УТВЕРЖДЕНЫ
Единственным участником ООО «КП Ритейл»
(Решение № 3/2019 от 12 июля 2019 г.)
Вступают в силу с 12 августа 2019 г.

Правила платежной системы «КП Ритейл»

Оглавление

Протокол изменения документа

Дата	Номер версии документа	Описание
06.04.2015	1-я версия	Первоначальная версия
30.10.2018	2-я версия	Внесены изменения в части приведения Правил в соответствие требованиям Федерального закона от 27 июня 2011 г. N 161-ФЗ "О национальной платежной системе" и Положения Банка России от 3 октября 2017 г. № 607-П "О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков"
15.03.2019	3-я версия	Внесены изменения в части приведения Правил в соответствие требованиям Федерального закона от 27 июня 2011 г. N 161-ФЗ "О национальной платежной системе" и Указания Банка России от 11 июня 2014 г. № 3280-У "О порядке информирования оператором платежной системы Банка России, участников платежной системы о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры"
12.06.2019	4-я версия	Внесены изменения в части приведения Правил в соответствие требованиям Федерального закона от 27 июня 2011 г. N 161-ФЗ "О национальной платежной системе"

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.

Наименование на английском языке - Payment system CP Retail.

Настоящие Правила Платежной системы «КП Ритейл» (далее – Правила) определяют порядок и условия участия, взаимодействия в Системе, осуществления перевода денежных средств, в том числе трансграничного перевода денежных средств, оказания 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 в области защиты информации, управления рисками, обеспечения бесперебойного функционирования в рамках Системы.

Правила, а так же тарифы, являющиеся частью Правил (Приложение №1), публикуются в открытом доступе на официальном сайте Оператора в информационно-телекоммуникационной сети «Интернет» по адресу: www.cpretail.ru

2. Термины и определения.

Для целей настоящих Правил используются следующие термины и определения:

Адресный перевод — перевод, при отправлении которого указывается наименование Участника-исполнителя и пункт выдачи/зачисления Перевода и/или наименование Клиента Участника – юридического лица в пользу которого осуществляется перевод.

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

Банкомат – автоматическое (без участия уполномоченного лица Участника) устройство для осуществления расчетов, обеспечивающее возможность выдачи и (или) приема наличных денежных средств, в том числе с использованием электронных средств платежа, и по передаче распоряжений Участнику об осуществлении перевода денежных средств.

Безадресный перевод — перевод, при отправлении которого указывается только страна выдачи.

Бивалютный перевод – перевод с автоматической конвертацией по курсу Системы из одной валюты в другую.

Банковский платежный агент (БПА) - юридическое лицо или индивидуальный предприниматель, привлекаемый Участником на основании отдельного договора для осуществления деятельности, предусмотренной ст. 14 Закона о НПС.

Банковский платежный субагент (**БПС)** - юридическое лицо или индивидуальный предприниматель, который привлекается Банковским платежным агентом на договорной основе для осуществления деятельности, предусмотренной ст. 14 Закона о НПС.

БФПС – бесперебойность функционирования платежной системы.

Дистанционное банковское обслуживание (ДБО) – услуги, оказываемые через платежные терминалы самообслуживания, банкоматы, системы интернет-банкинга и т.п.

Инцидент – событие, которое привело к нарушению оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, в том числе вследствие нарушений 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.

Личный кабинет (ЛК) – согласованный канал связи - интерфейс для информационного обмена между Участниками Системы и Оператором. ЛК размещается на официальном сайте Системы www.cpretail.ru. Доступ к ЛК осуществляется с использованием индивидуального логина и пароля, которые предоставляются Участнику при подключении к Системе.

Оператор по переводу денежных средств - организация, которая в соответствии с законодательством РФ вправе осуществлять перевод денежных средств – кредитная организация.

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

Отчетный период - период времени, за который проводятся расчеты в рамках Системы.

Перевод денежных средств (Перевод) – действия оператора по переводу денежных средств в рамках применяемых форм безналичных расчетов по предоставлению получателю средств денежных средств плательщика.

Плательщик/Отправитель – физическое или юридическое лицо, дающее поручение Участнику на осуществление в рамках Системы операции по переводу денежных средств.

Платежный терминал – программно-технический комплекс, предназначенный для осуществления без участия уполномоченного работника Участника приема наличных денежных средств и/или банковских карт, а также для составления документов, подтверждающих соответствующие операции.

Получатель - физическое или юридическое лицо, в пользу которого совершен Перевод.

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. Списки Пунктов обслуживания доступны для ознакомления на сайте www.cpretail.ru.

Персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (Отправителю, Получателю), доступная Субъекту Системы, принявшему данную информацию в обработку в соответствии с Законодательством РФ.

Согласованный канал связи – средства и способы, определенные Оператором, Участником и ОУПИ для информационного обмена и расчетов.

Субъекты Системы – Оператор, операторы услуг платежной инфраструктуры и Участники;

Тарифы – документ, устанавливающий размер платы за услуги по переводу денежных средств и услуги платежной инфраструктуры в рамках Системы (Приложение 1 к настоящим Правилам). Тарифы размещены на сайте Оператора в сети Интернет по адресу: www.cpretail.ru

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 настоящих 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 настоящих Правилах.

Управление рисками в Системе - организация системы управления рисками в Системе, оценке и управлению рисками в Системе.

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

Участник-отправитель – Участник, принимающий от Отправителя поручение и денежные средства на осуществление Перевода.

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

Услуги Системы - осуществление перевода денежