участия в работе комиссии их представителей с указанием фамилий, имен, отчеств, должностей, их контактной информации (телефон, факс, электронная почта).

После получения по согласованному каналу связи информации от инициатора и ответчиков, а также в случае неполучения информации в указанный выше срок, Оператор не позднее чем на следующий рабочий день формирует комиссию путем издания соответствующего распорядительного акта.

6.14.9. Если стороны не договорятся об ином, в состав комиссии входит по три уполномоченных лица Оператора, инициатора и каждого из ответчиков, участвующих в разрешении спорной ситуации в соответствии с полученными и направленными списками представителей инициатора, ответчиков и Оператора.

Право представителей на участие в комиссии, на представление соответствующих организаций должно подтверждаться официальным документом (доверенностью, копией приказа или распоряжения).

6.14.10. Задача комиссии - установить на организационно-техническом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о наличии спорной ситуации, ее причинах и последствиях.

Комиссия рассматривает спорную ситуацию и выносит решение в тридцатидневный срок. В исключительных случаях срок работы комиссии по решению членов комиссии может быть дополнительно продлен не более чем на тридцать дней. Любой из членов комиссии вправе выступить с инициативой о привлечении для проведения технической экспертизы независимого эксперта. Решение о привлечении независимого эксперта комиссия принимает простым большинством голосов, при этом сторона, чей представитель выступил с инициативой привлечения независимого эксперта, самостоятельно решает вопрос об оплате экспертных услуг.

6.14.11. Все действия, предпринимаемые комиссией для выяснения фактических обстоятельств, а также выводы, сделанные комиссией, заносятся в протокол работы комиссии. Протокол работы комиссии должен содержать следующие данные:

- состав комиссии с указанием сведений о фамилиях, именах, отчествах, местах работы, занимаемых должностях, контактной информации каждого из членов комиссии;
- краткое изложение обстоятельств, свидетельствующих, по мнению инициатора, о возникновении и/или наличии спорной ситуации;
- установленные комиссией фактические обстоятельства;

- мероприятия, проведенные комиссией для установления наличия, причин возникновения и последствий возникшей спорной ситуации, с указанием даты времени и места их проведения;
- выводы, к которым пришла комиссия в результате проведенных мероприятий;
- подписи всех членов комиссии.

В случае, если мнение члена или членов комиссии относительно порядка, методики, целей проводимых мероприятий не совпадает с мнением большинства членов комиссии, в протокол заносится соответствующая запись, которая подписывается членом или членами комиссии, чье особое мнение отражает соответствующая запись.

Протокол составляется в форме документа на бумажном носителе по одному экземпляру для каждой из сторон. По обращению любого из членов комиссии стороной, к которой было направлено обращение, ему должна быть выдана заверенная уполномоченным лицом этой стороны копия протокола.

6.14.12. По итогам работы Комиссии составляется акт, при этом акт должен содержать следующую информацию:

- состав комиссии;
- дату и место составления акта;
- даты и время начала и окончания работы комиссии;
- фактические обстоятельства, установленные комиссией;
- краткий перечень мероприятий, проведенных комиссией;
- выводы, к которым пришла комиссия в результате проведенных мероприятий;
- подписи членов комиссии;
- в случае наличия - особое мнение члена или членов комиссии.

Акт составляется в форме документа на бумажном носителе по одному экземпляру для каждой из сторон. При обращении любого из членов комиссии, сторона, к которой было направлено обращение, должна выдать ему заверенную уполномоченным лицом этой стороны копию акта.

Акт комиссии является основанием для принятия сторонами решения по урегулированию конфликтной ситуации.

6.14.13. В срок не более трех рабочих дней со дня окончания работы комиссии, стороны на основании выводов комиссии принимают меры по разрешению спорной ситуации и извещают другие заинтересованные стороны о принятых мерах.

Спорная ситуация признается разрешенной по итогам работы комиссии, если стороны удовлетворены выводами, полученными комиссией, мерами, принятыми другими участвующими в разрешении спорной ситуации сторонами, и не имеют взаимных претензий.

В случае, если спорная ситуация признается сторонами разрешенной, то в срок не позднее пяти рабочих дней со дня окончания работы комиссии стороны оформляют решение об урегулировании спорной ситуации.

Решение составляется в форме документа на бумажном носителе по одному экземпляру каждой стороне. Решение подписывается уполномоченными в разрешении конфликтной ситуации лицами сторон.

6.14.14. В случае, если спорная ситуация не разрешена по итогам работы комиссии, в случае прямого или косвенного отказа одной из сторон от участия в работе, или, если одной из сторон создавались препятствия работе комиссии, инициатор, считающий, что его права были нарушены, обязан направить ответчику претензию.

Претензия должна содержать:

- изложение существа требований инициатора;
- при возможности денежной оценки претензии - ее сумму и расчет;
- изложение фактических обстоятельств, на которых основываются требования инициатора и доказательства, подтверждающие их, со ссылкой на соответствующие нормы законодательства Российской Федерации и нормативных правовых актов, а также Правил;

- сведения о работе комиссии и, в случае если комиссия работала в связи с рассматриваемой спорной ситуацией, копии материалов работы комиссии, независимо от выводов комиссии, согласия или несогласия с этими выводами инициатора;
- иные документы, имеющие значение, по мнению инициатора;
- перечень прилагаемых к претензии документов и других доказательств, а также иные сведения, необходимые для урегулирования разногласий по претензии.

Претензия составляется в форме документа на бумажном носителе, подписывается руководителем инициатора либо иным уполномоченным лицом, заверяется печатью инициатора. Претензия и прилагаемые к ней документы направляются в адрес ответчика в установленном порядке, обеспечивающим подтверждение вручения корреспонденции; одновременно копия направленных ответчику документов направляется Оператору.

Ответчик, в адрес которого направлена претензия, обязан в срок не позднее пяти рабочих дней удовлетворить требования претензии или представить инициатору мотивированный отказ в их удовлетворении, одновременно направив копию отказа Оператору. Непредставление ответа на претензию в течение указанного срока является нарушением установленного Правилами претензионного порядка и может рассматриваться в качестве отказа в удовлетворении требований претензии.

6.14.15. В случае невозможности разрешения споров и разногласий по спорной ситуации в рабочем порядке, по итогам работы комиссии или в претензионном порядке, разрешение споров и разногласий по конфликтной ситуации передается на рассмотрение Арбитражного суда города Москвы.

6.15. Ответственность за несоблюдение Правил

6.15.1. Субъекты Системы несут ответственность за неисполнение или ненадлежащее исполнение своих обязательств в соответствии с законодательством Российской Федерации и Правилами.

6.15.2. В случае неисполнения Участником предусмотренных Правилами и/или Договором участия обязательств, связанных с обеспечением достаточности денежных средств на Счете Участника для осуществления расчетов по операциям, совершенным Клиентами Участника, а также в случае неисполнения обязательств по оплате оказанных услуг, указанных в Тарифах, Оператор вправе начислить, а Участник обязан (в случае начисления) уплатить пеню в размере 0,1% (Ноль целых одна десятая) процентов от недостающей суммы за каждый день просрочки.

В случае неоднократного нарушения Участником Правил Оператор вправе лишить Участника статуса Участника, расторгнув Договор участия в одностороннем порядке с последующим уведомлением Участника о расторжении Договора участия в порядке, определенном в п. 6.5 Правил.

В случае однократного неисполнения Участником предусмотренных Правилами и Договором участия обязательств, связанных с обеспечением завершения расчетов, Оператор вправе лишить Участника статуса Участника, расторгнув Договор участия в одностороннем порядке с последующим уведомлением Участника о расторжении Договора участия в порядке, определенном в п. 6.5 Правил.

6.15.3. Расчетный центр несет ответственность перед Оператором за незавершение расчетов по Операциям, в размере незавершенных расчетов, за исключением случаев неполучения по вине Оператора Реестра распоряжений. Оператор вправе потребовать, а Расчетный центр обязан (в случае получения соответствующего требования) уплатить Оператору штраф в размере сумм незавершенных расчетов, а также уплатить пеню в размере 0,1% (Ноль целых одна десятая) процентов от суммы незавершенных расчетов за каждый день просрочки.

6.15.4. Субъекты Системы освобождаются от ответственности за неисполнение или ненадлежащее исполнение своих обязательств, если оно явилось следствием непреодолимой

силы при условии, что эти обстоятельства непосредственно повлияли на исполнение обязательств.

Под непреодолимой силой понимаются чрезвычайные и непредотвратимые обстоятельства, которые невозможно было предвидеть и предотвратить имеющимися в распоряжении нарушившего обязательство Субъекта Системы разумными средствами, в том числе: землетрясения, наводнения, пожары, эпидемии, аварии на транспорте, военные действия, массовые беспорядки и др.

Субъект Системы, подвергшийся действию обстоятельств непреодолимой силы и оказавшийся вследствие этого не в состоянии выполнить свои обязательства, должен сообщить об этом Оператору в течение одного рабочего дня с момента возникновения указанных обстоятельств в устной форме и в течение трех рабочих дней в письменной форме. В противном случае Субъект Системы, нарушивший обязательство, не вправе ссылаться на обстоятельства непреодолимой силы. Уведомление должно содержать данные о характере обстоятельств, оценку их влияния на возможность исполнения своих обязательств и срок исполнения обязательств с приложением подтверждения официальных органов о действии обстоятельств непреодолимой силы.

7. Порядок осуществления платежного клиринга и расчетов

7.1. Общий порядок осуществления Операций в Системе и применяемые формы безналичных расчетов

7.1.1. Переводы денежных средств в Системе осуществляются в валюте Российской Федерации в соответствии с нормативными актами Банка России, регламентирующими порядок осуществления расчетов.

7.1.2. Перевод денежных средств осуществляется со Счета Участника на основании распоряжений, поступающих в Расчетный центр в электронном виде (по каналам связи и на отчуждаемых машинных носителях информации) или на бумажном носителе.

7.1.3. На основании распоряжения или Реестра распоряжений, переданного Расчетному центру Оператором, выполняющему функции Операционного центра и Платежного клирингового центра в случаях и в порядке, предусмотренных Правилами, Расчетный центр составляет распоряжения и осуществляет перевод денежных средств со Счета Участника Получателю средств.

7.1.4. Перевод денежных средств в Системе осуществляется в рамках следующих форм безналичных расчетов: расчеты платежными поручениями, расчеты инкассовыми поручениями, расчеты в форме перевода денежных средств по требованию получателя средств (прямое дебетование).

7.1.5. В Системе Переводы денежных средств могут быть осуществлены с использованием ЭСП. Предусмотрено инициирование Операции:

- с использованием мобильного приложения, обеспечивающего доступ Клиентов к Услугам Системы;
- с использованием программного интерфейса, обеспечивающего доступ Клиентов к Услугам Системы;
- с предъявлением Банковской карты, когда Банковская карта и Держатель Банковской карты присутствуют в месте совершения Операции;
- без предъявления Банковской карты, когда Банковская карта и Держатель Банковской карты отсутствуют в месте совершения Операции.

7.1.6. Операции с использованием ЭСП осуществляются при обязательном соблюдении следующих условий:

- сумма Авторизационного запроса не превышает сумму Предельного размера (лимита) обязательств Участника;

- при совершении Операции с использованием Банковской карты получена Авторизация Участника-эмитента Банковской карты на запрошенную Операцию;
- сумма Операции не превышает Лимит ЭСП.

Участники осуществляют Перевод денежных средств по распоряжению Пользователя ЭСП, оформленному с использованием ЭСП.

По завершении Операции с использованием ЭСП составляются документы на бумажном носителе и (или) в электронной форме. Документ по Операции является основанием для осуществления расчетов по указанной Операции и (или) служит подтверждением ее совершения. Документ по Операции составляется в соответствии с требованиями Правил, нормативных актов Банка России.

7.1.7. Формат распоряжений, используемых в Системе, размещаются на Официальном сайте Оператора в сети интернет.

7.2. Платежный клиринг

7.2.1. В целях обеспечения исполнения обязательств Участников операции в рамках Системы осуществляются исходя из доступного остатка платежной клиринговой позиции (далее – доступный остаток) каждого Участника, размер которого контролируется и изменяется Оператором, выполняющим функции Платежного клирингового центра при приеме распоряжений Участников в соответствии с порядком, установленным Правилами.

7.2.2. Доступный остаток формируется из фактического остатка денежных средств на Счете Участника в Расчетном центре, который уменьшается на сумму распоряжений Участника, комиссий, подлежащих уплате и увеличивается на сумму зачисленных денежных средств Получателям, комиссий, подлежащих зачислению Участнику, а также увеличивается на сумму аннулированных распоряжений, комиссий, подлежащих возврату.

7.2.3. Платежный клиринг в Платежной системе осуществляется Оператором, выполняющим функции Операционного центра и Платежного клирингового центра, посредством:

- выполнения процедур приема к исполнению распоряжений Участников, включая проверку соответствия распоряжений установленным требованиям, определение достаточности доступного остатка для исполнения распоряжений;
- определением размера платежных клиринговых позиций и направления Участникам отчета об операциях, совершенных Клиентами Участника в целях перевода денежных средств в течение операционного дня, расчеты по которым осуществляются на основании распоряжений и за счет Участника;
- передачи Расчетному центру для исполнения принятых распоряжений Участников.

7.2.4. Процедура приема к исполнению распоряжений Участников включает:

а) При передаче Оператору, выполняющему функции Операционного центра и Платежного клирингового центра распоряжений Участника в виде Реестра Участника:

- Удостоверение права Участника распоряжаться денежными средствами;
- Контроль целостности Реестра Участника;
- Контроль структуры Реестра Участника;
- Контроль полноты реквизитов Реестра Участника;
- Контроль достаточности денежных средств Плательщика;
- Контроль достаточности Лимитов ЭСП (опционально);
- Контроль достаточности денежных средств на Счете Участника;
- Контроль достаточности Предельного размера (лимита) обязательств Участника для исполнения распоряжений или Реестра Участника.

При положительном результате процедур приема распоряжений Участника, Оператор, выполняющий функции Операционного центра и Платежного клирингового центра, принимает к исполнению Реестр Участника и направляет Участнику по согласованному каналу связи извещение в электронном виде, подтверждающее прием Реестра Участника к исполнению. Все распоряжения по Операциям, входящие в состав Реестра Участника, принимаются к исполнению и включаются в платежный клиринг.

При отрицательном результате процедуры приема распоряжений Участника к исполнению Оператор, выполняющий функции Операционного центра и Платежного клирингового центра, если в Реестре Участника обнаружены ошибки, приводящие к невозможности приема:

- всего Реестра Участника. В этом случае Участнику, передавшему указанный Реестр Участника, направляется уведомление в электронном виде, содержащее информацию об обнаруженных ошибках;
- части распоряжений по Операциям, входящих в Реестр Участника. В этом случае Участнику направляется уведомление в электронном виде о частичном принятии Реестра Участника, содержащее информацию об обнаруженных ошибках. Распоряжения по Операциям, которые успешно прошли проверку, принимаются к исполнению и включаются в платежный клиринг.

б) При передаче Оператору, выполняющему функции Операционного центра и Платежного клирингового центра распоряжений Плательщиков:

- Удостоверение права Плательщика распоряжаться денежными средствами;
- Контроль целостности распоряжения Плательщика;
- Контроль структуры распоряжения Плательщика;
- Контроль полноты реквизитов распоряжения Плательщика;
- Контроль достаточности денежных средств Плательщика;
- Контроль достаточности Лимитов ЭСП (опционально);
- Определение Участника, обслуживающего Плательщика;
- Контроль достаточности денежных средств на Счете Участника;
- Контроль достаточности Предельного размера (лимита) обязательств Участника для исполнения распоряжения.

При положительном результате процедур приема распоряжения Плательщика, Оператор, выполняющий функции Операционного центра и Платежного клирингового центра, принимает к исполнению распоряжение Клиента и направляет Участнику по согласованному каналу связи извещение в электронном виде, подтверждающее прием распоряжения Плательщика к исполнению. Распоряжение Плательщика считается принятым Участником, обслуживающим Плательщика, к исполнению, при положительном результате процедуры приема распоряжения Плательщика, Оператором, выполняющим функции Операционного центра и Платежного клирингового центра.

7.2.5. Определение платежной клиринговой позиции Участника осуществляется на нетто-основе. Платежная клиринговая позиция определяется в размере разницы между общей суммой подлежащих исполнению распоряжений Участников, по которым Участник является плательщиком, и общей суммой распоряжений Участников, по которым Участник является получателем средств, расчеты по которым осуществляются за счет Участника, на основании информации об указанных Операциях, полученной за операционный день Оператором, выполняющим функции Операционного центра и Платежного клирингового центра, от Участников, а также информации с устройств приема платежей, зафиксированной в отчетах, передаваемых Оператором Участнику. Указанная информация является основанием для передачи Оператором, выполняющим функции Операционного центра и Платежного клирингового центра Расчетному центру от имени Участника подлежащих исполнению распоряжений о списании денежных средств со Счета Участника.

7.2.6. После определения платежной клиринговой позиции Оператор, выполняющий функции Операционного центра и Платежного клирингового центра, формирует Реестры ПКЦ для Участников и Реестр распоряжений для Расчетного центра, и направляет сформированные реестры по согласованным каналам связи адресатам.

7.2.7. Реестр распоряжений может быть сформирован и направлен в Расчетный центр до окончания операционного дня в рамках процедур управления рисками в Системе в случае приостановления или прекращения участия Участника в Системе. В случае направления Реестра распоряжений в связи с приостановлением или прекращением участия Участника в Системе, Реестр распоряжений содержит сведения о комиссиях за услуги, оказанные Участнику за период с начала календарного месяца оказания услуг по дате приостановления или прекращения участия в Системе.

7.2.8. Реестры ПКЦ, содержащие расшифровку каждой Операции, вошедшей в платежную клиринговую позицию соответствующего Участника, являются подтверждением исполнения распоряжений Участников.

7.2.9. Операции Участников за операционные дни, соответствующие выходным и праздничным дням, включаются в Реестры ПКЦ первого рабочего дня и направляются Участникам по его окончании.

7.2.10. Форматы Реестра Участника и Реестра ПКЦ, Реестра распоряжений, используемых в Системе, размещаются на Официальном сайте Оператора в сети интернет.

7.2.11. В случае, если платежная клиринговая позиция Участника была определена с учетом использования Предельного размера (лимита) обязательств Участника и Участник в срок, определенный п. 7.3.4 Правил не исполнил обязанности по поступлению на Счет Участника необходимой суммы денежных средств, то Оператор, выполняющий функции Операционного центра и Платежного клирингового центра уведомляет Участника о возврате принятого к исполнению распоряжения Участника/Плательщика и соответствующим образом корректирует платежную клиринговую позицию.

7.3. Расчеты

7.3.1. Расчеты в Системе по операциям, совершенным Клиентом Участника в целях Перевода денежных средств, в том числе с использованием Электронных средств платежа, эмитированных/предоставленных Участником, и по обязательствам Участника осуществляются со Счета Участника.

7.3.2. Расчеты осуществляются Расчетным центром посредством списания и зачисления (без дополнительного распоряжения Участника) денежных средств со/на Счета Участника на основании поступившего от Оператора, выполняющего функции Операционного центра и Платежного клирингового центра, Реестра распоряжений в размере сумм определенных платежных клиринговых позиций.

7.3.3. Расчеты осуществляются по рабочим дням в соответствии с законодательством Российской Федерации и Постановлениями Правительства Российской Федерации.

7.3.4. Участник обязан до 15.00 часов по московскому времени рабочего дня, следующего за днем совершения Клиентами Участника операций по переводу денежных средств, обеспечить поступление денежных средств на Счет Участника в размере, достаточном для осуществления расчетов по Операциям, принятым к исполнению Оператором, выполняющим функции Операционного центра и Платежного клирингового центра.

7.3.5. В случае, если Участник в срок, определенный п. 7.3.4 Правил не исполнил обязанности по поступлению на Счет Участника необходимой суммы денежных средств, то Расчетный центр возвращает неисполненное распоряжение Плательщика/Участника, о чем сообщает Оператору, выполняющему функции Операционного центра и Платежного клирингового центра в рамках процедуры подтверждения исполнения Реестра распоряжений.

7.3.6. Общая сумма совершенных Клиентами Участника операций по переводу денежных средств, списание по которым со Счета Участника в пользу получателей еще не произведено, не должна превышать сумму Предельного размера (лимита) обязательств, установленного Оператором Участнику в порядке, определенном Правилами.

7.3.7. Исполнение Участниками обязательств по переводу денежных средств в Системе обеспечивается:

- предоставлением Расчетным центром Оператору, выполняющему функции Операционного центра и Платежного клирингового центра, данные об остатках денежных средств на Счетах Участников для осуществления контроля за рисками неисполнения (ненадлежащего исполнения) Участниками обязательств по Переводу денежных средств;
- контролем Расчетного центра достаточности денежных средств на Счетах Участников для осуществления расчетов;
- обязательствами Расчетного центра осуществлять расчетные услуги в порядке, установленном Правилами, а также договором банковского счета, заключенного между Расчетным центром и соответствующим Участником;
- осуществлением расчетов со Счета Участника;
- совершением Операций с использованием Устройств приема платежей только в случае получения в режиме реального времени сведений о достаточности предельного размера (лимита) обязательств Участника и/или Лимита ЭСП (Лимит по Банковской карте) его Клиента, установленных в соответствии с Правилами.

7.3.8. Участники выполняют в отношении Реестров ПКЦ процедуры приема к исполнению распоряжений в соответствии с требованиями, установленными нормативными актами Банка России, и не позднее рабочего дня, следующего за днем получения Реестра ПКЦ, осуществляют зачисление (перевод) на банковские счета Получателей сумм Переводов, включенных в платежные клиринговые позиции на основании распоряжений Плательщиков и/или распоряжений/Реестров Участников.

7.4. Временной регламент функционирования Системы

7.4.1. В качестве единой шкалы времени признается московское время. Контрольным является время системных часов аппаратных средств Операционного центра. Время приема распоряжений представлено в Таблице №1, регламентное время обработки распоряжений и проведения расчетов представлены в Таблице №2.

7.4.2. Операционный день в Системе – с 00:00:00 до 23:59:59 каждого календарного дня.

7.4.3. Время приёма к исполнению распоряжений Участников.

Таблица №1

Событие	Время (по московскому времени)
Прием к исполнению распоряжений Участников (операционные услуги, услуги платежного клиринга)	Круглосуточно

7.4.4. Регламент обработки распоряжений и осуществления расчетов.

Таблица №2

Событие	Время (по московскому времени)
Направление Платежным клиринговым центром Участникам извещения о приеме распоряжения Плательщика к исполнению (операционные услуги, услуги платежного клиринга)	не позднее 5 минут после ввода распоряжения в ПК «КП РИТЕЙЛ»
Расчет платежной клиринговой позиции Участников	с 00:00:00 до 09:00:00 следующего

(услуги платежного клиринга)	рабочего дня
Формирование Реестров ПКЦ и Реестра распоряжений (услуги платежного клиринга)	с 00:00:00 до 09:00:00 следующего рабочего дня
Направление Платежным клиринговым центром Участникам Реестра ПКЦ за операционный день, являющийся рабочим днем (операционные услуги, услуги платежного клиринга)	с 09:00:00 до 10:00:00 следующего рабочего дня
Направление Платежным клиринговым центром Участникам Реестра ПКЦ за операционный день, являющийся выходным и/или праздничным днем (операционные услуги, услуги платежного клиринга)	с 09:00:00 до 10:00:00 первого рабочего дня
Направление Платежным клиринговым центром в Расчетный центр Реестра распоряжений за операционный день, являющийся рабочим днем (операционные услуги, услуги платежного клиринга)	с 09:00:00 до 10:00:00 следующего рабочего дня
Направление Платежным клиринговым центром в Расчетный центр Реестра распоряжений за операционный день, являющийся выходным и/или праздничным днем (операционные услуги, услуги платежного клиринга)	с 09:00:00 до 10:00:00 первого рабочего дня
Осуществление расчётов по счетам Участников Расчетным центром (расчетные услуги)	с момента получения Реестра распоряжений до 17:00:00 дня получения Реестра распоряжений
Направление Расчетным центром в Платежный клиринговый центр подтверждения исполнения Реестра распоряжений (расчетные услуги, операционные услуги)	с 17:00:00 до 18:00:00 дня приема Реестра распоряжений
Направление Платежным клиринговым центром в Расчетный центр распоряжения при приостановлении участия Участника в Системе (операционные, услуги платежного клиринга)	с 09:00:00 до 18:00:00 дня принятия решения о приостановке участия Участника в Системе
Направление Расчетным центром в Платежный клиринговый центр подтверждения исполнения распоряжения, направленного в связи с приостановлением участия Участника в Системе (расчетные услуги)	с момента получения распоряжения до 23:59:29 дня получения распоряжения

7.4.5. Система функционирует круглосуточно без выходных и праздничных дней, за исключением времени, необходимого на осуществление технических, профилактических, ремонтных работ, а также работ, вызванных необходимостью устранения чрезвычайных обстоятельств, повлиявших на работоспособность Системы. В случае разового изменения времени операционного дня Оператор, выполняющий функции Операционного центра и Платежного клирингового центра, доводит соответствующую информацию по согласованным каналам связи до Участников.

7.4.6. Допускается отклонение в пределах тридцати минут от времени завершения (закрытия) операционного дня, время начала (открытия) следующего операционного дня сдвигается на величину отклонения времени закрытия предыдущего операционного дня в соответствующую сторону. Отклонение времени начала и/или завершения операционного дня в пределах установленного значения является нормальным, не требует специального уведомления Участников.

7.4.7. О проведении плановых технических, профилактических и ремонтных работ, проводимых не чаще, чем ежемесячно, Оператор, уведомляет Участников и привлеченных Операторов УПИ заранее, не позднее, чем за один рабочий день до даты начала проведения работ, путем информирования по согласованным каналам связи или путем опубликования на Официальном сайте Оператора в сети интернет. В уведомлении указываются дата и время начала проведения работ, предполагаемые дата и время окончания проведения работ.

7.4.8. О проведении внеплановых ремонтных работ, а также работ, вызванных необходимостью устранения чрезвычайных обстоятельств, повлиявших на работоспособность Системы, Оператор уведомляет Участников и привлеченных Операторов УПИ не позднее одного рабочего дня с даты начала проведения работ, путем информирования по согласованным каналам связи или путем опубликования на Официальном сайте Оператора в сети интернет. В уведомлении указываются предполагаемые дата и время окончания проведения работ.

7.4.9. В Системе допускаются технологические перерывы в оказании операционных и услуг платежного клиринга, которые устанавливаются Оператором на основании оценки допустимого уровня рисков. Общая продолжительность технологических перерывов в Системе не может превышать 48 часов в течение календарного года работы.

8. Порядок осуществления перевода денежных средств, включая моменты наступления безотзывности, безусловности и окончательности

8.1. Порядок осуществления перевода денежных средств

8.1.1. Прием/списание денежных средств Участником-отправителем от Отправителя может осуществляться наличными (только для Отправителей-физических лиц) или безналичными денежными средствами. Прием/списание осуществляются сотрудником Участника-отправителя в Пункте обслуживания или самостоятельно Плательщиком (Отправителем) в Устройствах приема платежей.

8.1.2. Участник-отправитель отказывает Отправителю в приеме его распоряжения к исполнению при недостаточности предоставленных денежных средств для осуществления перевода с учетом комиссии, подлежащей уплате Отправителем.

8.1.3. При отправке Переводу присваивается уникальный номер.

8.1.4. В случаях, предусмотренных законодательством страны регистрации Участника– отправителя, а также в случаях наличия требований Системы, приём от Отправителя денежных средств (списание с его счета) производится с обеспечением процессов идентификации Отправителя.

8.1.5. Участник-отправитель обязан предоставить Отправителю документ, подтверждающий осуществление перевода, и сведения о переводе в электронном виде, в том числе путем отправки на адрес электронной почты или на бумажном носителе.

8.1.6. Переводы денежных средств в Системе с использованием Электронных средств платежа через Устройства приема платежей осуществляются в следующем порядке:

- уполномоченное лицо Клиента Участника (в случае, если Клиент – юридическое лицо) или Клиент Участника (в случае, если Клиент – физическое лицо), являющееся Пользователем ЭСП, инициирует Операцию с использованием Устройства приема платежей;
- на основании инициированной Операции Устройством приема платежей формируется и передается Оператору, выполняющему функции Операционного центра, Авторизационный запрос разрешения проведения Операции;
- Оператор, выполняющий функции Операционного центра, определяет Участника и его Клиента, инициировавшего Операцию, осуществляет проверку достаточности

установленного Лимита ЭСП, а также достаточности Предельного размера (лимита) обязательств Участника;

- в случае если Предельный размер (лимит) обязательств Участника, а также Лимит ЭСП, являются достаточными для совершения Операции, Оператор, выполняющий функции Операционного центра, в зависимости от вида Устройства приема платежей либо подтверждает осуществление инициированной Пользователем ЭСП Операции, либо формирует положительный ответ на запрос и уменьшает доступный Лимит ЭСП, и доступный Предельный размер (лимит) обязательств Участника на сумму Операции, в противном случае формируется отказ в проведении Операции;

- расчет размера и проверка достаточности Лимита ЭСП и Предельного размера (лимита) обязательств Участника осуществляется в порядке, определенном Правилами;

- в случае, если Устройством приема платежей предусмотрено получение предварительного ответа на запрос после получения положительного ответа на запрос Пользователь ЭСП подтверждает намерение совершить Операцию и совершает действия, направленные на завершение Операции с использованием Устройства приема платежей, направляющего сообщение Оператору, выполняющему функции Операционного центра о положительном завершении Операции;

- по результатам положительного завершения Операции Пользователю ЭСП Устройством приема платежей формируется документ (на материальном носителе и/или в электронном виде), подтверждающий осуществление Операции.

8.1.7. При использовании для осуществления Операции ЭСП, Перевод денежных средств осуществляется в пределах Лимита ЭСП.

8.2. Эмиссия и обслуживание ЭСП

8.2.1. Эмиссия и обслуживание Банковских карт, осуществляется Участником на основании договоров, заключенных между Участником и его Клиентами-физическими или юридическими лицами, а также в соответствии с требованиями законодательства Российской Федерации и нормативными актами Банка России.

8.2.2. Регистрацию Клиента в ПК «КП РИТЕЙЛ» для дальнейшей эмиссии Банковской карты, осуществляет Участник, заключивший договор с Клиентом.

8.2.3. Для осуществления доступа Клиента к использованию Банковской карты Участник, заключивший с Клиентом договор, предоставляет Оператору данные Клиента, необходимые для регистрации Клиента в ПК «КП РИТЕЙЛ».

8.2.4. Клиент имеет возможность оформлять несколько Банковских карт у разных Участников.

8.2.5. Участник направляет Оператору Реестр Участника, содержащий сведения об эмитированных за день Банковских картах не позднее дня, следующего за датой эмиссии Банковской карты.

8.2.6. Деятельность Участника по обслуживанию Банковских карт, включает:

- предоставление Клиенту Банковской карты;
- предоставление Оператору данных о Клиенте для доступа Клиента к использованию Банковской карты в Системе;
- учет предоставленных Клиентом денежных средств;
- перевод денежных средств на основании распоряжений Клиента;
- осуществление других операций с использованием Банковской карты в порядке, предусмотренном договором между Клиентом и Участником.

8.2.7. Участник осуществляет свою деятельность в соответствии с требованиями законодательства по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

8.2.8. Договором между Участником и Клиентом может быть предусмотрено информирование Клиента о совершении каждой Операции с использованием ЭСП, в том

числе Банковской карты, путем направления Оператором, выполняющим функции Операционного центра от имени Участника Клиенту соответствующего уведомления.

8.3. Моменты наступления безотзывности, безусловности и окончательности Перевода

8.3.1. По Переводам, принятым в Системе в пользу юридических лиц, а также при наличии у Участника-исполнителя или у Получателя индивидуальных требований к информации, которая должна содержаться в Переводе, безусловность наступает на этапе введения данных операции в ПК «КП РИТЕЙЛ» Участником-отправителем (при отрицательном результате проверки перевод не принимается к исполнению).

8.3.2. Окончателность Перевода наступает в момент зачисления перевода денежных средств на Счет Участника-исполнителя.

8.3.3. Безотзывность переводов денежных средств в Системе наступает в момент предоставления Отправителем наличных денежных средств или списания денежных средств со счета Отправителя в целях осуществления перевода денежных средств.

8.3.4. При переводе денежных средств в Системе с использованием Электронных средств платежа момент наступления безусловности и безотзывности перевода денежных средств наступает при выдаче Устройством приема платежей документа (на материальном носителе и/или в электронном виде), подтверждающего осуществление операции по переводу денежных средств.

8.3.5. Списание Расчетным центром денежных средств со Счетов Участников в пользу Получателей по операциям по переводу денежных средств определяет момент наступления окончательности переводов денежных средств, совершенных в рамках Системы.

8.3.6. Возврат ошибочно уплаченных денежных средств осуществляется в Системе в общем порядке, предусмотренном действующим законодательством Российской Федерации.

8.4. Порядок сопровождения перевода денежных средств сведениями о Плательщике

8.4.1. Система предоставляет техническую возможность сопровождения Перевода сведениями о Плательщике в соответствии с требованиями законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения.

8.4.2. Участники самостоятельно несут ответственность за реализацию комплекса мер, направленных на предотвращение легализации (отмывания) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения, в т.ч. при сопровождении перевода денежных средств сведениями о Плательщике, а также ответственность за достоверность и полноту передаваемых сведений. Участник, у которого открыт банковский счет Плательщика, обязан обеспечить контроль за наличием, полноту, передачу Оператору, выполняющему функции Операционного центра и Платежного клирингового центра в составе расчетных документов или иным способом, а также хранение информации, предусмотренной законодательством Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения.

8.4.3. Оператор, выполняя функции Операционного центра и Платежного клирингового центра, обеспечивает контроль за наличием, полноту, передачу в составе расчетных документов или иным способом, соответствие сведениям, полученным от Участника и имеющимся в его распоряжении, а также хранение информации в соответствии с требованиями законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения.

8.4.4. В случае, если в распоряжении Участника не содержатся сведения о Плательщике в соответствии с требованиями законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения, Оператор, выполняя функции Операционного центра и Платежного клирингового центра, имеет право отказать в приеме в обработку распоряжения Участника.

8.4.5. Расчетный центр при осуществлении расчетов обеспечивает неизменность информации, содержащейся в полученном от Оператора, выполняющего функции Операционного центра и Платежного клирингового центра, распоряжении или Реестре распоряжений, и ее хранение в соответствии с требованиями законодательства Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения, а при отсутствии в распоряжении или неполучении иным способом указанной информации от Оператора или Участника обязан отказать в выполнении распоряжения Плательщика, либо самостоятельно осуществлять заполнение расчетных документов Плательщиков с использованием информации, полученной Участниками от Плательщиков, в том числе при осуществлении процедуры идентификации.

8.4.6. Если у Субъектов Системы, участвующих в переводе денежных средств, возникают подозрения, что операция по переводу денежных средств осуществляется в целях легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма или финансирования распространения оружия массового уничтожения, Субъект Системы обязан не позднее рабочего дня, следующего за днем признания данной операции подозрительной, направить в уполномоченный орган сведения о данной операции в соответствии с требованиями законодательства Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения.

8.5. Порядок оформления, формирования и отправки запроса на изменение реквизитов ранее отправленного Перевода

8.5.1. Порядок внесения изменений в реквизиты ранее отправленного Перевода определяется и доводится до сведения Отправителя Участником-отправителем самостоятельно.

8.5.2. Для внесения изменений в Перевод, направленный в пользу юридического лица-Клиента Участника Системы, Отправитель обращается к соответствующему юридическому лицу-Получателю или к кредитной организации/иностранному банку, в котором открыт счет Получателя, напрямую. В случае невозможности такого обращения Отправитель может направить Участнику-отправителю соответствующее заявление. При этом сама возможность внесения изменений в такой Перевод по Системе, а также порядок и сроки внесения изменений, определяются условиями информационно-технологического взаимодействия Оператора Системы с кредитной организацией/иностранным банком, в которых открыт счет Получателя.

8.5.3. Условием осуществления приема заявления на изменение реквизитов Операции для Отправителя-физического лица является предъявление Отправителем документа, подтверждающего факт совершения отправки, и, при необходимости, документов, подтверждающих его личность, что он является Отправителем.

8.5.4. Порядок взаимодействия Участника-отправителя с Отправителями, утерявшими документы, являющиеся подтверждением совершения Операции, определяется и доводится до сведения Отправителей Участником-отправителем самостоятельно.

8.5.5. Участник-отправитель, принявший заявление Отправителя на внесение изменений, обязан незамедлительно с момента его принятия направить запрос на изменение Оператору. В случае невозможности внесения изменений в Перевод по причине его зачисления на счет Получателя или в соответствии с условиями осуществления Перевода,

установленными Участником-получателем, Оператор обеспечивает невозможность передачи такого запроса программным способом.

8.5.6. Участник-отправитель уведомляет Отправителя о результатах обработки запроса.

8.5.7. Дополнительная комиссия за внесение изменений не взимается, если иное не оговорено в договорах с соответствующими юридическими лицами-Получателями, кредитными организациями, в которых открыты счета Получателей.

8.6. Отзыв, возврат (аннулирование) Переводов

8.6.1. Отзыв, возврат (аннулирование) Переводов осуществляется:

- по инициативе Участника-отправителя, в т.ч. на основании заявления Отправителя;

- при наступлении обстоятельств, делающих невозможной доставку денежных средств Получателю.

8.6.2. Аннулирование Переводов возможно до наступления их окончательности.

8.6.3. Заявление об отзыве Перевода принимается Участником при условии предъявления Отправителем документа, удостоверяющего личность, и сообщения им уникального номера перевода.

8.6.4. Заявление об отзыве перевода подается через тот же Пункт обслуживания Участника-отправителя, что и заявление на осуществление перевода.

8.6.5. При возврате денежных средств ранее уплаченная Клиентом Комиссия не подлежит возврату. Дополнительная комиссия за возврат денежных средств с Клиента не взимается.

8.6.6. В случае, если Участник в срок, указанный в п. 7.3.4 Правил не обеспечил поступление денежных средств на Счет Участника в размере, достаточном для осуществления расчетов по Операциям, принятым к исполнению Оператором, выполняющим функции Операционного центра и Платежного клирингового центра, то возврат принятого к исполнению распоряжения Плательщика/Участника осуществляется в порядке, приведенном в п.п. 7.3.5, 7.2.11 Правил.

8.6.7. При возврате принятого к исполнению распоряжения Плательщика по причине неисполнения Участником в срок, указанный в п. 7.3.4 Правил обязанности по обеспечению достаточности денежных средств на Счете Участника для расчетов по Операциям, принятым к исполнению Оператором, выполняющим функции Операционного центра и Платежного клирингового центра, Участник направляет Плательщику уведомление об аннулировании распоряжения Плательщика с соблюдением нормативных требований Банка России.

9. Порядок оплаты услуг по переводу денежных средств и услуг платежной инфраструктуры, услуг Оператора

9.1. Порядок оплаты услуг

9.1.1. Порядок оплаты услуг по переводу денежных средств, услуг платежной инфраструктуры в рамках Системы является едиными и единообразными для всех Участников и/или их Клиентов.

9.1.2. Порядок определения и уплаты Комиссии за перевод, оплаты услуг платежной инфраструктуры и услуг Оператора, предоставленные в рамках Системы, является неотъемлемой частью Тарифов.

9.1.3. Услуги Расчетного центра не тарифицируются Оператором и не включаются в Тарифы. Порядок оплаты услуг Расчетного центра определяется двусторонними договорами, заключаемыми с Оператором и Участниками.

9.1.4. В случаях, когда плательщиком Комиссии за перевод является Клиент, вознаграждение сверх суммы перевода взимается в полном объеме Участником, обслуживающим Клиента. Далее Участник уплачивает комиссионное вознаграждение Оператору за услуги платежной инфраструктуры, включая часть комиссионного вознаграждения Участник-исполнителя за осуществление перевода денежных средств.

9.1.5. Оператор осуществляет дальнейшее распределение комиссионного вознаграждения за перевод денежных средств:

- привлеченным Операторам УПИ за услуги платежной инфраструктуры;
- Участнику-исполнителю вознаграждение за осуществление перевода денежных средств.

9.1.6. Оператор вправе проводить маркетинговые акции путем установления комиссионного вознаграждения в рамках Системы с ограниченным сроком действия. Данные акции не являются действиями по изменению Тарифов. Информация о таких акциях доводится до Участников заблаговременно, в т.ч. по согласованным каналам связи. Оператор оставляет за собой право продлевать либо ограничивать срок действия акций неограниченное количество раз.

9.1.7. Оператор имеет право вносить изменения в Тарифы. При внесении изменений, предусматривающих введение новых Тарифов или увеличение размера Тарифов, Оператор обязан уведомить об этом Банк России с соблюдением срока, установленного законодательством Российской Федерации.

9.1.8. Оператор имеет право в одностороннем порядке менять размер оплаты услуг Операторов УПИ и размер комиссии, уплачиваемой Оператором Участникам за обслуживание Отправителей или Получателей в пределах Тарифов. При этом, информацию об изменениях размера комиссий, причитающихся Операторам платежной инфраструктуры и Участникам, Оператор обязуется направить заблаговременно, по согласованным каналам связи.

9.1.9. При использовании Участником при обслуживании Клиентов Устройств приема платежей, при привлечении банковских платежных агентов (субагентов), а также при осуществлении денежных переводов через определенные Пункты обслуживания, допускается установление Участником индивидуальных комиссий для Клиентов при условии предварительного согласования индивидуальных комиссий с Оператором.

9.1.10. Участник имеет право направить Оператору предложения с обоснованием внесения изменений в Тарифы с изменением ставок комиссионного вознаграждения.

9.1.11. Индивидуальные комиссии за перевод, устанавливаемые Участником сверх суммы, указанной в Тарифах без согласования с Оператором, не являются Тарифами Системы и признается нарушением Правил Системы.

9.1.12. При установлении Участником индивидуальных комиссий за перевод ниже Тарифов без внесения соответствующих изменений в Тарифы, Участник обязан оплачивать услуги платежной инфраструктуры и перечислять часть комиссионного вознаграждения Участника-исполнителя в полном объеме, предусмотренном Тарифами.

9.1.13. Тарифы, а также самостоятельно установленное Участником в соответствии с пп.9.1.12 Правил комиссионное вознаграждение доводятся до сведения Клиентов, обслуживаемых Участником в порядке, устанавливаемом Участником самостоятельно, но обязательно до момента совершения операции.

9.1.14. Оплата предоставленных Участнику и/или Клиентам Участника услуг, указанных в Тарифах, осуществляется в сроки, установленные в Тарифах, путем перевода денежных средств в сумме стоимости услуг со Счета Участника, на счет Оператора на основании распоряжения, передаваемого Оператором, выполняющего функции Платежного клирингового центра, Расчетному центру, на что Участник дает свое безусловное согласие. Получение дополнительного распоряжения Участника на осуществление указанного перевода не требуется.

Для осуществления расчетов за оказанные услуги в установленные в настоящем пункте сроки Участник обязан обеспечить на своем Счете Участника достаточность денежных средств, доступных для целей расчетов за оказанные услуги.

9.1.15. Расшифровка сумм, списанных со Счета Участника в качестве оплаты стоимости оказанных Участнику и/или Клиентам Участника услуг, приводится в акте об объеме предоставленных услуг, который предоставляется Оператором Участнику в срок не позднее пятого рабочего дня месяца, следующего за месяцем оказания услуг.

10. Управления рисками в Системе

10.1. Система управления рисками

10.1.1. Оператор совместно с Операторами УПИ и Участниками организует систему управления рисками, оценку и управление рисками в Системе (далее - управление рисками в Системе).

10.1.2. Система управления рисками направлена на поддержание принимаемых на себя Системой рисков на определенном уровне. Приоритетным является обеспечение надлежащего уровня БФПС. Под системой управления рисками в Системе понимается комплекс мероприятий и способов снижения вероятности возникновения неблагоприятных последствий для БФПС. Система управления рисками включает:

- организационную модель управления рисками;
- порядок обмена информацией, необходимой для управления рисками;
- мероприятия по управлению рисками;
- способы управления рисками.

10.1.3. Оператор определяет и соблюдает порядок обеспечения БФПС, который включает:

- управление рисками в Системе;
- управление непрерывностью функционирования Системы;
- организацию взаимодействия Субъектов Системы по обеспечению БФПС;
- контроль Оператора за соблюдением Операторами УПИ и Участниками Системы порядка обеспечения БФПС.

10.1.4. Оператор обеспечивает БФПС путем осуществления скоординированной с Операторами УПИ и Участниками Системы деятельности:

- по управлению рисками в Системе;
- по управлению непрерывностью функционирования Системы.

10.1.5. Субъекты Системы организуют деятельность по реализации порядка обеспечения БФПС в рамках внутренних систем управления рисками, присущими их деятельности.

10.1.6. Цель управления рисками, присущими деятельности Системы, достигается на основе системного, комплексного подхода, который подразумевает решение следующих задач:

- получение оперативных и объективных сведений о состоянии и размере рисков, присущих деятельности Системы;
- выявление и анализ рисков в процессе функционирования Системы;
- установление взаимосвязей между отдельными видами рисков с целью оценки воздействия мероприятий, планируемых для ограничения одного вида риска, на рост или уменьшение уровня других рисков;
- управление риском нарушения БФПС на стадии возникновения негативной тенденции, а также минимизация риска, путем создания системы быстрого и адекватного реагирования, направленной на предотвращение достижения рисками критических и значительных для Системы размеров.

10.2. Организационная модель управления рисками

10.2.1. Оператор самостоятельно управляет рисками в Системе. Модель управления рисками выбирается с учетом выполнения Оператором функций Операционного центра и Платежного клирингового центра, и представляет собой централизованную систему управления рисками, в которой Оператор самостоятельно определяет виды рисков, способы их мониторинга, анализа и оценки, процессы противодействия реализации рисков и т.д.

10.2.2. Расчетный центр и Участники в целях обеспечения бесперебойности функционирования Системы осуществляют мониторинг рисков и управление рисками, присущими их виду деятельности, в рамках внутренних систем управления рисками и несут ответственность за оперативное информирование Оператора о реализации указанных рисков и их последствиях, оказывающих непосредственное влияние на функционирование Системы

10.2.3. Оператор разрабатывает и утверждает в соответствии с требованиями нормативных актов Банка России локальные документы, которые определяют и детализируют мероприятия и способы управления рисками, предусматриваемые системой управления рисками в Системе.

10.2.4. Оператор проводит оценку рисков в Системе не реже одного раза в год с использованием методик анализа рисков в Системе, включая профили рисков.

10.2.5. Участники, привлеченные ОУПИ самостоятельно осуществляют деятельность:

- по мониторингу рисков, присущих их виду деятельности;
- по управлению рисками, присущими их виду деятельности, и несут ответственность за последствия реализации указанных рисков, за оперативное информирование Оператора о реализации указанных рисков и их последствиях, оказывающих непосредственное влияние на функционирование Системы;
- по реализации порядка обеспечения бесперебойности функционирования Системы (БФПС) в рамках внутренних систем управления рисками своей деятельности в части обслуживания клиентов—физических и юридических лиц, в т.ч. банков—корреспондентов;
- по обеспечению защиты информации, в т.ч. при осуществлении своей деятельности в рамках Системы;
- по обеспечению надлежащего функционирования операционных и технологических средств, устройств, информационных систем, используемых ими в работе с Системой;
- по обеспечению и контролю соблюдения Правил Системы, заключенных договоров с Оператором, Расчетным центром (для Участников), требований законодательства Российской Федерации;
- по контролю соблюдения привлеченными БПА, банковскими платежными субагентами (далее – БПС) условий их привлечения Участниками, а также законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения;
- по разработке необходимых внутренних нормативных документов по управлению рисками и обеспечению непрерывности функционирования Системы в соответствии с требованиями законодательных, нормативных документов, Правил и рекомендаций Оператора.

10.2.6. Оператор предъявляет следующие требования к управлению рисками Участниками, привлеченными ОУПИ в рамках Системы:

- Участники поддерживают на счетах для расчетов в Системе остаток денежных средств, достаточный для бесперебойного проведения операций и расчетов, предпринимают меры для соблюдения порядка и своевременности расчетов.

- Участники, привлеченные ОУПИ соблюдают требования к защите информации, указанные в п. 13.2 Правил.
- Участники, привлеченные ОУПИ обеспечивают надлежащее функционирование операционных и технологических средств, устройств, информационных систем, используемых ими при работе с Системой.
- Участники, привлеченные ОУПИ самостоятельно обеспечивают управление рисками в собственной деятельности, в том числе разрабатывают необходимые методики в соответствии с требованиями законодательства Российской Федерации, нормативными требованиями Банка России и настоящими Правилами.
- Участники, привлеченные ОУПИ разрабатывают и соблюдают Планы ОНиВД.
- Участники, привлеченные ОУПИ соблюдают порядок информационного взаимодействия в рамках Системы в соответствии с Правилами.
- Участники, привлеченные ОУПИ предоставляют внутренние документы по управлению рисками и обеспечению БФПС по запросу Оператора для проверки их наличия и соответствия законодательным актам, нормативным документам Банка России и требованиям Правил.

10.3. Порядок обмена информацией, необходимой для управления рисками

10.3.1. В целях управления рисками Оператор вправе запрашивать и получать от Участников и привлеченных ОУПИ информацию, необходимую для управления рисками, а также систематизировать, обрабатывать, накапливать и хранить такую информацию.

10.3.2. Оператор определяет состав, периодичность, форму предоставляемой информации, а также функции, выполняемые Операторами УПИ по оперативному информированию Оператора о нарушении оказания услуг платежной инфраструктуры (далее – УПИ), соответствующего требованиям к оказанию услуг, при котором превышено время восстановления оказания УПИ в случае их приостановления и (или) время восстановления оказания УПИ, соответствующего требованиям к оказанию услуг.

10.3.3. В случае если запрашиваемая информация содержит сведения, составляющие коммерческую тайну, Оператор обязуется обеспечить конфиденциальность такой информации в соответствии с требованиями законодательства Российской Федерации и не предоставлять её третьим лицам за исключением случаев, предусмотренных требованиями законодательства Российской Федерации.

10.3.4. Запрашиваемая информация может касаться вопросов:

- защиты информации;
- мер по поддержанию бесперебойности функционирования Субъекта Системы;
- финансового состояния и выполнения требований Банка России (для кредитных организаций);
- выполнения Правил;
- выполнения требований законодательства, в т.ч. в сфере противодействия легализации преступных доходов, финансированию терроризма и финансированию распространения оружия массового уничтожения.

10.3.5. Участники, привлеченные ОУПИ при возникновении событий, не связанных с БФСР, но способных повлиять на уровень рисков Системы, предоставляют информацию Оператору по каждому инциденту в соответствии с пп. 11.2.4 Правил.

10.3.6. Участники, привлеченные ОУПИ при возникновении событий, вызвавших спорные, нестандартные и чрезвычайные ситуации, включая системные сбои, а также неисполнение или ненадлежащее исполнение обязательств Участников доводят до сведения Оператора информацию о таких событиях.

10.3.7. При возникновении угрозы нарушения бесперебойности функционирования Системы информация, указанная в п.п. 10.3.6 Правил, незамедлительно предоставляется Оператору по согласованным каналам связи. Участникам и привлеченным ОУПИ следует руководствоваться при этом порядком информирования и взаимодействия, определенным в пп.6.12.1 Правил.

10.3.8. О событиях, вызвавших спорные, нестандартные и чрезвычайные ситуации, включая системные сбои, а также неисполнение или ненадлежащее исполнение обязательств Участников, не повлиявших на БФПС, Участники и привлеченные ОУПИ сообщают Оператору по согласованным каналам связи не позднее третьего рабочего дня месяца, следующего за месяцем наступления события.

10.3.9. Участники, привлеченные ОУПИ по запросу Оператора предоставляют Оператору информацию о своей деятельности в виде финансовых отчетов (в том числе: баланс, расчет обязательных экономических нормативов, расчет собственных средств и отчет о прибылях и убытках).

10.3.10. Информация может предоставляться по электронной почте, либо путем публикации отчетности на официальных сайтах Участников, привлеченных ОУПИ, сайте Банка России, либо направляется в электронном виде по запросу Оператора по согласованным каналам связи.

10.3.11. Оператор вправе использовать информацию:

- из открытых, доступных источников, в т.ч. СМИ, сайты национальных центральных банков стран Участников, сайты Участников, привлеченных ОУПИ, систем агрегирования данных, рейтинговых агентств;
- автоматизированного контроля, осуществляемого Оператором.

10.3.12. Оператор обязуется предоставлять Участникам, привлеченным ОУПИ информацию, необходимую для управления рисками в Системе как по собственной инициативе, так и по запросу последних.

10.3.13. Информация, касающаяся обеспечения защиты информации, пересмотра Планов ОНВД Участника, привлеченного Оператора УПИ, а также оценки качества функционирования операционных и технологических средств и информационных систем привлеченного Оператора УПИ, предоставляется по запросу Оператора, но не реже 1 раза в два года. Форма предоставления информации определяется Оператором самостоятельно.

10.4. Мероприятия по управлению рисками

10.4.1. Система управления рисками состоит из комплекса мероприятий по определению:

- организационной структуры управления рисками, обеспечивающей контроль выполнения Участниками требований к управлению рисками, установленных Правилами;
- функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений Оператора;
- показателей бесперебойности функционирования Системы (показатели БФПС) и значений их пороговых уровней в соответствии с требованиями нормативных актов Банка России;
- порядка обеспечения БФПС;
- методик анализа рисков в Системе, включая определение профиля рисков, в соответствии с требованиями нормативных актов Банка России, а также способы управления рисками;
- порядка обмена информацией между Субъектами Системы, необходимой для управления рисками;

- порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев;
 - уровней оказания услуг платежной инфраструктуры, характеризующих качество функционирования операционных и технологических средств платежной инфраструктуры (далее – уровни оказания услуг платежной инфраструктуры);
 - порядка изменения операционных и технологических средств и процедур;
 - порядка оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией;
 - порядка обеспечения защиты информации в Системе.
- а также включает:
- доведение до органов управления Оператора соответствующей информации о рисках;
 - управление непрерывностью и порядок обеспечения бесперебойности функционирования Системы, отраженных в разделе 11 Правил;
 - установление требований к содержанию деятельности по обеспечению бесперебойности функционирования Системы, осуществляемой Субъектами Системы;
- взаимодействие Субъектов Системы при реализации мероприятий по управлению рисками и управлению непрерывностью функционирования Системы.

10.5. Способы управления рисками

10.5.1. Оператор определяет способы управления рисками в Системе исходя из способов управления рисками, предусмотренных частью 5 статьи 28 Закона о НПС. Способы управления рисками определяются Оператором с учетом особенностей организации Системы, модели управления рисками, процедур платежного клиринга и расчета, количества переводов денежных средств и их сумм, времени окончательного расчета.

10.5.2. В целях управления рисками в Системе по решению Оператора может быть создан гарантийный фонд Системы в порядке, предусмотренном законодательством Российской Федерации и нормативными актами Банка России.

10.5.3. Система управления рисками предусматривает следующие способы управления рисками:

- осуществление расчета в пределах, предоставленных Участником денежных средств (в пределах доступного остатка), если иное дополнительно не установлено Оператором в отношении Участника;
- осуществление расчетов в Системе до конца рабочего дня;
- установление Оператором предельных размеров (лимитов) обязательств Участников с учетом уровня риска;
- осуществление Оператором мониторинга выполнения Субъектами Системы требований к управлению непрерывностью функционирования Системы, и разработка в случае необходимости рекомендаций, в целях повышения ими эффективности управления;
- управление очередностью исполнения распоряжений Участников, обеспечивающее завершение расчетов по операциям, совершенным в рамках Системы, в приоритетном порядке, в пределах допустимых законодательством Российской Федерации;
- осуществление Оператором мониторинга соответствия деятельности Субъектов Системы законодательству Российской Федерации и Правилам;
- разработка Субъектами Системы Планов ОНиВД, содержащих комплекс мер, реализуемый в повседневной деятельности, обеспечивающий подготовку к

чрезвычайным и нестандартным ситуациям и обеспечения бесперебойности деятельности Системы;

- право Оператора на приостановление, в том числе с последующим прекращением участия Участника в Системе в случаях, предусмотренных Правилами.

10.5.4. В целях управления рисками Оператор может проводить анализ и изучение финансовой отчетности, других сведений и документов Участников, привлеченных Операторов УПИ, осуществлять контроль и фиксирование параметров их деятельности в Системе, включая соблюдение порядка расчетов, а также анализировать и изучать информацию о Системе и ее Субъектах в средствах массовой информации.

10.5.5. На основании анализа параметров, с использованием которых Оператор производит оценку функционирования Системы, и иных данных, аккумулируемых Оператором и получаемых от остальных Субъектов Системы в установленном в Правилах порядке, Оператор:

- выявляет закономерности функционирования Системы;
- проводит анализ и оценку рисков, присущих деятельности Системы;
- осуществляет разделение инцидентов на не способные оказать влияние на БФПС и на способные оказать влияние на БФПС, в том числе приводящие к нарушению БФПС (приостановлению оказания услуг платежной инфраструктуры);
- вырабатывает рекомендации по снижению уровней рисков, присущих деятельности Системы;
- принимает меры и решения, направленные на исключение (минимизацию) выявленных возможностей нарушений надлежащего функционирования Системы.

10.6. Виды рисков, присущих деятельности Системы

10.6.1. Деятельности Системы присущи следующие виды рисков:

- правовой риск – риск нарушения БФПС и ненадлежащего оказания услуг платежной инфраструктуры вследствие несоблюдения Субъектами Системы требований законодательства Российской Федерации, Правил, договоров, заключенных между Субъектами Системы, внутренних нормативных документов Оператора и внутренних нормативных документов привлеченных Операторов УПИ либо вследствие наличия правовых коллизий и (или) правовой неопределенности в законодательстве Российской Федерации, нормативных актах Банка России, Правилах и договорах, заключенных между Субъектами Системы, а также вследствие нахождения привлеченных Операторов УПИ и Участников под юрисдикцией различных государств;
- операционный риск – риск нарушения БФПС и ненадлежащего оказания услуг платежной инфраструктуры вследствие возникновения у Субъектов Системы сбоев, отказов и аварий в работе информационных и технологических систем, недостатков в организации и выполнении технологических и управленческих процессов, ошибок или противоправных действий персонала Субъектов Системы либо вследствие воздействия событий, причины возникновения которых не связаны с деятельностью Субъектов Системы, включая чрезвычайные ситуации, ошибочные или противоправные действия третьих лиц;
- кредитный риск – риск ненадлежащего оказания услуг платежной инфраструктуры Расчетным центром вследствие невыполнения Участником или Участниками договорных обязательств перед Расчетным центром в установленный срок или в будущем;
- риск ликвидности – риск нарушения БФПС и ненадлежащего оказания услуг платежной инфраструктуры вследствие отсутствия у Участников денежных

средств, достаточных для своевременного выполнения их обязательств перед другими Субъектами Системы;

- общий коммерческий риск (системный риск) – риск нарушения БФПС и ненадлежащего оказания услуг платежной инфраструктуры вследствие уменьшения доходов и (или) увеличения расходов, ухудшения финансового состояния Оператора и (или) привлеченного Операторов УПИ, не связанного с реализацией кредитного риска Системы и риска ликвидности Системы;
- риск нарушения БФПС – риск приостановления (прекращения) осуществления переводов денежных средств или надлежащего функционирования Системы, а также невозможность восстановления оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, и восстановления оказания услуг платежной инфраструктуры в случае приостановления их оказания в течение периодов времени, установленных Оператором в Правилах, вследствие неблагоприятного стечения обстоятельств – возникновения инцидентов в деятельности Субъектов Системы.

10.7. Методики анализа рисков в Системе

10.7.1. Выявление и анализ рисков в Системе проводится Оператором с применением элементов методик в соответствии с ГОСТ Р ИСО/МЭК 31010-2011. Национальный стандарт Российской Федерации. Менеджмент риска. Методы оценки риска» (далее – Стандарт) и предусматривает, в том числе:

- сбор, фиксирование, отслеживание и анализ параметров работы Участников в Системе, в т. ч. анализ соблюдения порядка расчетов согласно Правил;
- накопление и статистический анализ информации о нестандартных, спорных и чрезвычайных ситуациях, а также иных событий реализации рисков Системы;
- оценка и ретроспективный анализ данных мониторинга показателей БФПС с целью выявления закономерностей и выработки мер по улучшению функционирования Системы.

10.7.2. Методики анализа рисков в Системе (далее - методики) обеспечивают:

- выявление и анализ рисков в Системе, включая выявление риск-событий, и определение для каждого из выявленных риск-событий величины риска, характеризующего вероятностью наступления риск-событий и величиной возможных последствий их реализации (далее - уровень риска);
- определение для каждого из выявленных рисков в Системе уровня риска, имеющегося до применения способов управления рисками в Системе (далее - уровень присущего риска), а также максимального уровня риска, при котором восстановление оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, включая восстановление оказания услуг платежной инфраструктуры в случае приостановления их оказания, осуществляется в течение периодов времени, установленных Оператором, и предполагаемый ущерб от которого Оператор готов принять без применения способов управления рисками в Системе (далее - уровень допустимого риска);
- определение рисков в Системе, для которых уровень присущего риска выше уровня допустимого риска (далее - значимые для Системы риски);
- определение уровня каждого из значимых для Системы рисков после применения способов управления рисками в Системе (далее - уровень остаточного риска).

10.7.3. Методики предусматривают выполнение следующих мероприятий:

а. Идентификация риска – выявление риска, определение его причин и предпосылок, которое включает в себя:

- формирование и поддержание в актуальном состоянии перечней бизнес-процессов;

- разработка и поддержание в актуальном состоянии классификаторов (структурированных перечней) рисков в Системе, риск-событий, причин риск-событий;
- проведение анализа бизнес-процессов в Системе, включая анализ и оценку технологического обеспечения привлеченных Операторов УПИ и других факторов, влияющих на БФПС;
- формирование перечня возможных риск-событий для каждого бизнес-процесса с указанием причин риск-событий и их последствий.

б. Анализ и оценка риска – анализ информации, полученной в результате идентификации риска, определение вероятности наступления и последствий риск-событий, который включает в себя:

- определение уровня присущего риска для каждого из выявленных рисков в Системе и установление уровня допустимого риска;
- сопоставление определенного уровня присущего риска и установленного уровня допустимого риска по каждому из выявленных рисков в Системе для выделения значимых для Системы рисков;
- применение способов управления рисками в Системе для каждого из значимых для Системы рисков и последующее определение уровня остаточного риска для каждого из значимых для Системы рисков;
- сопоставление уровней остаточного риска и допустимого риска для каждого из значимых для Системы рисков и принятие решения о необходимости применения других способов управления рисками в Системе в дополнение к ранее примененным способам.

в. Мониторинг уровня риска – выявление событий, способствующих изменению степени подверженности риску, уровня риска, отслеживание динамики характеризующих уровень риска показателей с целью выявления отклонений и определению тенденций в изменении уровня риска, которые включают в себя:

- мониторинг рисков в Системе, в том числе уровней остаточных рисков в Системе, их соответствия уровню допустимого риска;
- составление и пересмотр (актуализацию) по результатам оценки рисков в Системе и анализа эффективности мероприятий по восстановлению оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, профиля каждого из выявленных рисков в Системе, включая профиль риска нарушения БФПС.

10.7.4. Составление профилей рисков, включая профиль риска нарушения БФПС, осуществляется в соответствии с законодательством Российской Федерации и нормативными актами Банка России, а также с учетом следующих требований:

- особенностей структуры Системы;
- условий и способов проведения расчетов;
- количественных характеристик потоков расчетных документов;
- распределения прав, ответственности и обязанностей Субъектов Системы.

Профили рисков составляются по всем выявленным рискам в Системе.

Профиль риска нарушения БФПС составляется в отношении значимых для Системы рисков.

В случае возникновения инцидента, приведшего к приостановлению оказания услуг платежной инфраструктуры, который не отражен в профилях рисков как риск-событие, профили рисков подлежат пересмотру (актуализации) в срок, не превышающий трех месяцев со дня возникновения данного инцидента.

Пересмотр (актуализация) профилей рисков производится структурным подразделением (работником) Оператора, ответственным за управление рисками, присущими деятельности Системы по мере необходимости, но не реже одного раза в год.

Оператор хранит сведения, содержащиеся в профилях рисков, не менее трех лет со дня составления и пересмотра (актуализации) профилей рисков.

10.7.5. Оператор в рамках системы управления рисками разрабатывает методику анализа рисков в Системе в соответствии с вышеуказанными требованиями. Операторы услуг платежной инфраструктуры, и Участники самостоятельно разрабатывают свою методику анализа рисков. Оператор вправе рекомендовать Операторам услуг платежной инфраструктуры и Участникам взять за основу методику Оператора.

10.7.6. Оценка эффективности методики анализа рисков осуществляется на основании данных, представляемых Операторами услуг платежной инфраструктуры и Участниками, в том числе, по запросу Оператора.

10.8. Порядок проведения оценки рисков и мониторинг рисков в Системе

10.8.1. Оценка рисков в Системе проводится структурным подразделением (работником) Оператора, ответственным за управление рисками, присущими деятельности Системы по мере необходимости, но не реже одного раза в год с использованием методик, включая профили рисков.

10.8.2. Контроль за состоянием рисков осуществляется Оператором посредством проведения на постоянной основе мониторинга рисков в Системе. В ходе мониторинга осуществляется проведение следующих мероприятий:

- сбор и анализ первичной информации о функционировании Системы, включая информацию об инцидентах;
- расчет показателей БФПС;
- выявление изменений профилей рисков;
- проверка соответствия результатов оценки риска, включая риск нарушения БФПС, фактической информации о риске;
- контроль соблюдения операторами УПИ уровней оказания услуг платежной инфраструктуры;
- оценка влияния на БФПС инцидентов, возникших в деятельности Субъектов Системы;
- инициирование принятия мер, необходимых для достижения допустимого уровня рисков, включая риск нарушения БФПС.

10.9. Организационная структура системы управления рисками

10.9.1. Оператор определяет собственную структуру управления рисками и функциональные обязанности лиц в соответствующих структурных подразделениях, ответственных за управление рисками в Системе. По осуществлению управления рисками устанавливается разграничение ответственности и полномочий между Субъектами Системы.

10.9.2. Организационная структура органов управления рисками Оператора включает:

- единоличный исполнительный орган Оператора;
- структурное подразделение (работника) Оператора, ответственное за управление рисками, присущими деятельности Системы.

10.9.3. Функциональные обязанности и компетенция единоличного исполнительного органа Оператора включает, в том числе, следующее:

- утверждение Правил;
- утверждение формата распоряжений, Реестра Участника, Реестра ПКЦ, Реестра распоряжений, используемых в Системе;

- утверждение форматов сообщений, используемых в Системе;
- утверждение порядка эмиссии и обслуживания ЭСП, используемых для осуществления Операций;
- утверждение внутренних документов, регулирующих систему управления рисками, в том числе «Порядка бесперебойности функционирования и анализа рисков платежной системы «КП Ритейл»;
- обеспечение условий для эффективной реализации политики в сфере управления рисками;
- определение структурных подразделений (работника) Оператора, ответственного за управление рисками, присущими деятельности Системы;
- утверждение Плана ОНиВД;
- обеспечение принятия организационных решений по вопросам управления рисками в Системе;
- утверждение критериев оценки системы управления рисками, в том числе используемых методов оценки рисков;
- утверждение профилей рисков, присущих деятельности Системы;
- утверждение допустимых уровней рисков, присущих деятельности Системы;
- принятие мер по обеспечению бесперебойности функционирования Системы и минимизации уровня рисков;
- установление предельных размеров (лимитов) обязательств Участников с учетом уровня рисков;
- рассмотрение отчетов о состоянии рисков, присущих деятельности Системы, и системы управления рисками в целом;
- контроль за выполнением мероприятий по управлению рисками;
- утверждение отчета об оценке системы управления рисками в Системе, в том числе, используемых методов оценки рисков в Системе, результатов применения способов управления рисками в Системе, не реже одного раза в два года и документальное оформление результатов указанной оценки;
- внесение изменений в систему управления рисками в Системе в случае, если действующая система управления рисками в Системе не позволила предотвратить нарушение оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, а также восстановить оказание услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, и (или) восстановить оказание услуг платежной инфраструктуры в случае приостановления их оказания в течение периодов времени, установленных Оператором в Правилах; проведение оценки эффективности системы управления рисками Системы и ее совершенствование.
- иные функции, установленные законодательством Российской Федерации, нормативными актами Банка России, Правилами.

10.9.4. Функциональные обязанности структурного подразделения (работника) Оператора, ответственного за управление рисками, присущими деятельности Системы включает, в том числе, следующее:

- разработка внутренних документов, регулирующих систему управления рисками в Системе и порядка обеспечения БФПС;
- проведение оценки системы управления рисками в Системе, в том числе, используемых методов оценки рисков в Системе, результатов применения способов управления рисками в Системе, не реже одного раза в два года и документальное оформление результатов указанной оценки;

- анализ первичной информации о функционировании Системы;
- анализ показателей уровней оказания услуг платежной инфраструктуры;
- анализ сведений об инцидентах, в целях определения их влияния на БФПС. Инцидентом является событие, которое привело к нарушению оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, в том числе вследствие нарушений требований к обеспечению защиты информации при осуществлении переводов денежных средств, в результате которых приостанавливалось оказание услуг платежной инфраструктуры и/или нарушался регламент выполнения процедур (время начала, время окончания, продолжительность и последовательность процедур, выполняемых Операторами УПИ при оказании операционных услуг, услуг платежного клиринга и расчетных услуг, предусмотренных временным регламентом функционирования Системы, установленным Правилами);
- анализ нестандартных ситуаций с целью выявления возможных дополнительных рисков в Системе;
- расчет, анализ и мониторинг показателей БФПС;
- проведение мониторинга и оценки рисков, присущих деятельности Системы, включая системный риск (общий коммерческий риск Системы);
- проведение оценки рисков в Системе с использованием методик анализа рисков в Системе, включая профили рисков по мере необходимости, но не реже одного раза в год;
- разработка мер по минимизации рисков в Системе;
- информирование единоличного исполнительного органа Оператора о выявлении факторов, указывающих на реализацию риска нарушения БФПС;
- информирование единоличного исполнительного органа Оператора о состоянии рисков;
- контроль актуальности состояния перечней бизнес-процессов;
- контроль актуальности состояния классификаторов (структурированных перечней) рисков в Системе, событий, реализация которых может привести к возникновению инцидентов (далее – риск-событие), причин риск-событий;
- вынесение на рассмотрение единоличным исполнительным органом Оператора предложений по предупреждению возникновения, устранению и минимизации риск-событий, могущих повлечь реализацию риска нарушения БФПС;
- анализ подверженности рискам бизнес-процессов Системы - взаимосвязанных, последовательных технологических процедур, выполняемых при оказании услуг платежной инфраструктуры (далее – бизнес-процесс);
- составление и пересмотр (актуализация) профилей рисков, присущих деятельности Системы;
- разработка и вынесение на обсуждение единоличным исполнительным органом Оператора мер, необходимых для достижения допустимых уровней рисков, включая риск нарушения БФПС;
- участие в разработке новых продуктов, внедрении новых технологий, освоении новых направлений деятельности с целью своевременного отслеживания возникновения рисков на стадии внедрения и принятия мер по их минимизации;
- инициирование внесения изменений в систему параметров, на основании которых производится оценка функционирования Системы;

- организация обмена информацией о рисках и мерах по управлению ими между структурными подразделениями Оператора, Участниками и привлеченными Операторами УПИ;
- иные функции, установленные законодательством Российской Федерации, нормативными актами Банка России, Правилами.

10.9.5. Участники и привлеченные ОУПИ определяют должностных лиц и/или структурные подразделения, к обязанностям которых относится обеспечение мониторинга и проведение мероприятий, связанных с управлением рисками, присущими их деятельности. Информация о вышеуказанных лицах (фамилия, имя, отчество, должность, контактные данные), а также любые связанные с ними изменения Участники и привлеченные ОУПИ предоставляют Оператору по согласованным каналам связи самостоятельно и по запросам Оператора.

10.9.6. В целях систематизации информации о состоянии рисков в Системе, получения своевременных и актуальных сведений, используемых Оператором для принятия соответствующих управленческих решений и формирования достоверной отчетности, Оператором может быть создана информационная система состояния рисков в Системе.

Информационная система состояния рисков в Системе базируется на:

- постоянстве функционирования информационной системы и непрерывности передачи информации;
- достоверности и своевременности размещения в информационной системе информации;
- удобстве использования информационной системы;
- обеспечении доступа к информационной системе сотрудников, участвующих в управлении рисками Системы и органов управления Оператора;
- обеспечении защиты информационной системы от несанкционированного доступа.

10.10. Доведение до органов управления Оператора информации о рисках

10.10.1. В целях доведения до органов управления Оператора сведений о рисках информация о выявленных рисках незамедлительно предоставляется сотрудником подразделения (работником) Оператора, ответственного за управление рисками, присущими деятельности Системы, единоличному исполнительному органу Оператора.

10.10.2. Информация об общем уровне рисков Системы, о результатах оценки эффективности системы управления рисками Системы, предложения по её совершенствованию доводится до сведения участников Оператора не реже одного раза в год.

10.10.3. Участники, привлеченные ОУПИ самостоятельно разрабатывают процедуры доведения информации, необходимой для управления рисками до своих органов управления и Оператора, с учетом положений Правил.

10.10.4. Участники и привлеченные ОУПИ, незамедлительно информируют по согласованным каналам связи Оператора Системы о любых фактах реализации рисков, способных повлиять на бесперебойность функционирования Системы.

11. Управление непрерывностью и порядок обеспечения бесперебойности функционирования Системы

11.1. Общие положения по обеспечению бесперебойности функционирования Системы

11.1.1. Оператор совместно с Операторами УПИ и Участниками организует выявление оказания услуг платежной инфраструктуры, не соответствующего требованиям Закона о НПС и принятых в соответствии с ним нормативных актов Банка России, а также положениям Правил, договоров об оказании услуг платежной инфраструктуры, внутренних организационно-распорядительных документов Оператора и привлеченных им Операторов

УПИ (далее – требования к оказанию услуг), обеспечению функционирования Системы в случае нарушения оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, и восстановлению оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, включая восстановление оказания услуг в случае приостановления их оказания в течение периодов времени, установленных Оператором (далее - управление непрерывностью функционирования Системы).

Оператор координирует деятельность Субъектов Системы по обеспечению БФПС.

11.1.2. В Системе БФПС достигается при условии:

- оказания Участникам услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг;
- надлежащего функционирования Системы;
- восстановления оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг и восстановления оказания услуг платежной инфраструктуры в случае приостановления их оказания в течение периодов времени, установленных Оператором в Правилах.

11.1.3. Продолжительность периодов времени, в течение которых должно быть восстановлено надлежащее функционирование Системы в случае его нарушения, в том числе в случае приостановления (прекращения) оказания услуг платежной инфраструктуры, в том числе при возникновении инцидентов, устанавливается в следующих пределах:

- восстановление надлежащего функционирования платежной системы – не более 72 часов;
- возобновление осуществления переводов денежных средств в случае его приостановления (прекращения) с момента приостановления (прекращения) – не более 6 часов.

11.1.4. В целях обеспечения БФПС Оператор определяет в качестве структурного подразделения (работника), ответственного за осуществление деятельности, предусмотренной Правилами в части обеспечения БФПС структурное подразделение (сотрудника), ответственное за управление рисками, присущими деятельности Системы.

11.1.5. Оператор, привлеченные Операторы УПИ, Участники при обеспечении ими БФПС обязаны соблюдать требования, установленные действующим законодательством Российской Федерации, нормативными актами Банка России и Правилами.

11.1.6. Субъекты Системы используют Правила, внутренние нормативные документы Субъекта Системы (при наличии), разработанные с целью обеспечения непрерывности осуществляемой деятельности, в том числе осуществляемой в рамках Системы. При разработке внутренней нормативной документации по обеспечению БФПС Субъекты Системы руководствуются требованиями законодательства Российской Федерации и нормативных актов Банка России.

11.1.7. Каждый Субъект Системы несет индивидуальную ответственность за невыполнение и несоблюдение мер по обеспечению БФПС, закрепленных в Правилах.

11.1.8. Порядок и формы координации деятельности Субъектов Системы по обеспечению БФПС и реализации ими мероприятий системы управления рисками платежной системы заключаются в публикации Правил.

11.2. Управление непрерывностью и порядок осуществления деятельности по обеспечению бесперебойности

11.2.1. Оператор управляет непрерывностью функционирования Системы с учетом следующих требований.

Оператор организует деятельность по управлению непрерывностью функционирования Системы, в том числе путем установления прав и обязанностей Субъектов Системы по управлению непрерывностью функционирования Системы в зависимости от организационной модели управления рисками в платежной системе, определенной в соответствии с

требованиями части 2 статьи 28 Закона о НПС и указанной в Правилах. В соответствии с Правилами организационная модель управления рисками в Системе предусматривает распределение функций между Участниками, Оператором, привлеченными ОУПИ.

11.2.2. Оператор системы организует деятельность по управлению непрерывностью функционирования Системы, которая включает в себя следующие мероприятия:

- планирование и координацию ресурсов;
- определение подхода к восстановлению оказания услуг платежной инфраструктуры;
- принятие мер по предотвращению, обнаружению, подготовке к чрезвычайным и нестандартным ситуациям, уменьшению степени их воздействия;
- распределение прав и обязанностей Субъектов Системы по управлению непрерывностью функционирования Системы;
- сбор и обработку сведений, в том числе от привлеченных Операторов УПИ, используемых для расчета показателей БФПС, а также сведений об инцидентах;
- проведение контроля соблюдения Субъектами Системы регламента выполнения процедур;
- реализацию мероприятий и способов достижения и поддержания допустимого уровня риска нарушения БФПС, включая проведение оценки их эффективности;
- организацию разработки и контроля наличия планов ОНиВД у привлеченных Операторов УПИ;
- установление системы параметров, на основании которых производится оценка функционирования Системы;
- координацию и контроль деятельности Субъектов Системы по обеспечению БФПС.

11.2.3. Оператор анализирует эффективность мероприятий по восстановлению оказания услуг платежной инфраструктуры, соответствующего надлежащему функционированию Системы, и использует полученные результаты при управлении рисками в Системе. Анализ эффективности мероприятий по восстановлению оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, осуществляет структурное подразделение (сотрудник) Оператора, ответственное за управление рисками, присущими деятельности Системы. Результаты мониторинга ежегодно оформляются в виде отчета и направляются не позднее последнего числа первого месяца года, следующего за отчетным, на рассмотрение единоличному исполнительному органу Оператора.

11.2.4. Оператор организует сбор и обработку сведений, в том числе от привлеченных Операторов услуг платежной инфраструктуры, используемых для расчета показателей БФПС, указанных в пп.11.3.4 Правил (далее - сведения по Платежной системе), а также следующих сведений об инцидентах:

- время и дата возникновения инцидента (в случае невозможности установить время возникновения инцидента указывается время его выявления);
- краткое описание инцидента (характеристика произошедшего события и его последствия);
- наименование взаимосвязанных последовательных технологических процедур, выполняемых при оказании услуг платежной инфраструктуры (далее - бизнес-процесс), в ходе которых произошел инцидент;
- наименование бизнес-процесса, на который оказал влияние инцидент;
- наличие (отсутствие) факта приостановления (прекращения) оказания услуг платежной инфраструктуры в результате инцидента;
- влияние инцидента на БФПС, определяемое с учетом требований, предусмотренных настоящим пунктом Правил;
- степень влияния инцидента на функционирование Системы в зависимости от количества Операторов услуг платежной инфраструктуры, и (или) количества и

значимости Участников Системы, на которых оказал непосредственное влияние инцидент, и (или) количества и суммы неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных распоряжений Участников Системы, и иных факторов;

- время и дата восстановления оказания услуг платежной инфраструктуры в случае приостановления их оказания;
- мероприятия по устранению инцидента и его неблагоприятных последствий с указанием планируемой и фактической продолжительности проведения данных мероприятий;
- дата восстановления оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг;
- неблагоприятные последствия инцидента по Субъектам Системы, в том числе:

- сумма денежных средств, уплаченных Оператором и (или) взысканных с Оператора,

- сумма денежных средств, уплаченных Оператором (Операторами) услуг платежной инфраструктуры и (или) взысканных с Оператора (Операторов) услуг платежной инфраструктуры,

- количество и сумма неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных распоряжений Участников Системы, на исполнение которых оказал влияние инцидент,

- продолжительность приостановления оказания услуг платежной инфраструктуры.

Оператор обеспечивает хранение первичной информации о функционировании Системы и сведений об инцидентах не менее трех лет с даты получения указанных сведений.

11.2.5. Оператор организует деятельность по разработке регламентов выполнения процедур и контролирует их соблюдение.

11.2.6. Участники и привлекаемые Операторы УПИ (расчетные центры), являются кредитными организациями, реализующими меры, направленные на обеспечение непрерывности и (или) восстановление деятельности, в соответствии с требованиями нормативных актов Банка России.

11.2.7. Каждый из привлеченных Операторов УПИ обязан обеспечивать бесперебойность оказания услуг платежной инфраструктуры, предоставляемых им Участникам и их Клиентам, а также управление риском нарушения БФПС.

11.2.8. Обязанностями Оператора, выполняющего функции Операционного центра и Платежного клирингового центра, в части управления непрерывностью функционирования Системы являются:

- осуществление деятельности в соответствии с требованиями законодательства Российской Федерации, нормативных актов Банка России и Правил;
- осуществление мер, направленных на недопущение нарушений функционирования операционных и технологических средств, информационных систем, обеспечивающих учет информации о переводах денежных средств, платежных позициях Участников и о состоянии расчетов (организация бесперебойности электропитания, дублирование каналов связи и вычислительных мощностей, защита информационных систем от воздействия вредоносного программного кода), а в случае возникновения указанных нарушений осуществление мер по их устранению;
- обеспечение сохранения функциональных возможностей операционных и технологических средств, информационных систем при сбоях в их работе (отказоустойчивость), проведение их тестирования в целях выявления недостатков функционирования, а в случае выявления указанных недостатков - принятие мер по их устранению;

- проведение анализа причин нарушений функционирования операционных и технологических средств, информационных систем, телекоммуникационных каналов связи и разработка и реализация мер по их устранению;
- обеспечение наличия аппаратно-программных средств, используемых для выполнения требований по защите информации при осуществлении переводов денежных средств в рамках Системы;
- обеспечение постоянного учета и контроля состава программного обеспечения, установленного и используемого на средствах вычислительной техники;
- обеспечение наличия и своевременной актуализации процедур восстановления программного обеспечения и аппаратного комплекса, задействованного в рамках функционирования системы и влияющего на БФПС;
- обеспечение работы службы круглосуточной поддержки и мониторинга;
- обеспечение наличия квалифицированного персонала;
- организация взаимодействия Субъектов Системы в целях управления непрерывностью функционирования Системы;
- сбор, систематизация, накопление и обработка информации, в том числе полученной в рамках порядка предоставления Участниками и Операторами УПИ информации о своей деятельности Оператору и информационное взаимодействие при выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Правилами;
- прием и обработка обращений Субъектов Системы по вопросам БФПС;
- обеспечение собственной финансовой устойчивости;
- заблаговременное осуществление инвестиций в новые системы безопасности и параллельные средства защиты и технологическую и информационную платформы;
- построение современной технологической и информационной платформ;
- построение эффективной системы обеспечения информационной безопасности (применение организационных мер защиты информации и использование средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации);
- построение системы оценки и управления рисками, способными оказать влияние на БФПС;
- обеспечение сохранности имущества;
- организация в течение установленных периодов времени восстановления оказания услуг Операторами УПИ в случае приостановления их оказания и восстановления оказания услуг платежной инфраструктуры, соответствующего надлежащему функционированию Системы;
- разработка и внедрение мер, направленных на предупреждение и минимизацию риска БФПС;
- иные меры, направленные на обеспечение непрерывности функционирования Системы.

11.2.9. Обязанностями Расчетного центра в части управления непрерывностью функционирования Системы являются:

- осуществление деятельности в соответствии с требованиями законодательства Российской Федерации, нормативных актов Банка России и Правил;
- осуществление мер, направленных на недопущение нарушений функционирования операционных и технологических средств, информационных систем, обеспечивающих учет информации о переводах денежных средств и состоянии расчетов (организация бесперебойности электропитания, дублирование каналов связи и вычислительных мощностей, защита информационных систем от

- воздействия вредоносного программного кода), а в случае возникновения указанных нарушений осуществление мер по их устранению;
- обеспечение сохранения функциональных возможностей операционных и технологических средств, информационных систем при сбоях в их работе (отказоустойчивость), проведение их тестирования в целях выявления недостатков функционирования, а в случае выявления указанных недостатков - принятие мер по их устранению;
 - анализ причин нарушения функционирования операционных и технологических средств, информационных систем, обеспечивающих осуществление переводов денежных средств и учет информации о переводах денежных средств и состоянии расчетов в рамках Системы;
 - обеспечение наличия аппаратно-программных средств, используемых для выполнения требований по защите информации при осуществлении переводов денежных средств в рамках Системы;
 - обеспечение постоянного учета и контроля состава программного обеспечения, установленного и используемого на средствах вычислительной техники;
 - обеспечение наличия и своевременной актуализации процедур восстановления программного обеспечения и аппаратного комплекса, задействованного в рамках функционирования платежной системы и влияющего на БФПС;
 - обеспечение наличия квалифицированного персонала;
 - сбор, систематизация, накопление и направление документов и информации Оператору в рамках порядка предоставления Участниками и Операторами УПИ информации о своей деятельности Оператору и информационного взаимодействия при выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Правилами, в том числе первичной информации о функционировании Системы, информации для расчета показателей БФПС, информации об инцидентах и уровнях оказания услуг платежной инфраструктуры;
 - осуществление мер, направленных на поддержание остатка денежных средств на своих счетах, достаточного для бесперебойного осуществления расчетов с получателями и иных операций в Системе;
 - прием и обработка обращений Участников по вопросам БФПС;
 - осуществление взаимодействия с Оператором в целях управления непрерывностью функционирования Системы;
 - обеспечение собственной финансовой устойчивости;
 - построение системы оценки и управления рисками, способными оказать влияние на БФПС;
 - разработка и внедрение мер, направленных на предупреждение и минимизацию риска БФПС;
 - заблаговременное осуществление инвестиций в новые системы безопасности и параллельные средства защиты и технологическую и информационную платформы;
 - построение современной технологической и информационной платформы;
 - построение эффективной системы обеспечения информационной безопасности (применение организационных мер защиты информации и использование средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации);
 - обеспечение сохранности имущества;
 - иные меры, направленные на обеспечение непрерывности функционирования Системы.

11.2.10. Обязанности Участников в части управления непрерывностью функционирования Системы являются:

- осуществление деятельности в соответствии с требованиями законодательства Российской Федерации, нормативных актов Банка России и Правил;
- осуществление мер, направленных на недопущение нарушений функционирования операционных и технологических средств, информационных систем, обеспечивающих учет информации о переводах денежных средств и состоянии расчетов (организация бесперебойности электропитания, дублирование каналов связи и вычислительных мощностей, защита информационных систем от воздействия вредоносного программного кода), а в случае возникновения указанных нарушений осуществление мер по их устранению;
- обеспечение сохранения функциональных возможностей операционных и технологических средств, информационных систем при сбоях в их работе (отказоустойчивость), проведение их тестирования в целях выявления недостатков функционирования, а в случае выявления указанных недостатков - принятие мер по их устранению;
- анализ причин нарушения функционирования операционных и технологических средств, информационных систем, обеспечивающих учет информации о переводах денежных средств и состоянии расчетов;
- обеспечение наличия аппаратно-программных средств, используемых для выполнения требований по защите информации при осуществлении переводов денежных средств в рамках Системы;
- обеспечение постоянного учета и контроля состава программного обеспечения, установленного и используемого на средствах вычислительной техники;
- обеспечение наличия и своевременной актуализации процедур восстановления программного обеспечения и аппаратного комплекса, задействованного в рамках функционирования Системы и влияющего на БФПС;
- обеспечение наличия квалифицированного персонала;
- обеспечение достаточности денежных средств на Счете Участника в порядке и в сроки, установленные Правилами;
- прием и обработка обращений Клиентов Участников по вопросам БФПС;
- осуществление взаимодействия с Оператором в целях обеспечения непрерывности функционирования Системы;
- обеспечение собственной финансовой устойчивости;
- разработка и внедрение мер, направленных на предупреждение и минимизацию риска нарушения БФПС.

11.3. Показатели бесперебойности функционирования Системы

11.3.1. Контроль за соблюдением регламента выполнения процедур осуществляется Оператором посредством анализа первичной информации о функционировании Системы и параметров, на основании которых производится оценка функционирования Системы.

11.3.2. Уровни оказания услуг платежной инфраструктуры:

- а. Уровень оказания операционных услуг:
- показатель доступности услуг Операционного центра – не менее 96% времени в течение календарного месяца;
 - количество аварий, сбоев по вине Операционного центра, влияющих на доступность услуг Операционного центра – не более 2 (двух) аварий, сбоев в месяц;
 - количество отказов в приеме от Расчетного центра сообщений об остатках денежных средств на Счетах Участников – не более 2 (двух) раз в месяц;
 - показатель количества обрабатываемых Операций – 100 % операций;
 - время на обработку запроса на совершение Операции не более 30 (тридцати) секунд;

- время на прием и первичную обработку сообщений от Расчетного центра об остатках денежных средств на Счете Участника – не более 1 (одного) часа;
- показатель количества распоряжений Участников, по которым в течение календарного месяца были оказаны операционные услуги без нарушения регламента выполнения процедур – не менее 98% распоряжений в течение календарного месяца;
- восстановление надлежащего оказания операционных услуг и/или возобновление осуществления операционных услуг в случае его приостановления в течение установленных временных периодов.

б. Уровень оказания услуг платежного клиринга:

- количество допущенных ошибок при определении платежной клиринговой позиции Участника – 0;
- показатель количества распоряжений Участников, по которым в течение календарного месяца были оказаны услуги платежного клиринга без нарушения регламента выполнения процедур – не менее 98 % распоряжений в течение календарного месяца;
- восстановление надлежащего оказания услуг платежного клиринга и/или возобновление осуществления услуг платежного клиринга в случае его приостановления в течение установленных временных периодов.

в. Уровень оказания расчетных услуг:

- показатель достаточности денежных средств для осуществления расчетов – отношение остатка денежных средств на момент осуществления расчетов на счетах Расчетного центра к сумме совершенных операций по переводу денежных средств, по которым осуществляется расчет – коэффициент ≥ 1 ;
- показатель количества обрабатываемых распоряжений на перевод денежных средств – 100% распоряжений на перевод денежных средств, поступивших на исполнение в Расчетный центр в составе Реестра распоряжений;
- количество допущенных ошибок при проведении операций по списанию/зачислению денежных средств по Счетам Участников – 0;
- показатель количества распоряжений Участников, по которым в течение календарного месяца были оказаны расчетные услуги без нарушения регламента выполнения процедур – не менее 99% распоряжений в течение календарного месяца;
- восстановление надлежащего оказания расчетных услуг и/или возобновление осуществления расчетных услуг в случае его приостановления в течение установленных временных периодов;
- показатель достаточности денежных средств на Счетах Участников для осуществления расчетов – отношение остатков денежных средств на Счетах Участников на момент осуществления расчетов к сумме совершенных Клиентами Участника операций по переводу денежных средств, по которым осуществляется расчет - коэффициент ≥ 1 .

11.3.3. Показатели бесперебойности (БФПС) определяются в целях анализа риска нарушения БФПС, описания профиля рисков нарушения БФПС для принятия решения о необходимости изменения (корректировки) мер по обеспечению БФПС, выбора конкретных мер, необходимых для достижения и поддержания допустимого уровня риска нарушения БФПС и идентификации Субъекта Системы, ответственного за их реализацию.

11.3.4. К показателям БФПС относятся:

- Продолжительность восстановления оказания УПИ (П1);
- Непрерывность оказания УПИ (П2);
- Соблюдение регламента (П3);
- Доступность операционного центра ПС (П4);
- Изменение частоты инцидентов (П5).

11.3.5. Оператор имеет право определять другие показатели, в зависимости от текущей ситуации в обеспечении БФПС Системы.

11.3.6. Показатели бесперебойности:

Наименование показателя	Формат	Пороговые уровни показателей бесперебойности функционирования платежной системы	Процедура/методика формирования
Продолжительность восстановления оказания УПИ (П1):			
<p>период времени восстановления оказания услуг операторами УПИ в случае приостановления оказания УПИ, в том числе вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств.</p> <p>Определяется как период времени с момента приостановления оказания УПИ вследствие инцидента, произошедшего у оператора УПИ, и до момента восстановления оказания УПИ.</p>	в часах/ минутах/ секундах	$P1 \leq 6$ часов Приостановление оказания УПИ длительностью не более 6 часов 00 мин. 00 секунд	<p>Рассчитывается по каждому из ОУПИ и по каждому из инцидентов, повлекших приостановление оказания УПИ.</p> <p>При возникновении инцидентов, повлекших приостановление оказания УПИ одновременно двумя и более ОУПИ, показатель П1 должен рассчитываться как период времени с момента приостановления оказания УПИ в результате первого из возникших инцидентов и до момента восстановления оказания УПИ всеми ОУПИ, у которых возникли инциденты</p>
Непрерывность оказания УПИ (П2):			
<p>период времени между двумя последовательно произошедшими в Системе инцидентами, в результате которых приостанавливалось оказание УПИ, с момента устранения первого инцидента и до момента возникновения следующего</p>	в часах/ минутах/ секундах	$P2 \geq 24$ часов 00 мин.00 сек. Не рассматривается в качестве инцидентов приостановление (прекращение) участия в платежной системе в случаях, предусмотренных настоящими правилами платежной системы в соответствии с пунктом 4 части 1 статьи 20 Закона о НПС	<p>Рассчитывается по каждому из ОУПИ при возникновении каждого из инцидентов, повлекших приостановление оказания УПИ.</p> <p>Если ОУПИ оказывает более одного вида УПИ одновременно, показатель П2 должен рассчитываться одновременно по всем видам УПИ, оказываемым данным</p>

			ОУПИ
Соблюдение регламента (П3):			
<p>Характеризует соблюдение операторами УПИ времени начала, времени окончания, продолжительности и последовательности процедур, выполняемых операторами УПИ при оказании операционных услуг, услуг платежного клиринга и расчетных услуг. Рассчитывается как отношение количества распоряжений участников платежной системы (их клиентов), по которым в течение календарного месяца были оказаны операционные услуги без нарушения регламента выполнения процедур, к общему количеству распоряжений участников платежной системы (их клиентов), по которым были оказаны операционные услуги в течение календарного месяца</p>	<p>% с точностью до двух знаков после запятой (с округлением по математическому методу).</p>	<p>$P3 \geq 98,00$ % - для операционного центра и платежного клирингового центра, $P3 \geq 99,00$ % - для расчетного центра, рассчитывается ежемесячно по каждому оператору УПИ по формулам, определенным нормативным актом Банка России. Значение показателя П3 по платежной системе в целом принимается равным наименьшему из значений данного показателя, рассчитанных по всем ОУПИ в отношении всех видов оказываемых ими услуг. При этом если ОУПИ оказывает более одного вида УПИ одновременно, показатель П3 должен рассчитываться по данному оператору УПИ в отношении всех видов оказываемых им услуг.</p>	<p>Для платежного клирингового центра показатель П3 должен рассчитываться как отношение количества распоряжений участников платежной системы (их клиентов), по которым в течение календарного месяца были оказаны услуги платежного клиринга без нарушения регламента выполнения процедур, к общему количеству распоряжений участников платежной системы (их клиентов), по которым были оказаны услуги платежного клиринга в течение календарного месяца</p>
Доступность операционного центра ПС (П4):			
<p>характеризует оказание операционных услуг операционным центром платежной системы как среднее значение коэффициента доступности операционного центра платежной системы за календарный месяц</p>	<p>% с точностью до двух знаков после запятой (с округлением по математическому методу).</p>	<p>$P4 \geq 96,00$ %, рассчитывается ежемесячно по каждому оператору УПИ по формуле, определенной нормативным актом Банка России. Значение показателя П4 по платежной системе в целом принимается равным наименьшему из значений данного показателя, рассчитанных по всем операционным центрам платежной системы</p>	<p>Для платежных систем с несколькими операционными центрами показатель П4 должен рассчитываться для каждого операционного центра платежной системы</p>

Изменение частоты инцидентов (П5):			
Темп прироста среднедневного количества инцидентов за оцениваемый календарный месяц по отношению к среднедневному количеству инцидентов за предыдущие 12 календарных месяцев, включая оцениваемый календарный месяц	%, с точностью до одного знака после запятой (с округлением по математическому методу).	$P5 \leq 400\%$, рассчитывается ежемесячно по платежной системе в целом и для каждого оператора УПИ в отдельности по формуле, определенной нормативным актом Банка России. В случае если за предыдущие 12 календарных месяцев, включая оцениваемый месяц, инцидентов не было, значение показателя признается равным нулю	В платежных системах, в которых ОУПИ оказывает более одного вида УПИ одновременно, показатель П5 должен рассчитываться по данному оператору УПИ в отношении всех видов оказываемых им услуг.

11.3.7. Алгоритмы (формулы) расчета показателей БФПС установлены в Порядке бесперебойности функционирования и анализа рисков платежной системы «КП Ритейл».

Оператор осуществляет анализ полученных значений показателей БФПС и показателей уровней оказания услуг платежной инфраструктуры, проводимый посредством их сравнения с установленными пороговыми уровнями.

Превышение показателями БФПС и показателями уровней оказания услуг платежной инфраструктуры установленных для них пороговых уровней означает увеличение влияния рисков на деятельность Системы в целом, и приближение критического его состояния и размера для текущих условий.

В случае, когда любой из показателей БФПС и показателей уровней оказания услуг платежной инфраструктуры превышает установленный для него пороговый уровень, руководитель структурного подразделения (работник) Оператора, ответственного за управление рисками, присущими деятельности Системы, незамедлительно информирует об этом единоличный исполнительный орган Оператора и принимает меры по устранению выявленных нарушений.

Оператор осуществляет пересмотр системы параметров, на основании которых производится оценка функционирования Системы, по мере необходимости, но не реже одного раза в год.

Расчет и оценка параметров, на основании которых производится оценка функционирования Системы, производится с использованием первичной информации о функционировании Системы, сведений об инцидентах и иной информации.

11.3.8. Сбор соответствующей информации и сведений осуществляется путем аккумулирования данных, полученных в ходе ведения Оператором своей деятельности (в том числе в связи с выполнением функций Операционного центра и Платежного клирингового центра), а также полученных от остальных Субъектов Системы в установленном в Правилах порядке.

Сбор информации осуществляется Оператором следующим образом:

- работниками структурного подразделения (работником) Оператора, ответственного за управление рисками, присущими деятельности Системы, в том числе с использованием ПК «КП РИТЕЙЛ» и посредством анализа жалоб и обращений Участников, их Клиентов – участников ВЭД и Получателей;

- посредством информационного взаимодействия с Субъектами Системы.

11.3.9. Оператор проводит оценку влияния на БФПС каждого произошедшего в Системе инцидента в течение 24 часов с момента его возникновения (выявления), а также в

течение 24 часов после устранения инцидента (восстановления оказания УПИ, соответствующего требованиям к оказанию услуг).

В случае если вследствие произошедшего в Системе инцидента нарушен регламент выполнения процедур, но при этом не нарушен пороговый уровень каждого из показателей П1, П2, данный инцидент признается непосредственно не влияющим на БФПС.

Произошедший в Системе инцидент признается влияющим на БФПС в случае, если вследствие данного инцидента реализовано хотя бы одно из следующих условий:

- нарушен регламент выполнения процедур при одновременном нарушении порогового уровня показателя П2;
- нарушен пороговый уровень показателя П1;
- превышена продолжительность установленного Оператором времени, в течение которого должно быть восстановлено оказание услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг.

В случае выявления дополнительных обстоятельств инцидента, оценка влияния которого на БФПС уже завершена, проводится повторная оценка произошедшего инцидента с учетом вновь выявленных обстоятельств.

Оператор проводит оценку влияния на БФПС всех инцидентов, произошедших в Системе в течение календарного месяца. Оценка влияния на БФПС данных инцидентов проводится в течение пяти рабочих дней после дня окончания календарного месяца, в котором возникли инциденты.

В случае если вследствие произошедших в Системе в течение календарного месяца инцидентов не нарушен пороговый уровень показателя П4, рассчитанного по данным инцидентам, и одновременно нарушен пороговый уровень показателя П3 и (или) показателя П5, рассчитанных по этим же инцидентам, данные инциденты признаются непосредственно не влияющими на БФПС.

В случае если вследствие произошедших в Системе в течение календарного месяца инцидентов одновременно нарушены пороговые уровни всех показателей П3, П4, П5, рассчитанных по данным инцидентам, данные инциденты признаются влияющими на БФПС.

В случае выявления инцидентов или дополнительных обстоятельств инцидентов, произошедших в Системе в течение календарного месяца, за который уже проведена оценка их влияния на БФПС, Оператор проводит повторную оценку влияния на БФПС этих инцидентов с учетом вновь выявленных обстоятельств в течение пяти рабочих дней после дня окончания календарного месяца, в котором выявлены инциденты или дополнительные обстоятельства.

11.3.10. Привлеченные Операторы УПИ обязаны информировать и предоставлять Оператору информацию обо всех инцидентах, произошедших в их деятельности, которые привели к нарушению требований регламента выполнения процедур или оказали влияние на БФПС в порядке и сроки, определенные Правилами для взаимодействия в рамках Системы в чрезвычайных ситуациях, и руководствуясь пп. 11.2.4 Правил.

11.3.11. Сбор первичной информации о функционировании Системы, в том числе от привлеченных Операторов УПИ, используемой для расчета показателей БФПС и для оценки уровней оказания услуг платежной инфраструктуры, а также сведений об инцидентах осуществляется Оператором посредством предоставления Участниками и Операторами УПИ информации Оператору в порядке, определенном в пп. 12.1.7 Правил, а также в рамках информационного взаимодействия при выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, порядок которых установлен Правилами.

11.3.12. В случае выявления инцидентов или дополнительных обстоятельств инцидентов, произошедших в Системе в течение календарного месяца, за который уже проведена оценка их влияния на БФПС, Оператор проводит повторную оценку влияния на БФПС этих инцидентов с учетом вновь выявленных обстоятельств в течение пяти рабочих

дней после дня окончания календарного месяца, в котором выявлены инциденты или дополнительные обстоятельства.

11.4. Требования к содержанию деятельности по обеспечению БФПС, осуществляемой Субъектами Системы

11.4.1. В Системе установлены требования к деятельности по обеспечению БФПС, осуществляемой Оператором, Операторами УПИ и Участниками, которые включают:

- требования к планам ОНиВД привлеченных Операторов УПИ;
- мероприятия, направленные на управление Оператором непрерывностью функционирования Системы в случае возникновения инцидентов, связанных с приостановлением оказания услуг платежной инфраструктуры или нарушением установленных уровней оказания услуг платежной инфраструктуры;
- порядок оценки качества функционирования операционных и технологических средств, информационных систем;
- порядок изменения операционных и технологических средств и процедур.

11.4.2. Требования к планам действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности в случае возникновения нестандартных и чрезвычайных ситуаций привлеченных Операторов УПИ заключаются в следующем:

- Привлеченные Операторы УПИ обязаны разработать, реализовывать, пересматривать, а также проводить проверку (тестирование) плана ОНиВД;
- В целях контроля за выполнением указанной обязанности Оператор с периодичностью не реже одного раза в два года направляет в адрес Расчетного центра запрос о предоставлении:
 - копии плана ОНиВД Расчетного центра;
 - информации о проведении Расчетным центром проверки (тестирования) и/или ее сроках/результатах, а также о периодичности пересмотра плана ОНиВД.
- План ОНиВД должен определять порядок, способы и сроки осуществления комплекса мероприятий по предотвращению или своевременной ликвидации последствий возможного нарушения режима повседневного функционирования привлеченного Оператора УПИ, вызванного непредвиденными обстоятельствами (возникновением чрезвычайной ситуации или иным событием, наступление которого возможно, но трудно предсказуемо и связано с угрозой существенных материальных потерь или иных последствий, препятствующих выполнению оператором УПИ принятых на себя обязательств).

11.4.3. Мероприятия, направленные на управление Оператором непрерывностью функционирования Системы в случае возникновения инцидентов, связанных с приостановлением оказания услуг платежной инфраструктуры или нарушением установленных уровней оказания услуг платежной инфраструктуры предусматривают:

а. В случае нарушения обслуживающим Участников Расчетным центром, времени восстановления оказания услуг платежной инфраструктуры при приостановлении их оказания более двух раз в течение трех месяцев подряд либо нарушения Правил, выразившегося в отказе в одностороннем порядке от оказания услуг Участнику (Участникам), не связанного с приостановлением (прекращением) участия в Системе в случаях, предусмотренных Правилами, Оператор в срок не более одного года с даты повторного превышения времени восстановления оказания услуг платежной инфраструктуры осуществляет следующие мероприятия по привлечению другого Расчетного центра в качестве резервного:

- поиск кредитной организации, имеющей возможность осуществления услуг расчетного центра платежной системы;
- проведение переговоров и заключение договора с кредитной организацией, имеющей возможность осуществления услуг расчетного центра платежной системы;

- проведение правовой и технологической интеграции вновь привлеченного Оператора УПИ в Систему;
- перевод Участников на обслуживание к вновь привлеченному Оператору УПИ в срок, определенный в пп. 6.12.5 Правил.

В случае, если в течение шести месяцев с момента начала проведения Оператором мероприятий по привлечению нового расчетного центра отсутствовали факты нарушения Расчетным центром требований к бесперебойности оказания услуг либо нарушения Правил, выразившегося в превышении времени восстановления оказания услуг платежной инфраструктуры при приостановлении их оказания, Оператор вправе прекратить мероприятия по привлечению другого расчетного центра.

В случае нарушения обслуживающим Участников Расчетным центром требований к бесперебойности оказания услуг, выразившегося в отказе в одностороннем порядке от оказания услуг Участнику (Участникам), не связанного с приостановлением (прекращением) участия в Системе в случаях, предусмотренных Правилами, Оператор в срок не более трех месяцев с даты такого отказа осуществляет следующие мероприятия по привлечению другого Расчетного центра в качестве резервного:

- поиск кредитной организации, имеющей возможность осуществления услуг расчетного центра платежной системы;
- проведение переговоров и заключение договора с кредитной организацией, имеющей возможность осуществления услуг расчетного центра платежной системы;
- проведение правовой и технологической интеграции вновь привлеченного Оператора УПИ в Систему;
- перевод Участников на обслуживание к вновь привлеченному Оператору УПИ в срок, определенный в пп. 6.12.5 Правил.

б. В случае превышения Оператором, выполняющим согласно Правилам функции Операционного центра и Платежного клирингового центра, времени восстановления оказания услуг платежной инфраструктуры при приостановлении их оказания более двух раз в течение трех месяцев подряд либо нарушения Правил, выразившегося в отказе в одностороннем порядке от оказания услуг Участнику (Участникам), не связанного с приостановлением (прекращением) участия в Системе в случаях, предусмотренных Правилами, Оператор в срок не более четырех месяцев с даты повторного превышения времени восстановления оказания услуг платежной инфраструктуры либо даты отказа в одностороннем порядке от оказания услуг Участнику (Участникам), не связанного с приостановлением (прекращением) участия в Системе в случаях, предусмотренных Правилами, осуществляет следующие мероприятия по привлечению другого Операционного центра и/или Платежного клирингового центра и по переходу Участников на обслуживание к вновь привлеченному Оператору УПИ:

- поиск специализированной организации, имеющей право и возможность осуществления услуг операционного центра и/или платежного клирингового центра платежной системы;
- проведение переговоров и заключение договора со специализированной организацией, имеющей право и возможность осуществления услуг операционного центра и/или платежного клирингового центра платежной системы;
- проведение правовой и технологической интеграции вновь привлеченного Оператора УПИ в Систему;
- перевод Участников на обслуживание к вновь привлеченному Оператору УПИ в срок, определенный в пп. 6.12.5 Правил.

В случае, если в течение трех месяцев с момента начала Оператором проведения мероприятий по привлечению нового Оператора УПИ факты превышения Оператором, выполняющим согласно Правилам функции Операционного центра и Платежного

клирингового центра, времени восстановления оказания услуг платежной инфраструктуры при приостановлении их оказания более двух раз в течение трех месяцев подряд либо нарушения Правил, выразившегося в отказе в одностороннем порядке от оказания услуг Участнику (Участникам), не связанного с приостановлением (прекращением) участия в Системе в случаях, предусмотренных Правилами, отсутствовали, - Оператор вправе прекратить мероприятия по привлечению другого операционного центра и/или платежного клирингового центра.

11.5. Порядок оценки качества функционирования операционных и технологических средств, информационных систем

11.5.1. Проведение оценки качества функционирования операционных и технологических средств, информационных систем, применяемых Оператором, обусловлено оказанием Оператором также услуг платежной инфраструктуры (за исключением услуг Расчетного центра), и осуществляется путем контроля соответствия качества функционирования операционных и технологических средств, информационных систем Оператора целям, задачам и масштабу деятельности Системы, объему оказываемых услуг платежной инфраструктуры, поддержания уровня качества операционных услуг и услуг платежного клиринга, обеспечивающего БФПС.

11.5.2. Оценка качества функционирования операционных и технологических средств, информационных систем осуществляется Оператором самостоятельно (по мере необходимости) или с привлечением сторонней независимой организации (не реже одного раза в 5 лет), выбираемой Оператором самостоятельно. Привлекаемая сторонняя независимая организация должна соответствовать требованиям, иметь лицензии (разрешения), необходимые для осуществления соответствующей деятельности (в случае, если такие требования, лицензии (разрешения) предусмотрены законодательством Российской Федерации). Оценка качества функционирования операционных и технологических средств, информационных систем осуществляется сторонней независимой организацией в соответствии со стандартами и правилами привлекаемой организации, стандартами и правилами, установленными законодательством Российской Федерации (при их наличии), в сроки, согласованные с Оператором и обеспечивающие качественное выполнение поставленной задачи. Периодичность проведения оценки качества функционирования операционных и технологических средств, информационных систем определяется Оператором с учетом изменения (модификации) угроз нарушения нормального функционирования средств и систем, а также в зависимости от изменения иных факторов, влияющих на функционирование операционных и технологических средств, информационных систем.

11.5.3. Участники и привлеченные Операторы УПИ по своему усмотрению и за свой счет самостоятельно или с привлечением независимых организаций проводят оценку качества функционирования операционных и технологических средств, информационных систем. В случае, если порядок привлечения независимых организаций установлен законодательством Российской Федерации или нормативными требованиями Банка России, то Участники и привлеченные Операторы УПИ обязаны привлекать для оценки качества функционирования операционных и технологических средств, информационных систем стороннюю независимую организацию, соответствующую установленным нормативным требованиям.

11.5.4. Привлеченные Операторы УПИ проводят оценку качества функционирования операционных и технологических средств и информационных систем не реже 1 раза в два года.

11.5.5. Привлеченные Операторы УПИ обязаны предоставлять результаты проверки Оператору. Привлеченные Операторы УПИ совместно с Оператором вправе принимать решения об изменении операционных и технологических средств и процедур Системы в порядке, предусмотренном Правилами.

11.5.6. Субъекты Системы самостоятельно выбирают мероприятия и способы достижения и поддержания допустимого уровня рисков нарушения БФПС и реализуют их в рамках своих систем управления рисками.

11.5.7. Оценка эффективности и совершенствование мероприятий и способов управления рисками осуществляется Субъектами Системы на постоянной основе.

11.6. Порядок изменения операционных и технологических средств и процедур

11.6.1. Оператор вправе изменять операционные и технологические средства и процедуры в следующих случаях:

- изменения порядка оказания услуг или вида услуг по переводам денежных средств;
- в случаях, предусмотренных законодательством Российской Федерации и нормативными документами и/или рекомендациями Банка России;
- в рамках системы управления рисками;
- в результате проведения оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией.

Привлеченные Операторы УПИ вправе изменять операционные и технологические средства и процедуры в указанных выше случаях только по согласованию в письменной форме с Оператором.

11.6.2. Оператор устанавливает следующие уровни оказания услуг платежной инфраструктуры, характеризующие качество функционирования операционных и технологических средств платежной инфраструктуры, которые должны быть обеспечены Операторами услуг платежной инфраструктуры:

- услуги платежной инфраструктуры, соответствующие требованиям к оказанию услуг;
- услуги платежной инфраструктуры, несоответствующие требованиям к оказанию услуг.

К услугам платежной инфраструктуры, соответствующим требованиям к оказанию услуг, относятся услуги платежной инфраструктуры, при которых одновременно соблюдаются:

- требования законодательства Российской Федерации, Правил, заключенных договоров при взаимодействии Субъектов Системы;
- временной регламент функционирования Системы;
- пороговые уровни показателей БФПС.

К услугам платежной инфраструктуры, несоответствующим требованиям к оказанию услуг, относятся услуги платежной инфраструктуры, при которых не соблюдаются все или одно их указанных выше требований.

11.6.3. В случае если изменение операционных и технологических средств и процедур требует внесения изменений в Правила, Оператор вносит соответствующие изменения в порядке, предусмотренном законодательными, нормативными документами и настоящими Правилами.

В случае если изменение операционных и технологических средств и процедур не требует внесения изменений в Правила, Оператор либо привлеченный ОУПИ направляет Участникам уведомление об изменении операционных и технологических средств и процедур с описанием таких изменений не позднее, чем за 10 (десять) календарных дней до даты вступления в силу соответствующих изменений.

Изменение операционных и технологических средств и процедур в Системе осуществляется Оператором при наличии необходимости в случае изменения порядка совершения или видов операций, совершаемых в рамках Системы, в целях совершенствования системы управления рисками, по результатам проведения оценки качества функционирования операционных и технологических средств, информационных систем, проведенной

самостоятельно или с привлечением независимой организации, а также в случаях, предусмотренных законодательством Российской Федерации, и по требованию Банка России.

11.6.4. Участник, привлеченный ОУПИ вправе самостоятельно вносить изменения в операционные и технологические средства и процедуры по взаимодействию с Системой на стороне Участника, привлеченного ОУПИ, если внесение таких изменений не противоречит законодательным, нормативным документам соответствующих регуляторов, настоящим Правилам и условиям договоров, заключенных в рамках взаимодействия между Субъектами Системы и не приводит к изменению порядка оказания услуг по переводам денежных средств, предусмотренного настоящими Правилами, к объему и характеру их оказания Участником, привлеченным ОУПИ, а также не повлияет негативно на обеспечение БФПС, управление рисками и обеспечение защиты информации в платежной системе.

11.7. Порядок информационного взаимодействия Субъектов платежной системы и документационного обеспечения их деятельности по обеспечению БФПС

11.7.1. Оператор организует взаимодействие Субъектов Системы по обеспечению БФПС с учетом нижеперечисленных требований.

Оператор определяет порядок взаимодействия Субъектов Системы при реализации мероприятий по управлению рисками и непрерывностью функционирования Системы с учетом организационной модели управления рисками в Платежной системе, определенной в соответствии с требованиями части 2 статьи 28 Закона о НПС и Правил.

Оператор определяет функции, выполняемые привлеченными ОУПИ по оперативному информированию Оператора о нарушении оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, при котором превышено время восстановления оказания услуг платежной инфраструктуры, в случае их приостановления и (или) время восстановления оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг.

11.7.2. С целью обеспечения БФПС Оператор, привлеченные ОУПИ, и Участники осуществляют информационное взаимодействие. Обмен информацией осуществляется по согласованным каналам связи. Порядок обмена информацией аналогичен указанному в п.10.3 Правил.

11.7.3. Привлеченные ОУПИ и Участники должны разработать и использовать в работе документы, устанавливающие порядок обеспечения непрерывности деятельности в рамках выполняемых в Системе функций (план ОНиВД), в соответствии с требованиями, указанными в пп. 11.4.2 Правил, в котором также предусмотреть план восстановления деятельности после сбоев.

Кроме того, Оператор рекомендует привлеченным ОУПИ и Участникам разработать следующие внутренние нормативные документы, регламентирующие:

- политику информационной безопасности;
- политику защиты от вредоносного кода;
- политику использования сети Интернет;
- политику резервного копирования.

11.7.4. Оператор, привлеченные ОУПИ и Участники Системы осуществляют сбор, документирование и статистическую обработку первичной информации о функционировании Системы.

Хранение первичной информации осуществляется в электронном виде. По запросу от Оператора привлеченные ОУПИ и Участники предоставляют первичную информацию о функционировании системы в электронном виде (или в другом согласованном с Оператором формате).

В состав первичной информации о функционировании Системы входит, в том числе:

- информация о времени приема к исполнению, исполнения распоряжений Участников Системы об осуществлении Переводов;

- информация о количестве и суммах указанных распоряжений;
- информация о размерах платежных клиринговых позиций и остатках денежных средств на Счетах Участников;
- иная информация о функционировании Системы, предусмотренная настоящими Правилами.

11.7.5. Оператор информирует о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры Участников и привлеченных ОУПИ в порядке, установленном пп. 4.1.17 Правил.

11.8. Обеспечение БФПС Субъектами Системы

11.8.1. Оператор осуществляет проведение оценки эффективности системы управления рисками Системы: устанавливает критерии оценки, осуществляет оценку на ежегодной основе. По итогам оценки принимаются решения о необходимости внесения изменений в систему управления рисками, формируются предложения и рекомендации по итогам проверки.

11.8.2. Обеспечение БФПС Оператором осуществляется путем:

- осуществления координации деятельности Субъектов Системы по обеспечению БФПС путем её регламентации в Правилах и путем осуществления контроля за выполнением Правил;
- установления структурным подразделением или ответственным сотрудником, отвечающим за управление рисками, не реже одного раза в год допустимого уровня риска нарушения БФПС;
- выявления факторов риска нарушения БФПС, определения степени и характера влияния указанных факторов на БФПС, проведения оценки соответствия уровня риска нарушения БФПС предельно допустимому уровню;
- проведения мониторинга изменений характера и степени влияния факторов риска;
- участия в проведении расследований событий, вызвавших операционные сбои, анализ их причин и последствий;
- проведения оценки рисков, присущих видам деятельности Оператора для обеспечения непрерывности деятельности Системы;
- принятия мер по устранению или минимизации рисков нарушения БФПС; к Участникам Оператор вправе применить: использование мер воздействия, включая применение штрафных санкций, предусмотренных договором участия, вплоть до приостановления деятельности в Системе (временное или постоянное), в случае несоответствия установленному уровню обеспечения бесперебойности;
- проведения оценки и мониторинга финансовой устойчивости Участников, факторов, несущих риски потери финансовой устойчивости Участников, в том числе потенциальных, способных привести к потере финансовой устойчивости Участников в будущем;
- осуществления контроля соблюдения требований Правил, договорных обязательств, соблюдения порядка обеспечения БФПС привлеченными ОУПИ и Участниками;
- проведения регулярных проверок Участников на предмет соблюдения условий осуществления переводов денежных средств, требований Правил;
- контроль соблюдения условий может осуществляться как путем выездных проверок, так и направлением запросов о предоставлении требуемой информации;

- осуществления контроля использования наименования и товарных знаков Системы исключительно в рамках заключенных договоров, соглашений и Правил;
- доведения информации о возникающих рисках нарушения БФПС до органов управления Оператора;
- выявления Оператором организаций, предоставляющих участникам, их клиентам услуги платежной инфраструктуры;
- обеспечения возможности для Участников осуществить переход в течение не более 20 (двадцати) рабочих дней на обслуживание к другому привлеченному ОУПИ, включая РЦ в случае нарушения обслуживающим их РЦ требований к бесперебойности оказания услуг платежной инфраструктуры, в том числе приостановления (прекращения) оказания услуг.

11.8.2.1. Обеспечение БФПС привлеченными ОУПИ осуществляется путем:

- выполнения функций по управлению риском нарушения БФПС в соответствии с организационной моделью управления рисками в Системе;
- сбора и обработки доступной привлеченному ОУПИ информации и времени поступления в Систему распоряжений Участников по переводам денежных средств, ходе исполнения указанных распоряжений, характеристиках осуществляемых переводов денежных средств, количестве, сумме и времени наступления окончательности переводов, размере платежных клиринговых позиций и остатках денежных средств на Счетах Участников;
- письменного информирования, либо по согласованным каналам связи (в т.ч. по электронной почте) Оператора о событиях, вызвавших операционные сбои, об их причинах и последствиях, а также в случае возникновения или реализации угрозы неисполнения или ненадлежащего исполнения Участниками принятых на себя обязательств;
- организации и осуществления деятельности по обеспечению бесперебойности оказания услуг Участникам в соответствии с принятыми на себя обязательствами и требованиями порядка обеспечения БФПС;
- обеспечения непрерывности деятельности и/или восстановления деятельности по оказанию услуг платежной инфраструктуры, нарушенной в результате непредвиденных обстоятельств, в сроки и в соответствии с требованиями, установленными порядком обеспечения БФПС;
- регулярной оценки качества и надежности функционирования применяемых информационных систем, работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивает функционирование Системы.
- разработки планов восстановления деятельности после сбоев функционирования операционной и клиринговой системы;
- определения допустимых технологических перерывов в оказании операционных и услуг платежного клиринга на основании оценки допустимого уровня рисков;
- осуществления сбора и обработки информации об инцидентах, вызвавших операционные сбои в Системе;
- обеспечения наличия резервирования компонентов сетевой, вычислительной инфраструктуры и систем электроснабжения и охлаждения;
- обеспечения регулярного резервного копирования данных Системы;
- обеспечения наличия территориально удаленного резервного центра обработки данных для восстановления функционирования Системы в случае наступления кризисной ситуации в основном центре обработки данных.

11.8.2.2. Обеспечение БФПС Участниками осуществляется путем:

- проведения оценки рисков, присущих виду деятельности Участников, для обеспечения непрерывности деятельности;
- принятия мер по обеспечению соответствия требованиям Системы и надлежащего исполнения принятых на себя обязательств;
- информирования Оператора о случаях неоказания или ненадлежащего оказания услуг, предоставляемых в рамках Системы, и событиях, вызвавших операционные сбои, а также о событиях, вызвавших спорные, нестандартные и чрезвычайные ситуации, включая случаи системных сбоев, об их причинах и последствиях;
- осуществления контроля соблюдения требований законодательства, Правил, договоров и условий осуществления переводов денежных средств;
- осуществления контроля использования наименования и товарных знаков Системы исключительно в рамках заключенных договоров и Правил.

11.9. Порядок и формы контроля соблюдения Участниками, привлеченными ОУПИ порядка обеспечения БФПС

11.9.1. Расчетный центр в рамках процедур открытия банковских счетов:

- контролирует правоспособность Участников;
- устанавливает наличие всех необходимых лицензий и разрешений;
- осуществляет идентификацию Участников, их представителей, бенефициарных владельцев;
- удостоверяется в осуществлении Участниками мероприятий в рамках противодействия легализации доходов, полученных преступным путем, и финансированию терроризма.

11.9.2. Оператор в рамках процедур управления рисками:

- изучает на постоянной основе ситуацию, складывающуюся на финансовом рынке, в т.ч. на наличие признаков проблем в банковской сфере в целом, а также в отношении конкретных контрагентов;
- изучает финансовое состояние в отношении каждого привлеченного ОУПИ, а также Участников, которым установлен лимит на операции;
- осуществляет контроль за соблюдением Правил в соответствии с п.6.9 Правил;
- Оператор организует сбор и обработку сведений, в т.ч. от привлеченных Операторов УПИ, используемых для расчетов показателей БФПС, в том числе, сведений об инцидентах, указанных в пп.11.2.4 Правил.

11.9.3. Оператор в рамках осуществления контроля за соблюдением Правил проверяет соблюдение привлеченными ОУПИ и Участниками порядка обеспечения БФПС с учетом следующих требований.

Оператор определяет указанный ниже порядок проведения контроля за соблюдением привлеченными ОУПИ и Участниками порядка обеспечения БФПС.

Оператор контролирует соответствие документов привлеченных ОУПИ порядку обеспечения БФПС и при выявлении несоответствия документов привлеченных ОУПИ порядку обеспечения БФПС направляет рекомендации привлеченным ОУПИ по устранению выявленных несоответствий.

Оператор при выявлении нарушения порядка обеспечения БФПС привлеченными ОУПИ и Участниками:

- информирует привлеченных Операторов услуг платежной инфраструктуры и Участников Платежной системы о выявленных в их деятельности нарушениях и устанавливает сроки устранения нарушений;

- осуществляет проверку результатов устранения нарушений и информирует привлеченных Операторов услуг платежной инфраструктуры и Участников Платежной системы, в деятельности которых выявлены нарушения, о результатах проведенной проверки.

Оператор определяет ответственность привлеченных Операторов услуг платежной инфраструктуры и Участников Платежной системы за неисполнение порядка обеспечения БФПС.

11.10. Обязанности ОУПИ по обеспечению бесперебойности оказания услуг платежной инфраструктуры

11.10.1. Расчетный центр, Оператор, выполняющий функции Операционного центра и Платежного клирингового центра, обязаны осуществлять в части обеспечения бесперебойности оказания услуг:

- меры, направленные на недопущение нарушений функционирования операционных и технологических средств, устройств, информационных систем, обеспечивающих учет информации о состоянии расчетов, а в случае возникновения указанных нарушений осуществляет меры по их устранению;
- анализ причин нарушений функционирования операционных и технологических средств, устройств, информационных систем, выработку и реализацию мер по их устранению;
- обеспечение сохранения функциональных возможностей операционных и технологических средств, устройств, информационных систем при сбоях в их работе (отказоустойчивость), проведение их тестирования в целях выявления недостатков функционирования, а в случае выявления указанных недостатков - принятие мер по их устранению;
- анализ рисков нарушения надлежащего функционирования Системы, оценку эффективности методик анализа и минимизации выявленных рисков, а также выявление новых рисков в рамках внутренних систем управления рисками своей деятельности в части выполнения функций ОУПИ;
- другие меры по своему усмотрению.

11.10.2. Ответственность и полномочия разграничиваются в соответствии с применяемой в Системе организационной моделью управления рисками.

11.11. Права и обязанности Оператора по обеспечению БФПС

11.11.1. Оператор имеет право и обязан:

- координировать деятельность Субъектов Системы по обеспечению БФПС;
- осуществлять информационное взаимодействие Субъектов Системы в целях управления рисками нарушения БФПС;
- принимать решения в области управления рисками в Системе;
- определять мероприятия по управлению рисками в Системе;
- определять и внедрять способы управления рисками в Системе;
- определять показатели БФПС;
- устанавливать требования к содержанию деятельности по обеспечению БФПС, осуществляемой Субъектами Системы;
- контролировать выполнение Субъектами Системы требований к управлению рисками, присущими их деятельности и оказывающими влияние на БФПС;
- контролировать соблюдение субъектами Системы порядка обеспечения БФПС;
- определять соответствие действий, осуществляемых Субъектами Системы в рамках Системы, требованиям Правил;

- приостанавливать в одностороннем порядке участие Участника в Системе до устранения допущенного Участником нарушения;
- приостанавливать в одностороннем порядке участие в Системе Участника, если имеющиеся в распоряжении Оператора сведения позволяют сделать вывод о высокой вероятности возникновения рисков, ведущих к невозможности осуществления расчетов по операциям, совершенным Клиентами Участника для целей перевода денежных средств, в том числе неисполнения обязанности по обеспечению достаточности денежных средств на Счете Участника в сроки и порядке, установленные Правилами;
- лишать кредитную организацию статуса Участника;
- устанавливать уровни оказания услуг платежной инфраструктуры и допустимый уровень рисков нарушения БФПС;
- осуществлять анализ рисков нарушения БФПС;
- разрабатывать методики анализа рисков в Системе, включая профили рисков;
- составлять профили рисков, присущих деятельности Системы, включая риск нарушения БФПС;
- рассчитывать и анализировать значения показателей БФПС, в том числе путем их сравнения с пороговыми уровнями показателей БФПС, и использовать результаты указанного анализа при оценке системы управления рисками в Системе и при
- проводить оценку влияния инцидентов на БФПС;
- определять меры, направленные на предупреждение и минимизацию риска нарушения БФПС;
- осуществлять мероприятия по минимизации рисков, необходимые для достижения или поддержания допустимого уровня рисков, включая риск нарушения БФПС;
- выявлять текущие изменения присущего уровня риска нарушения БФПС (далее - мониторинг рисков нарушения БФПС);
- обеспечивать восстановление надлежащего функционирования Системы в случае его нарушения, в том числе восстановление оказания услуг платежной инфраструктуры, в установленные Правилами временные периоды;
- утверждать комплекс мероприятий для кризисных ситуаций, в случае длительного нахождения Системы под влиянием какого-либо риска;
- проводить оценку системы управления рисками в Системе, в том числе используемых методов оценки рисков в Системе, результатов применения способов управления рисками в Системе, не реже одного раза в год и документально оформлять результаты указанной оценки;
- вносить изменения в систему управления рисками в Системе в случае, если действующая система управления рисками в Системе не позволила предотвратить нарушение оказания УПИ, соответствующего требованиям к оказанию услуг, а также восстановить оказание УПИ, соответствующее требованиям к оказанию услуг, и (или) восстановить оказание УПИ в случае приостановления их оказания в течение периодов времени, установленных Оператором в Правилах;
- проверять соблюдение привлеченными Операторами УПИ и Участниками порядка обеспечения БФПС, в том числе контролировать соответствие документов привлеченных Операторов УПИ порядку обеспечения БФПС, и при выявлении несоответствия документов привлеченных Операторов УПИ порядку обеспечения БФПС направлять рекомендации привлеченным Операторам УПИ по устранению выявленных несоответствий;

- при выявлении нарушения порядка обеспечения БФПС привлеченными Операторами УПИ и Участниками Оператор должен информировать привлеченных Операторов УПИ и Участников о выявленных в их деятельности нарушениях и устанавливать сроки устранения нарушений, а также осуществлять проверку результатов устранения нарушений и информировать привлеченных Операторов УПИ и Участников, в деятельности которых выявлены нарушения, о результатах проведенной проверки;
- определить ответственность привлеченных Операторов УПИ и Участников за неисполнение порядка обеспечения БФПС;
- разрабатывать, проверять (тестировать) и пересматривать План ОНиВД Оператора, а также организовать проведение привлеченными Операторами УПИ проверки (тестирования) и пересмотра планов ОНиВД с периодичностью не реже 1 раза в два года;
- осуществлять иные меры, установленные Правилами для обеспечения Оператором управления рисками, возникающими в процессе функционирования Системы.

11.12. Права и обязанности Участников по обеспечению БФПС

11.12.1. Участники имеют право и обязаны:

- обеспечивать соблюдение Правил, заключенных договоров, законодательных требований;
- обеспечивать надлежащее функционирование операционных и технологических средств, устройств, информационных систем, используемых в работе с Системой;
- обеспечивать надлежащую защиту информации;
- осуществлять мониторинг рисков нарушения БФПС;
- предпринимать меры по поддержанию необходимого остатка денежных средств на банковских счетах, используемых для расчетов в рамках Системы для исполнения обязательств Участника.

11.13. Права и обязанности привлеченных Операторов УПИ по обеспечению БФПС

11.13.1. Привлеченные Операторы УПИ имеют право и обязаны обеспечивать:

- создание внутренней системы управления рисками, присущими деятельности привлеченного Оператора УПИ, включая риск нарушения БФПС;
- соблюдение заключенного с Оператором договора, Правил, законодательных требований;
- соблюдение регламента выполнения процедур, предусмотренных Правилами;
- надлежащее функционирование операционных и технологических средств, устройств, информационных систем, используемых при расчетах в работе с Системой;
- соблюдение уровней оказания услуг платежной инфраструктуры;
- соблюдение продолжительности временных периодов, в течение которых должно быть восстановлено надлежащее функционирование Системы в случае его нарушения, в том числе в случае приостановления (прекращения) оказания услуг платежной инфраструктуры;
- осуществление мониторинга рисков нарушения БФПС и уведомление Оператора о реализации рисков, оказывающих влияние на БФПС;
- осуществление анализа и оценки рисков, присущих деятельности привлеченного Оператора УПИ;

- принятие мер, направленных на предупреждение и минимизацию рисков, присущих деятельности привлеченного Оператора УПИ;
- поддержание Расчетным центром ликвидности в объемах, необходимых для обеспечения обязательств по переводу денежных средств;
- надлежащую защиту информации;
- взаимодействие с Оператором при реализации мероприятий по управлению рисками;
- информационное взаимодействие с Оператором, установленного Правилами и указанного в разделе 12 Правил.

12. Порядок информационного взаимодействия Субъектов Системы и документационного обеспечения их деятельности по обеспечению БФПС

12.1. Документы, используемых Субъектами Системы при осуществлении деятельности по обеспечению БФПС

12.1.1. Субъекты Системы в целях управления непрерывностью функционирования Системы обязаны руководствоваться Правилами при осуществлении деятельности по обеспечению БФПС. Формы взаимодействия Субъектов Системы и управления рисками включают следующее:

- контроль Оператора за предоставлением Участниками и привлеченными Операторами УПИ информации о своей деятельности Оператору, в том числе в рамках информационного взаимодействия при выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- организацию Оператором работы службы круглосуточного мониторинга и поддержки Участников и их Клиентов;
- разработку Оператором при необходимости рекомендаций/требований, касающихся мероприятий по снижению уровня риска БФПС, и контроль за их применением Участниками и привлеченными Операторами УПИ;
- иные формы взаимодействия в части, не противоречащей Правилам.

12.1.2. Участники, привлеченные ОУПИ дополнительно разрабатывают, утверждают и реализуют в своей деятельности Планы ОНиВД.

12.1.3. Участники, привлеченные ОУПИ имеют право дополнительно разрабатывать документы, регламентирующие деятельность по обеспечению БФПС, по управлению рисками, защите информации.

12.1.4. Оператор, Расчетный центр осуществляют сбор, документирование и статистическую обработку первичной информации о функционировании Системы.

12.1.5. Первичная информация, в т.ч. включает:

- информацию о времени приема к исполнению, времени исполнения распоряжений Участников, количестве и суммах указанных распоряжений;
- информацию о размерах платежных клиринговых позиций, состоянии лимитов, о доступном остатке, о выполнении распоряжений и Реестров распоряжений Платежного клирингового центра.

12.1.6. Сбор, документирование и обработка информации может осуществляться автоматизированным способом с использованием специализированного программного обеспечения, применяемого Оператором и Расчетным центром.

12.1.7. Расчетный центр ежемесячно, не позднее 3 (третьего) рабочего дня месяца, следующего за отчетным, предоставляет Оператору по согласованным каналам связи сведения, используемые для расчета показателей БФПС.

12.2. Контроль за соблюдением операторами УПИ и участниками платежной системы порядка обеспечения БФПС

12.2.1. Деятельность по обеспечению БФПС осуществляется Субъектами Системы в соответствии с порядком обеспечения БФПС, установленным в Правилах, и контролируется Оператором.

12.2.2. Координацию деятельности Субъектов Системы по обеспечению БФПС и контроль за ней осуществляет Оператор путем определения в Правилах порядка обеспечения БФПС, проведения контроля порядка исполнения Субъектами Системы Правил, в том числе и в части обеспечения БФПС, мониторинга и анализа, осуществления иных мероприятий системы управления рисками в Системе.

12.2.3. Оператор осуществляет контроль за соблюдением привлеченными Операторами УПИ и Участниками порядка обеспечения БФПС в рамках осуществления контроля за соблюдением Правил.

В целях контроля за соблюдением Участниками и привлеченными Операторами УПИ порядка обеспечения БФПС Оператор:

- запрашивает и получает документы и информацию о деятельности, связанной с выполнением требований по обеспечению БФПС, в соответствии с порядком предоставления Участниками и Операторами УПИ информации о своей деятельности Оператору и в рамках информационного взаимодействия Субъектов Системы при выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- проводит на основе полученной информации анализ и оценку рисков;
- проводит проверку соответствия результатов оценки риска, включая риск нарушения БФПС, фактической информации о риске.

12.2.4. Контроль за соблюдением Участниками и Операторами УПИ порядка обеспечения БФПС осуществляется на постоянной основе посредством:

- расчета и анализа показателей БФПС;
- мониторинга уровней оказания услуг платежной инфраструктуры;
- мониторинга деятельности Расчетного центра и Участников в процессе оказания услуг в рамках Системы;
- анализа жалоб и обращений Участников, их Клиентов и Получателей.

12.2.5. Оператор при выявлении нарушения порядка обеспечения БФПС Операторами УПИ и Участниками выполняет следующие действия:

- информирует привлеченных Операторов УПИ и Участников о выявленных в их деятельности нарушениях, а также устанавливает сроки устранения нарушений;
- осуществляет проверку результатов устранения нарушений и информирует привлеченных Операторов УПИ и Участников, в деятельности которых выявлены нарушения, о результатах проведенной проверки.

12.2.6. Привлеченные Операторы УПИ и Участники несут ответственность за неисполнение порядка обеспечения БФПС.

а. Оператор, выполняющий в соответствии с Правилами функции Операционного центра и Платежного клирингового центра, отвечает за:

- организацию системы управления рисками в Системе в соответствии с требованиями законодательства Российской Федерации;

- последствия реализации рисков в осуществляемой деятельности вследствие неоказания (ненадлежащего оказания) услуг платежной инфраструктуры (за исключением услуг Расчетного центра);
- управление рисками путем контроля за выполнением Субъектами Системы своих функций, исходя из возложенной на них ответственности за оказание услуг по переводу денежных средств.

Ответственность Оператора за неоказание (ненадлежащее оказание) услуг платежной инфраструктуры установлена п. 4.1.15 Правил.

б. Расчетный центр и Участники несут ответственность за:

- несоблюдение требований законодательства Российской Федерации, нормативных актов Банка России, Правил и заключенных договоров;
- необеспечение надлежащего функционирования операционных и технологических средств, информационных систем, телекоммуникационных каналов, используемых для осуществления переводов денежных средств в рамках Системы;
- необеспечение надлежащей защиты информации при осуществлении переводов денежных средств в рамках Системы;
- несвоевременное обеспечение достаточности денежных средств на счетах, используемых для расчетов в рамках Системы;
- несоблюдение установленного Оператором регламента выполнения процедур;
- несоблюдение уровней оказания услуг платежной инфраструктуры.

За неисполнение порядка обеспечения БФПС по требованию Оператора Расчетным центром или Участниками уплачивается штраф. Размер штрафа устанавливается Оператором в пределах от 50 000 (Пятидесяти тысяч) рублей до 1 000 000 (Один миллион) рублей и определяется с учетом вида и повторяемости нарушения, характера ущерба (в том числе материального), причиненного Субъектам Системы, и способности Субъекта Системы к их устранению, а также последствий нарушения для безопасности и БФПС:

Нарушение	Размер штрафа
первое нарушение положений Правил, влияющих на БФПС	50 000 руб.
второе нарушение положений Правил, влияющих на БФПС, в течение 12 месяцев со дня первого нарушения	100 000 руб.
повторное нарушение одного и того же положения Правил, влияющих на БФПС, в течение 12 месяцев со дня первого нарушения	250 000 руб.
третье нарушение положений Правил, влияющих на БФПС, в течение 12 месяцев со дня первого нарушения	500 000 руб.
четвертое и последующие нарушения того же самого положения Правил, влияющих на БФПС, и Стандартов Системы в течение 12 месяцев со дня первого нарушения	1 000 000 руб.

13. Обеспечение защиты информации в Системе

13.1. Общие правила осуществления защиты информации

13.1.1. Оператор в Правилах устанавливает общие требования к защите информации, обрабатываемой Субъектами Системы, подлежащей обязательной защите в соответствии с законодательством Российской Федерации и Правилами.

13.1.2. Обязанности по определению порядка защиты информации распределяются между Оператором, Участниками и Операторами УПИ.

13.1.3. Защита информации при проведении операций по переводу денежных средств осуществляется Оператором, Участниками и Операторами УПИ в соответствии с требованиями, установленными Правилами, а также требованиями, предусмотренными законодательством Российской Федерации и ведомственными нормативными актами, в том числе с учетом специфики деятельности Субъекта Системы.

Субъекты Системы, являющиеся кредитными организациями, обеспечивают соответствие осуществляемой деятельности по защите информации требованиям и стандартам Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации.

13.1.4. Защита информации обеспечивается путем реализации Субъектами Системы правовых, организационных и технических мер, направленных:

- на соблюдение конфиденциальности информации;
- на реализацию права на доступ к информации в соответствии с законодательством Российской Федерации;
- на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления и распространения, а также от иных неправомерных действий в отношении информации.

13.1.5. К защищаемой в Системе информации относятся:

- информация о совершенных переводах денежных средств, в том числе информация, содержащаяся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений Участников, а также в извещениях (подтверждениях), касающихся исполнения распоряжений Участников;
- информация об остатках денежных средств на банковских счетах;
- информация, содержащаяся в оформленных в рамках применяемой формы безналичных расчетов распоряжениях Клиентов Участников, распоряжениях Участников, распоряжениях и Реестрах распоряжений Платежного клирингового центра;
- информации, хранящейся в операционном центре и Платежном клиринговом центре, о совершенных переводах денежных средств с использованием Электронных средств платежа;
- информация о платежных клиринговых позициях;
- информация, необходимая для удостоверения Клиентами права распоряжения денежными средствами, в том числе данных держателей Электронных средств платежа;
- информация о конфигурации, определяющей параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается Участниками, Операторами услуг платежной инфраструктуры, и используемых для осуществления переводов денежных

средств, а также информация о конфигурации, определяющей параметры работы технических средств по защите информации;

- ключевая информация средств криптографической защиты информации, используемых при осуществлении переводов денежных средств;
- информация ограниченного доступа, в том числе персональные данные, подлежащая обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемая при осуществлении переводов денежных средств.

13.1.6. Субъекты Системы утверждают внутренние нормативные документы, устанавливающие порядок реализации требований к защите информации.

13.2. Требования к обеспечению защиты информации

13.2.1. Субъекты Системы обязаны обеспечивать защиту информации при осуществлении переводов денежных средств в соответствии с законодательством Российской Федерации, нормативными актами Правительства Российской Федерации и Банка России, определяющих требования к обеспечению защиты информации, в том числе при осуществлении переводов денежных средств (далее – требования к защите информации).

13.2.2. Требования к обеспечению защиты информации включают в себя:

- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при назначении и распределении функциональных прав и обязанностей лиц, связанных с осуществлением переводов денежных средств;
- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры;
- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при осуществлении доступа к объектам информационной инфраструктуры, включая требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации от несанкционированного доступа;
- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код);
- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при использовании сети интернет при осуществлении переводов денежных средств;
- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при использовании средств криптографической защиты информации;
- требования к обеспечению защиты информации при осуществлении переводов денежных средств с использованием взаимосвязанной совокупности организационных мер защиты информации и технических средств защиты информации, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (далее - технологические меры защиты информации);
- требования к организации и функционированию подразделения (работника), ответственного за организацию и контроль обеспечения защиты информации;

- требования к повышению осведомленности работников Участников, Операторов услуг платежной инфраструктуры и Клиентов в области обеспечения защиты информации;
- требования к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и реагированию на них;
- требования к определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств;
- требования к оценке выполнения Оператором, Участником, Оператором услуг платежной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- требования к доведению Участником, привлеченным Оператором услуг платежной инфраструктуры до Оператора информации об обеспечении в Системе защиты информации при осуществлении переводов денежных средств;
- требования к совершенствованию Оператором, Участником, Оператором услуг платежной инфраструктуры защиты информации при осуществлении переводов денежных средств.

13.2.3. Для проведения работ по защите информации и контроля (оценки) соблюдения требований к защите информации Субъектами Системы могут привлекаться на договорной основе организации, имеющие лицензии на деятельность по технической защите конфиденциальной информации и (или) на деятельность по разработке и производству средств защиты конфиденциальной информации.

13.2.4. Субъекты Системы обязаны пересматривать действующий порядок обеспечения защиты информации при осуществлении переводов денежных средств в случаях:

- изменения законодательства Российской Федерации;
- изменения требований Банка России к обеспечению защиты информации в национальной платежной системе;
- совершенствования защиты информации в Системе;
- выявления недостатков при осуществлении контроля защиты информации в Системе.

13.3. Порядок обеспечения защиты информации в Системе

13.3.1. В целях обеспечения защиты информации в Системе при хранении, обработке, обмене защищаемой информации Субъекты Системы обеспечивают применение, включая, но, не ограничиваясь организационными мерами защиты информации, соблюдением стандартов Банка России в области защиты информации, поддержкой программ управления уязвимостями, созданием и поддержанием безопасной сетевой инфраструктуры, мониторингом сетевой инфраструктуры, а также внедрением и поддержанием мер по управлению доступом к защищаемой информации.

13.3.2. Субъекты Системы обеспечивают защиту информации при осуществлении переводов денежных средств с учетом распределения функциональных прав и обязанностей лиц, связанных с осуществлением переводов денежных средств в Системе.

13.3.3. В рамках создания и поддержания безопасной сетевой инфраструктуры Субъекты Системы обеспечивают поддержку конфигурации межсетевых экранов для защиты данных, обеспечивающую анализ проходящей через них информации, а также обеспечивающую ограничение прямого доступа извне к компонентам системы, содержащим защищаемую информацию.

13.3.4. В рамках реализации мер по поддержке программы управления уязвимостями Субъекты Системы обязаны выполнять установленные Правилами требования к обеспечению защиты информации от воздействия вредоносных кодов, обеспечить использование на всех компонентах системы, задействованных в хранении, обработке и обмене защищаемой

информацией только актуальных версий программных обеспечений, разработанных для целей противодействия внешнему или внутреннему использованию уязвимостей.

13.3.5. В рамках реализации мероприятий по внедрению и поддержанию мер управления доступом к защищаемой информации Субъекты Системы обязаны ограничить доступ и вести учет лиц, имеющих доступ к защищаемой информации. в том числе Субъекты Системы обеспечивают:

- предоставление доступа к Системе только тем лицам, которым такой доступ необходим для выполнения возложенных на них функций, в том числе связанных с осуществлением переводов денежных средств в Системе
- учет лиц, имеющих доступ к защищаемой информации;
- предоставление доступа каждому сотруднику с использованием уникального имени, учетной записи, пароля и/или ключа электронной подписи для доступа к защищаемой информации;
- многокомпонентность и многоразрядность (не менее пяти символов) используемых паролей, а также периодическую смену паролей;
- немедленный отзыв доступа при прекращении полномочий лица на доступ к защищаемой информации;
- ограничение доступа к техническим средствам автоматизированных систем, обеспечивающих взаимодействие в Системе;
- недопущение использования установленных производителем программного обеспечения паролей и иных параметров безопасности, устанавливаемых по умолчанию;
- ограничение доступа к материальным носителям, содержащим защищаемую информацию или её архивные и резервные копии, строгий контроль за хранением материальных носителей;
- включение в должностные обязанности работников, участвующих в обработке информации, обязанности по выполнению требований к защите информации;
- включение в должностные обязанности работников, участвующих в обработке информации, обязанности сообщения о подозрительных событиях в Системе, которые могут быть квалифицированы как инциденты безопасности;
- приостановление обработки информации Субъектом в случае инцидента безопасности, до устранения причин инцидента и/или предотвращения его возможных последствий.
- выявление инцидентов, связанных с нарушением требований к защите информации, немедленное сообщение Оператору Системы об инцидентах безопасности;
- контроль применения в автоматизированных системах Участников технических средств защиты информации (криптографические средства, средства защиты ПК от несанкционированного доступа, средства антивирусной защиты, средства межсетевого экранирования, системы обнаружения вторжений, средства контроля (анализа) защищенности) и оценка выполнения требований к защите информации на собственных объектах инфраструктуры не реже 1 раза в 2 года.

13.3.6. В рамках реализации мер по мониторингу сетевой инфраструктуры Субъекты Системы должны контролировать доступ к сетевым ресурсам и защищаемой информации, для чего организуют мониторинг событий, касающихся доступа к сетевым ресурсам, регистрируют действия пользователей, необходимых для проведения расследования и анализа причин инцидентов, обеспечивают хранение журналов событий не менее одного года, а в оперативном доступе не менее трех месяцев, обеспечивают плановую и внеплановую (при

внесении изменений) проверку систем, процессов и программного обеспечения для поддержания их защищенности на должном уровне.

13.3.7. Субъекты Системы определяют подразделение (сотрудника), ответственное за организацию и контроль обеспечения защиты информации, задачей которого, в том числе, является повышение осведомленности работников в области обеспечения защиты информации.

13.3.8. В части, не установленной в Правилах, Субъекты Системы, руководствуясь законодательством Российской Федерации и страны своего местонахождения, самостоятельно определяют порядок обеспечения защиты информации при выполнении своих функций в Системе при осуществлении переводов денежных средств, в том числе определяют состав и порядок применения организационных мер защиты информации, состав и порядок использования технических средств защиты информации, включая информацию о конфигурации технических средств защиты информации, определяющую параметры их работы, порядок регистрации и хранения информации на бумажных носителях и (или) в электронном виде, содержащей подтверждения выполнения порядка применения организационных мер защиты информации и использования технических средств защиты информации.

13.3.9. Субъекты Системы обязаны совершенствовать методы, процедуры, техническое и программное оснащение, обеспечивать соответствие требованиям в области защиты информации, предъявляемым действующим законодательством Российской Федерации и нормативными актами Банка России, уполномоченных органов исполнительной власти, и Правил с учетом изменяющихся и совершенствующихся угроз защиты информации при осуществлении переводов денежных средств.

13.3.10. Несоблюдение требований по защите информации, полученной Субъектом Системы в связи с выполнением возложенных на него функций в соответствии с Правилами, приведшее к нарушению конфиденциальности, доступности и целостности информации является существенным нарушением Правил и основанием для принятия Оператором мер воздействия, предусмотренных Правилами, вплоть до решения о расторжении в одностороннем порядке договора участия с указанным Субъектом Системы и прекращением его функций.

13.4. Использование средств криптографической защиты информации

13.4.1. В рамках Системы в процессе электронного обмена информацией в случаях, установленных Правилами, а также договорами, заключаемыми между Субъектами Системы для защиты информации используются средства криптографической защиты информации (шифрования) либо программно-аппаратные средства, содержащие модули криптографической защиты информации.

13.4.2. Для защиты электронных сообщений в Системе применяются средства электронной подписи, обеспечивающие работу "с открытым ключом". При обмене информацией между Субъектами Системы используются:

- средства криптозащиты, реализующие электронную подпись по ГОСТ 2012, сертифицированные ФСБ России, для обмена с абонентами - резидентами Российской Федерации;
- средства криптозащиты, входящие в состав операционных систем, реализующие электронную подпись по алгоритму RSA с длиной ключа не менее 2048 бит.

13.4.3. Также в Системе используются средства криптозащиты, входящие в состав операционных систем, реализующие криптографический протокол транспортного уровня TLS 1.2, с шифрованием AES на ключе не менее 192 бит и хешированием SHA разрядности не менее 256 бит.

13.4.4. Выбор используемых средств криптографической защиты информации осуществляется по соглашению сторон электронного обмена.

13.4.5. Доступ Участников, Расчетного центра к ПК «КП РИТЕЙЛ» осуществляется посредством «тонкого» клиента с использованием усиленной квалифицированной подписи, выданной удостоверяющим центром, имеющем аккредитацию Минкомсвязи России. Каждому пользователю, имеющему доступ к ПК «КП РИТЕЙЛ», назначается роль администратора или пользователя. Вход пользователя/администратора в ПК «КП РИТЕЙЛ» организуется посредством введения уникального логина и пароля.

13.5. Требования к обеспечению защиты информации от воздействия вредоносного кода на инфраструктуру Системы

13.5.1. Субъекты Системы в целях снижения возможных потерь от воздействия вредоносного кода, путем предотвращения проникновения и распространения, а также своевременного уничтожения вредоносного кода, обязаны обеспечить выполнение следующих требований:

- самостоятельно организовать работу по защите информации от воздействия вредоносных кодов, включающая в том числе меры, осуществляемые для предотвращения воздействия вредоносного кода, меры, направленные на выявление проникновения вредоносного кода, меры реагирования на данный вид инцидентов безопасности;
- использование технических средств защиты информации, предназначенных для выявления вредоносного кода и для предотвращения воздействия вредоносного кода на объектах информационной инфраструктуры (далее – антивирусные средства);
- регулярное обновление версий антивирусных средств и баз данных, используемых в работе антивирусных средств и содержащих описание вредоносных кодов и способы их обезвреживания, обеспечивая их актуальность;
- функционирование антивирусных средств в автоматическом неотключаемом режиме;
- обеспечение антивирусного контроля при обмене данными с недоверенными сетями передачи данных;
- проведение регулярного анализа информации из общедоступных источников о новых видах вредоносных кодов для своевременной организации противодействия новым угрозам.

13.5.2. Субъекты Системы обеспечивают использование технических средств защиты информации от воздействия вредоносного кода различных производителей и их отдельную установку на персональных электронных вычислительных машинах и серверах, используемых для осуществления переводов денежных средств, а также на межсетевых экранах, задействованных в осуществлении переводов денежных средств, при наличии технической возможности.

При наличии технической возможности Субъекты Системы обеспечивают выполнение проверки на отсутствие вредоносного кода средств вычислительной техники, включая Устройства приема платежей, выполняемой после установки или изменения программного обеспечения.

13.5.3. В случае обнаружения вредоносного кода или факта воздействия вредоносного кода, обнаруживший вредоносный код Субъект Системы, обеспечивают принятие мер, направленных на предотвращение распространения вредоносного кода и устранение последствий воздействия вредоносного кода.

13.5.4. Субъекты Системы при необходимости приостанавливают осуществление переводов денежных средств на период устранения последствий заражения вредоносным кодом.

13.5.5. В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Участник, привлеченные ОУПИ обеспечивают информирование Оператора; Оператор обеспечивает информирование привлеченных Операторов УПИ и Участников.

13.5.6. При обнаружении Субъектом Системы проникновения вредоносных кодов в средства вычислительной техники, задействованные в информационном обмене в рамках Системы, он прекращает информационный обмен в электронном виде с другими Субъектами Системы, и по любому из доступных каналов связи, в том числе посредством телефонной связи, по факсу информирует таких Субъектов Системы и Оператора о возникшей ситуации, включая сведения о причинах и последствиях, после чего принимает меры реагирования, предусмотренные локальными актами Субъекта Системы на случай возникновения данного вида инцидента безопасности.

13.5.7. Субъект Системы информирует стороны информационного обмена в электронном виде по согласованным каналам связи о возобновлении указанного вида информационного обмена после восстановления нормального функционирования средств, используемых в электронном обмене.

13.6. Обеспечение защиты персональных данных в Системе

13.6.1. Субъекты Системы обеспечивают в своей деятельности соблюдение требований законодательства Российской Федерации и страны своего местонахождения о работе с персональными данными и несут предусмотренную законодательством Российской Федерации и страны своего местонахождения ответственность за несоблюдение указанных требований.

13.6.2. Участники в случае, если указанное ниже предусмотрено законодательством Российской Федерации и страны своего местонахождения, информируют и, в случае необходимости, получают согласие лиц на обработку их персональных данных и предоставление их персональных данных Субъектам Системы.

13.7. Обеспечение банковской и коммерческой тайны в Системе

13.7.1. Участники в случае, если указанное предусмотрено законодательством Российской Федерации, информируют и, в случае необходимости, получают согласие Клиентов на предоставление информации, относящейся к банковской тайне, Субъектам Системы.

13.7.2. Субъекты Системы обеспечивают в своей деятельности соблюдение требований законодательства Российской Федерации о гарантировании банковской и коммерческой тайны в отношении информации, ставшей известной Субъекту Системы в связи с выполнением возложенных на него функций в соответствии с Правилами.

13.8. Порядок реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия Клиента Участника

13.8.1. Оператор устанавливает порядок и реализует в Системе мероприятия, которые в совокупности образуют систему выявления и мониторинга переводов денежных средств без согласия Клиента в Системе.

13.8.2. Субъекты Системы, в целях исключения риска осуществления переводов денежных средств без согласия Клиента Участника:

- реализуют определенные актами Банка России мероприятия по противодействию осуществлению переводов денежных средств без согласия Клиента;
- в рамках информационного взаимодействия направляют информацию, полученную в ходе реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия Клиента Участника, в порядке, установленном в пп. 13.8.5 Правил.

13.8.3. Субъекты Системы применяют информацию, содержащуюся в формируемой Банком России базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, в целях выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия Клиента.

13.8.4. При выявлении информации о технических данных, описывающих компьютерные атаки, направленные на информационную инфраструктуру Субъектов Системы и (или) Клиентов Участников, Субъекты Системы осуществляют мероприятия по противодействию осуществлению переводов денежных средств без согласия Клиента в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 08 августа 2017 года № 822-ст «Об утверждении национального стандарта».

13.8.5. В рамках информационного взаимодействия Субъекты Системы обязаны информировать о случаях и (или) попытках осуществления переводов денежных средств без согласия Клиента и компьютерных атаках, направленных на объекты информационной инфраструктуры Субъектов Системы и (или) Клиентов Участников, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия Клиента:

- Банк России в случаях, в порядке и в сроки, установленные нормативным актом Банка России, регулирующим порядок направления в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия Клиента;
- Оператора во всех случаях в соответствии с порядком взаимодействия в рамках Системы в чрезвычайных ситуациях.

Привлеченные Операторы УПИ и Участники по ранее направленной в адрес Оператора информации о технических данных, описывающих компьютерные атаки, уведомляют Оператора о предпринятых и (или) предпринимаемых мерах для противодействия выявленным компьютерным атакам, направленным на объекты информационной инфраструктуры привлеченных Операторов УПИ, Участников и (или) Клиентов Участников, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия Клиента в рамках Системы.

13.8.6. Оператор в рабочем порядке изучает полученную информацию и, в случае необходимости, может запросить дополнительную информацию, а также создать рабочую группу для разработки и реализации мер, направленных на предотвращение и устранение воздействия компьютерной атаки.

13.8.7. Оператор при получении запроса от Банка России направляет в Банк России информацию о переводах без согласия Клиента, указанных в запросе Банка России, в виде электронных сообщений по запросу в установленный в запросе Банка России срок.

13.9. Порядок информационного взаимодействия при выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств

13.9.1. Субъект Системы при выявлении в Системе инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, влекущих нарушение взаимодействия в рамках Системы, принимает меры по снижению негативных последствий, вызванных нарушением требований, информирует Оператора и Субъекта Системы, в функциональной зоне ответственности которого находится область возникновения инцидента, в порядке и сроки, определенные в порядке взаимодействия в рамках Системы в чрезвычайных ситуациях. Субъект Системы, допустивший инцидент, реализует комплекс мер, направленных на устранение причин, вызвавших инцидент, и на недопущение его повторного возникновения, и последствий инцидента.

Информирование Оператора о выявленных в отчетном месяце Участниками и Операторами УПИ инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, осуществляется ежемесячно (не позднее третьего рабочего дня месяца, следующего за отчетным) в случае, если в отчетном месяце инциденты имели место. При отсутствии инцидентов информирование Оператора Участниками и Операторами УПИ об отсутствии инцидентов не осуществляется.

13.9.2. Информирование Оператора осуществляется путем направления сообщения, составленного на бумажном носителе, подписанного уполномоченным лицом Участника или привлеченного Оператора УПИ, или в электронном виде по согласованным каналам связи. Сообщение в обязательно порядке включает описание инцидента, информацию о событиях, по мнению отправителя, вызвавших инцидент, о его причинах и последствиях. Сообщение может содержать иную информацию, которую Субъект Системы считает необходимым сообщить Оператору.

13.9.3. Участник, привлеченный ОУПИ обеспечивает регистрацию самостоятельно выявленных инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств.

Участник обеспечивает регистрацию ставших ему известными инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, выявленных Клиентами данного Участника.

Участник обеспечивает регистрацию ставших ему известными инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, выявленных БПА (БПС).

13.9.4. Участник, привлеченный ОУПИ определяют во внутренних документах порядок регистрации и хранения сведений об инцидентах, указанных в пп. 13.9.3 Правил.

13.9.5. Привлеченные ОУПИ и Участники в составе информации о своей деятельности, представляемой в порядке и сроки, определенные Правилами, представляют данные для целей анализа обеспечения в Системе защиты информации при осуществлении переводов денежных средств. При этом состав указанных данных должен соответствовать требованиям нормативных актов Банка России, регламентирующих требования к обеспечению защиты информации в Системе при осуществлении переводов денежных средств.

13.9.6. Оператор обеспечивает регистрацию в собственной информационной системе всех выявленных Субъектами Системы инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств.

13.9.7. Оператор информирует привлеченных ОУПИ и Участников о выявленных в Системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, а также о рекомендуемых методиках анализа и реагирования на указанные инциденты путем размещения соответствующей информации на Официальном сайте Оператора в сети интернет, или направляя им информацию по согласованным каналам связи.

13.9.8. Субъекты Системы обязаны проводить ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

Для проведения анализа уязвимостей в прикладном программном обеспечении автоматизированных систем и приложений Участникам, привлеченным Операторам УПИ рекомендуется привлекать организацию, имеющую лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение соответствующих работ и услуг.

Оператор, Участники, привлеченные ОУПИ обязаны пересматривать действующий порядок обеспечения защиты информации при осуществлении переводов денежных средств в связи с изменениями требований к защите информации, определенных законодательными актами Российской Федерации, нормативными актами Правительства Российской Федерации и Банка России, Правилами, изменениями установленных в Правилах требований к защите

информации, выявлением недостатков при осуществлении контроля выполнения порядка обеспечения защиты информации, в сроки, обеспечивающие исполнение Субъектами Системы требований пп. 13.2.2 Правил.

13.10. Порядок информационного взаимодействия для целей анализа обеспечения в Системе защиты информации

13.10.1. Привлеченные ОУПИ и Участники предоставляют Оператору информацию для целей анализа обеспечения защиты информации в Системе.

13.10.2. Содержание предоставляемой информации определяется Оператором, но в обязательном порядке должно отражать вопросы соблюдения Правил в части защиты информации, проведения оценки Субъектами Системы обеспечения защиты информации при осуществлении переводов денежных средств в рамках Системы.

13.10.3. Информация предоставляется Операторами УПИ и Участниками по запросу Оператора не реже 1 раза в два года.

13.10.4. Форма предоставления информации определяется Оператором в соответствующем запросе.

14. Приложения, являющиеся неотъемлемой частью Правил:

Приложение №1. Тарифы (перечень и стоимость услуг).

Приложение №2. Регламент электронного документооборота.

Приложение № 1 к Правилам. Тарифы

ТАРИФЫ

Платежной системы «КП Ритейл»

Категория перевода денежных средств	Тип операции	Тарифы для Отправителей/Плательщиков (ТДК)	Тарифы для Участников отправляющих (ТУО) и выдающих (ТУИ) переводы
Оплата в пользу юридических лиц за товары, работы, услуги	<ul style="list-style-type: none"> - От физических лиц для зачисления на счета физических лиц в кредитных организациях, в том числе переводы на карты Visa, MasterCard; - От физических лиц юридическим лицам/индивидуальным предпринимателям в счет оплаты услуг; - От физических лиц юридическим лицам, при предоставлении полных реквизитов платежа 	<ul style="list-style-type: none"> - От 0% до 25% от суммы Перевода денежных средств; -и/или фиксированная сумма от 0 до 1000 рублей 	<ul style="list-style-type: none"> - От 0% до 75% от суммы комиссии, уплачиваемой Клиентом в соответствии с Тарифами для Клиентов; -и/или от 0% до 20% от суммы Перевода денежных средств; - и/или фиксированная сумма от 0 до 400 рублей

Вознаграждение Оператора, выполняющего функции ОЦ и ПКЦ рассчитывается по следующей формуле:

$ТДК - ТУО - ТУИ = \text{Вознаграждение Оператора}$

Сумма удерживаемой Комиссии за перевод округляется к ближайшему целому (математическое округление).

Комиссия взимается в валюте перевода, если иное не установлено соответствующим договором Участника с Оператором.

Приложение № 2 к Правилам. Регламент электронного документооборота

Регламент электронного документооборота (РЭДО)

Термины и определения, используемые в Регламенте электронного документооборота и Правилах, связанные с электронным документооборотом, имеют следующее значение:

Абонент	Клиент, Субъект Системы.
Информационная Система	Корпоративная информационная система, обеспечивающая Электронный документооборот между Абонентом и Операционным центром.
Отправляющая сторона	Сторона электронного взаимодействия, которая направляет Электронное сообщение с использованием Информационной системы.
Подтверждение подлинности ЭП в Электронном документе	Положительный результат проверки соответствующим средством Электронной подписи с использованием Сертификата ключа проверки электронной подписи принадлежности электронной подписи в Электронном документе Владельцу сертификата ключа проверки электронной подписи и отсутствия искажений в подписанном данной электронной подписью Электронном документе.
Принимающая сторона	Сторона электронного взаимодействия, которой Электронное сообщение отправлено с использованием Информационной системы.
Точка информационного обмена	Программно-аппаратный комплекс, работающий на стороне Абонента, которому присвоен код в Системе, непосредственно осуществляющий информационный обмен с Операционным центром.
Формат Электронного документа	Структура содержательной части Электронного сообщения, на основе которого сформирован Электронный документ.
Криптографические ключи (ключи)	Создаваемые с помощью программного обеспечения ключ электронной подписи и парный ему ключ проверки электронной подписи
Ключ электронной подписи (Ключ ЭП)	Уникальная последовательность символов, предназначенная для создания электронной подписи
Ключ проверки электронной подписи	Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее – проверка электронной подписи)
Сертификат ключа проверки электронной подписи (Сертификат)	Электронный документ, выданный Удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи

Владелец сертификата ключа проверки электронной подписи (Владелец сертификата)	Физическое лицо, на имя которого Удостоверяющим центром выдан Сертификат ключа проверки электронной подписи и которое имеет право подписи ЭД с использованием ЭП и право подписи на финансовых документах.
Уполномоченное лицо	Сотрудник Абонента или оператора услуг платежной инфраструктуры, получивший право подписи ЭД от имени Владельца сертификата ключа проверки электронной подписи.
Электронная подпись (ЭП)	Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием ключа квалифицированной электронной подписи и позволяющий идентифицировать Владельца сертификата, а также установить отсутствие искажения информации в электронном документе.
Электронное сообщение	Логически целостная совокупность структурированных данных, имеющих смысл для участников информационного взаимодействия. Информация в Электронном сообщении представлена в электронно-цифровой форме, позволяющей обеспечить ее обработку средствами вычислительной техники, передачу по каналам связи и хранение на машиночитаемых носителях информации.
Электронный документ (ЭД)	Электронное сообщение, подписанное ЭП Субъекта Системы и имеющее равную юридическую силу с расчетными и иными документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати Субъекта Системы.
Электронный документооборот (ЭДО)	Обмен Электронными документами и Электронными сообщениями в Системе в соответствии с Правилами.
Компрометация ключа электронной подписи	Событие, определенное Владельцем сертификата ключа проверки электронной подписи как ознакомление неуполномоченным лицом (лицами) с его ключом электронной подписи;
Код оповещения	Уникальная последовательность цифр, вырабатываемая для Абонента, предназначенная для идентификации Абонента при передаче сообщений о компрометации ключа и высылаемая Абоненту в зашифрованном виде при первоначальном подключении и при восстановлении связи в случае компрометации действующего ключа.

Общие правила ЭДО

- 1) Информационное взаимодействие в процессе оказания Услуг Системы осуществляется посредством обмена электронными сообщениями, а также подтверждениями в их получении Принимающей стороной или ответа.
- 2) Применяемые в Системе средства защиты обеспечивают конфиденциальность, целостность и подлинность ЭД при осуществлении Сторонами обмена ЭД с использованием общедоступных каналов связи и нескомпрометированных ключей.

- 3) Электронные документы имеют равную юридическую силу с соответствующими документами на бумажных носителях информации, подписанными Владельцами сертификатов, если соблюдены следующие условия:
- Сертификаты, относящиеся к этим ЭП, изготовлены Удостоверяющим центром, имеющим аккредитацию Минкомсвязи России, и не утратили силу (действуют) на момент проверки подлинности подписи ЭД или на момент подписания ЭД
 - Подтверждена подлинность этих ЭП.
 - Владелец сертификата уполномочен от имени Отправляющей стороны подписывать расчетные и иные документы на бумажных носителях.
- 4) Единой шкалой времени при осуществлении ЭДО является московское поясное время. Контрольным является время системных часов аппаратных средств Операционного центра.

Электронные сообщения и документы

Категории Электронных сообщений

1) Электронные сообщения подразделяются на следующие категории:

Категория 1 – Электронные сообщения, не требующие наличие ЭП Отправляющей стороны и не требующие ответа.

Категория 2 – Электронные сообщения, требующие наличие ЭП Отправляющей стороны и не требующие ответа.

Категория 3 – Электронные сообщения, требующие наличие ЭП Отправляющей стороны и требующие ответа, не содержащего ЭП Принимающей стороны.

Категория 4 – Электронные сообщения, требующие наличие ЭП Отправляющей стороны и требующие ответа, подписанного ЭП Принимающей стороны.

2) К категории 1 относятся только информационные сообщения, не влекущие за собой юридических или финансовых последствий для Отправляющей стороны и/или Принимающей стороны.

3) Все отправляемые Клиентами, Участниками и Расчетным центром сообщения в рамках Системы являются Электронными документами, т.е. относятся к категориям 2, 3 или 4.

Условия признания Электронного сообщения отправленным

Электронное сообщение считается отправленным Отправляющей стороной в случае успешного завершения технических функций отправки. Датой и временем отправки считаются дата и время завершения технических функций отправки.

Условия признания Электронного сообщения полученным

Электронное сообщение считается полученным Принимающей стороной в случае:

Для категорий 1 и 2 – в момент его успешной отправки Отправляющей стороной.

Для категории 3 – в момент его получения Принимающей стороной. Датой и временем приема считаются дата и время его получения.

Для категории 4 - В момент получения Отправляющей стороной подтверждающего технологического ответа от Принимающей стороны о доставке сообщения Принимающей стороной. Датой и временем приема считаются дата и время формирования подтверждающего технологического ответа Отправляющей стороной.

Условия принятия Электронных сообщений в обработку Принимающей стороной

Электронное сообщение и ответ на него принимается в обработку в случае, если:

1) Сообщение успешно расшифровано - для сообщений, обмен которых происходит с использованием шифрования.

2) Получен положительный результат проверки Электронного сообщения – для сообщений, относящихся к категории 2, 3 или 4.

- 3) Электронное сообщение надлежащим образом оформлено, т.е. его формат соответствует формату такого сообщения, предусмотренному на момент формирования документа технологией Системы.

Условия организации и правила осуществления ЭДО

Общие положения организации ЭДО

1) Электронный документооборот может включать:

- формирование Электронного сообщения;
- отправку и доставку Электронного сообщения;
- проверку Электронного сообщения;
- подтверждение получения Электронного сообщения и ответ на него;
- учет входящих и исходящих Электронных документов;
- хранение Электронных документов;
- создание дополнительных Экземпляров электронного документа и бумажных копий Электронного документа.

Формирование Электронного сообщения:

Формирование электронного сообщения осуществляется в следующем порядке:

- формирование Электронного сообщения в формате, установленном для данного Электронного сообщения;
- подписание сформированного Электронного сообщения ЭП, при необходимости.
- шифрование Электронного сообщения, при необходимости;
- отправка Электронного сообщения.

Особенности отправки, доставки и получения Электронных сообщений могут устанавливаться дополнительными договорами, заключаемыми с Контрагентами.

Проверка подлинности доставленного Электронного документа

1) Проверка Электронного сообщения включает:

- расшифровку Электронного сообщения, при необходимости;
- проверку Электронного сообщения на соответствие установленному для него формату;
- проверку подлинности ЭП Электронного сообщения, при её наличии.

2) В случае положительного результата проверки Электронного сообщения, данное Электронное сообщение признается надлежащим. В противном случае Электронное сообщение считается не полученным, о чем Принимающая сторона может послать уведомление Отправляющей стороне.

Учет Электронных документов

1) Учет Электронных документов осуществляется путем ведения электронных журналов учета или журналов учета на бумажном носителе. Технология ведения электронных журналов учета должна включать программно-технологические процедуры заполнения и администрирования электронных журналов и средства хранения этой информации. Программные средства ведения электронных журналов учета являются составной частью программного обеспечения, используемого для организации электронного документооборота.

2) Для выполнения текущих работ по ведению учета Электронных документов назначаются ответственные лица.

3) Абоненты обеспечивают защиту от несанкционированного доступа и непреднамеренного уничтожения и/или искажения учетных данных, содержащихся в электронных журналах учета Электронных документов. Срок хранения учетных данных не может быть менее 5 лет.

Хранение электронных документов

- 1) Все учтенные Электронные документы должны храниться в течение сроков, предусмотренных Правилами. Электронные документы должны храниться либо в электронных архивах, либо в виде копий Электронных документов на бумажных носителях, заверенных ответственным лицом Абонента.
- 2) Если Правилами, а также дополнительными договорами, заключаемыми с Абонентами, не предусмотрено иное, Электронные документы должны храниться в том же формате, в котором они были сформированы, отправлены или получены. Срок хранения электронных документов не может быть менее 5 лет.
- 3) Хранение Электронных документов должно сопровождаться хранением соответствующих электронных журналов учета, сертификатов ключей проверки ЭП и программного обеспечения, обеспечивающего возможность работы с электронными журналами и проверки ЭП хранимых Электронных документов.
- 4) Обязанности хранения электронных документов возлагаются на Абонентов.
- 5) Для выполнения текущих работ по ведению электронных архивов в системах обработки данных Абоненты назначают ответственных лиц.
- 6) Электронные архивы подлежат защите от несанкционированного доступа и непреднамеренного или преднамеренного уничтожения и/или искажения.

Копии Электронного документа на бумажном носителе

- 1) Электронный документ может иметь неограниченное количество экземпляров, в том числе выполненных на машиночитаемых носителях различного типа. Для создания дополнительного экземпляра существующего Электронного документа осуществляется воспроизводство содержания документа вместе с ЭП.
- 2) Все экземпляры Электронного документа являются подлинниками данного Электронного документа.
- 3) Копии Электронного документа могут быть изготовлены (распечатаны) на бумажном носителе и должны быть заверены собственноручной подписью уполномоченного лица Субъекта, являющимся Отправляющей или Принимающей стороной.

Обеспечение информационной безопасности при ЭДО

Общие положения информационной безопасности

- 1) Абоненты самостоятельно обеспечивают информационную безопасность при организации ЭДО внутри своей корпоративной информационной системы.

Для криптографической защиты информации в системе применяются:

- 1) СКЗИ CryptoPro CSP на основе сертифицированных ФСБ России ГОСТ алгоритмов, или совместимые с ним
- 2) СКЗИ, встроенные в операционную систему, на основе криптографического алгоритма с открытыми ключами RSA – для Абонентов – нерезидентов Российской Федерации
- 3) Криптографический протокол TLS

Общие условия работы с ключевой информацией

- 1) Абоненты при действиях по выработке, смене и компрометации ключа руководствуются правилами Удостоверяющего центра.
- 2) Правила Удостоверяющего центра на русском языке размещены на официальном сайте Удостоверяющего центра.
- 3) Выполнение требований Удостоверяющего центра при работе с ключевой информацией обязательно для всех Абонентов.
- 4) Абоненты самостоятельно вырабатывают криптографические ключи и обеспечивают работу с ключевой информацией.

- 5) Владелец сертификата должен быть уполномочен подписывать расчетные и иные документы на бумажных носителях от имени Отправляющей стороны, на момент отправки подписанного ЭП Электронного сообщения.
- 6) При проверке документов для регистрации сертификата ключа проверки электронной подписи за Абонентом, Операционный центр в полном объеме проверяет документы Абонента, полномочия уполномоченного лица на право осуществления действий от имени Абонента в рамках Системы.
- 7) Владелец сертификата ключа проверки электронной подписи несёт ответственность за достоверность сведений, которые были предоставлены им Оператору Системы при создании и регистрации сертификата ключа проверки электронной подписи.
- 8) Владелец сертификата ключа проверки электронной подписи хранит собственные ключи электронной подписи в тайне и принимает все необходимые меры для предотвращения их компрометации в процессе хранения и использования.
- 9) Владельцы сертификатов ключей проверки электронной подписи самостоятельно хранят выданные им сертификаты ключей, в том числе и по истечению срока действия сертификата.
- 10) Владелец сертификата ключа проверки электронной подписи вправе передать право на использование ключей Уполномоченному лицу, в том числе по их использованию в составе аппаратно-программных средств, осуществляющих автоматическую обработку информации.
- 11) В каждой точке информационного обмена может использоваться один и только один действующий ключ.
- 12) Для обеспечения непрерывности ЭДО на каждый действующий ключ Абонент должен иметь резервный ключ и резервные копии криптографических ключей, если это предусмотрено правилами Удостоверяющего центра.

Требования по организации хранения и использования носителей ключевой информации

- 1) Субъект Системы самостоятельно генерирует криптографические ключи. Каждый ключ генерируется для одного работника Субъекта - Владельца ключа. Допускается генерация нескольких ключей одного Владельца, в том числе резервных ключей.
- 2) Подразделение Субъекта, ответственное за организацию и контроль обеспечения защиты информации в Системе, ведет поэкземплярный учет используемых в Системе криптографических средств защиты информации и изготовленных криптографических ключей, разрабатывает внутренний Порядок хранения и использования ключей и носителей ключевой информации. Администрирование ключевой информации возлагается на Администратора защиты информации (Администратора безопасности).
- 3) Порядок хранения и использования носителей ключевой информации должен исключать возможность использования ключей лицами, не являющимися их Владельцами.
- 4) Владельцам запрещается:
- 5) передавать носители ключевой информации лицам, к ним не допущенным;
- 6) выводить ключи электронной подписи на дисплей или принтер;
- 7) вставлять носитель ключевой информации в считывающее устройство компьютера в режимах, не предусмотренных функционированием АРМ, а также в считывающие устройства других компьютеров;
- 8) оставлять носитель ключевой информации без присмотра на рабочем месте;
- 9) записывать на носитель ключевой информации посторонние файлы.

- 10) Владелец ключа электронной подписи вправе использовать ключ в составе аппаратно-программных средств, осуществляющих автоматическую обработку информации, при условии осуществления контроля за состоянием защиты указанных средств не реже 1 раза в день.
- 11) Допускается доступ (в том числе, изготовление ключевой пары) Администратора защиты информации (Администратором безопасности) к ключевым носителям работников Субъекта Системы, при условии, что ключ генерируется в неизвлекаемом виде на аппаратном средстве криптозащиты (например, ruToken, eToken).
- 12) Допускается использование сетевых аппаратных модулей криптозащиты, предназначенных для работы с ключевой информацией, при условии нахождения как модуля, так и средств Системы в специальных помещениях, доступ в которые, в том числе по локальной сети Субъекта, ограничен Администраторами защиты информации (Администратором безопасности) и Владельцами ключей, и ведётся журнал такого доступа.
- 13) В иных случаях для хранения носителей ключевой информации должны использоваться надежные сейфы (металлические шкафы). В этом случае по окончании рабочего дня, а также вне времени сеансов связи с Системой, носители ключевой информации должны храниться в сейфе (металлическом шкафе). Допускается хранение носителей ключевой информации в одном сейфе с другими документами и ценностями, при этом отдельно от них и в упаковке, исключающей возможность негласного доступа к ним посторонних лиц.

Действия в случае компрометации ключей

- 1) Для подтверждения прав оповещения о компрометации ключей Операционным центром каждому Участнику выдается секретный код оповещения (если это предусмотрено правилами Удостоверяющего центра).
- 2) В случае компрометации криптографических ключей Владелец сертификата обязан незамедлительно уведомить Операционный центр о компрометации его ключа, указав скомпрометированный ключ и сообщив код оповещения (при его наличии в правилах Удостоверяющего центра). Датой и временем компрометации считаются дата и время получения Операционным центром уведомления о компрометации, сформированного в соответствии с требованиями правил Удостоверяющего центра по действиям с ключевой информацией, размещенных по адресу.
- 3) Все действия в Системе с использованием скомпрометированных ключей немедленно прекращаются.
- 4) Электронный документ, подписанный скомпрометированным криптографическим ключом электронной подписи, признается ненадлежащим.
- 5) Абонент после уведомления Операционного центра о компрометации ключа осуществляет процедуры в соответствии с правилами Удостоверяющего центра перехода на резервный ключ (при его наличии) или вырабатывает новый ключ и отправляет запрос на его сертификацию.
- 6) Операционный центр, получив уведомление с использованием кода оповещения, аннулирует действие данного кода, вырабатывает и высылает Участнику новый код оповещения.

Порядок разрешения конфликтных ситуаций, связанных с использованием ЭДО в Системе

- 1) Споры и разногласия, связанные с использованием ЭДО, расчетами в электронной форме и применением средств шифрования и электронной подписи, решаются путем переговоров.

- 2) В случае возникновения конфликтной ситуации по поводу авторства или подлинности текста Электронного документа, которую не удастся решить путем переговоров, Оператором Системы организуется проведение технической экспертизы спорного Электронного документа.
- 3) Разбор конфликтной ситуации выполняется по инициативе любого Абонента и включает:
 - предъявление претензии;
 - образование экспертной комиссии;
 - разбор конфликтной ситуации;
 - выработка заключения и решения по конфликтной ситуации.
- 4) Разбор конфликтной ситуации заключается в доказательстве принадлежности или не принадлежности ЭП конкретного Электронного документа со всеми его реквизитами конкретному Владельцу сертификата ключа проверки электронной подписи.
- 5) Проведение технической экспертизы организуется Оператором на основании письменного заявления заинтересованной стороны.
- 6) Заявление о споре подается Оператору в письменной форме с указанием наименования заявителя, наименования и реквизитов спорного Электронного документа, требований заявителя, обстоятельств, на которых заявитель основывает свои требования, перечня прилагаемых к заявлению документов. К заявлению также прилагается список должностных лиц заявителя, предлагаемых для включения в состав экспертной комиссии.
- 7) Для проведения технической экспертизы Оператор создает комиссию, включающую равное количество, но не менее двух, представителей от Оператора и от каждой из заинтересованных сторон, либо привлекает независимых экспертов, в том числе путем обращения в Удостоверяющий центр. В состав комиссии по соглашению сторон включаются представители служб безопасности заинтересованных сторон. В состав комиссии могут включаться независимые технические эксперты. В состав комиссии включается представитель Удостоверяющего центра.
- 8) В течение 3 (трех) рабочих дней Оператор обязан уведомить все имеющие отношение к рассматриваемому документу или вопросу стороны о месте и времени проведения экспертизы и составе экспертной комиссии.
- 9) Каждая из сторон вправе заявить об отводе эксперта из состава экспертной комиссии, если есть основания предполагать, что он прямо или косвенно заинтересован в исходе дела.
- 10) Оператор и экспертная комиссия принимают меры к тому, чтобы экспертиза была проведена в срок не более 7 (семи) рабочих дней со дня поступления заявления заинтересованной стороны. В исключительных случаях срок может быть продлен, но не более чем на 7 (семь) рабочих дней.
- 11) Неявка любой из спорящих сторон, надлежащим образом извещенных о месте и времени проведения экспертизы, не препятствует проведению экспертизы, если отсутствующая сторона не представила письменную просьбу отложить проведение экспертизы по уважительной причине, но на срок не более 2 (двух) рабочих дней.
- 12) Экспертная комиссия проводит экспертизу только после получения всех необходимых материалов, как правило, на территории и в помещении Оператора или Операционного центра.
- 13) При необходимости экспертная комиссия может провести у каждой из спорящих сторон осмотр помещений, где установлены СКЗИ, осуществить проверку программно-аппаратных средств, выполнить иные действия, которые, по мнению комиссии, являются необходимыми для проведения экспертизы и выработке решений комиссии.

- 14) Для проведения технической экспертизы в комиссию передаются:
- электронный документ, подписанный ЭП, подлинность которой оспаривается;
 - запрос на выведение из действия ключа, если таковой был;
 - Сертификаты ключей проверки электронной подписи Владельцев сертификатов, подписавших документ;
 - справочник сертификатов с сертификатом Владельца сертификата, подпись которого оспаривается;
 - съемные носители с файлами контрольных сумм исполняемых модулей СКЗИ сторон, участвующих в споре;
 - электронные журналы (архивы журналов).
- 15) Экспертная комиссия осуществляет корректные технологические процедуры, направленные на выявление истинности (например, устанавливает на персональный компьютер эталонную операционную систему и эталонное программное обеспечение, хранящееся у Операционного центра. Такой компьютер не должен иметь установленного на нем программного обеспечения. С этой целью его жесткий диск может форматироваться в присутствии всех членов экспертной комиссии).
- 16) Экспертная комиссия, если применимо, проверяет целостность программного обеспечения спорящих сторон путем сравнения с эталонным программным обеспечением, хранящимся у Операционного центра.
- 17) В случае выявления нарушения неизменности и целостности программного обеспечения СКЗИ в части неизменности и целостности программной реализации СКЗИ, виновной признается сторона, допустившая такие нарушения, в том числе при разборе любых конфликтных ситуаций.
- 18) Для разбора конфликта по поводу авторства или подлинности текста документа, подписанного ЭП, экспертная комиссия осуществляет следующие действия:
- проверяет актуальность сертификата ключа;
 - сравнивает содержание однотипных экземпляров сертификатов, представленных пользователем и Удостоверяющим центром.
 - проверяется подлинность ЭП спорного документа.

Авторство подписи под документом считается установленным, если в протоколе проверки подписи сформирована запись о положительном результате проверки подлинности ЭП.

- 19) Протокол проверки подписи является основным документом работы экспертной комиссии и должен быть подписан всеми ее членами.
- 20) При рассмотрении конфликтной ситуации по поводу актуальности сертификата ключа, когда одна сторона утверждает, что на момент времени T_0 сертификат другой стороны был зарегистрирован как действующий, а вторая сторона считает, что сертификат на этот же момент T_0 был в установленном порядке выведен из действия, вторая сторона должна представить экспертной комиссии уведомляющее сообщение о выведении из действия спорного ключа. При этом моменты наступления всех событий, имеющих отношение к возникшему по вопросу актуальности открытого ключа спору, указываются по времени Оператора Системы.

Заключение экспертной комиссии, в котором указано, что время T_0 более позднее, чем время, указанное в названном уведомляющем сообщении, является доказательством факта недействительности спорного ключа на момент времени T_0 .

В противном случае факт выведения спорного ключа из действия считается недоказанным.

- 21) По итогам проведения экспертизы составляется письменное заключение, содержащее:
- реквизиты Оператора Системы;

- дату, время и место ее проведения;
- фамилии, имена, отчества экспертов, с указанием реквизитов организаций, которые они представляют;
- требования стороны (сторон) и (или) вопросы, которые должны были быть разрешены при проведении экспертизы;
- описание выполненных в ходе экспертизы действий с указанием точных результатов, использованных аппаратных средств и программного обеспечения;
- выводы экспертной комиссии;
- подписи членов экспертной комиссии;
- оттиск печати Оператора Системы.

22) Экспертное заключение, составленное представителями независимой организации, может иметь иные реквизиты и содержать иной перечень информации, позволяющей однозначно определить и трактовать обстоятельства спорной ситуации.

23) При проведении экспертизы при необходимости по электронным документам в установленном порядке могут быть изготовлены их бумажные копии.

24) Экспертная комиссия не дает правовой оценки действиям сторон.

25) Решение экспертной комиссии может направляться в судебные инстанции в качестве приложения к исковому заявлению или рассматриваемому делу.

26) В случае согласия с выводами экспертной комиссии стороны, между которыми возник спор, заключают соглашение об урегулировании разногласий.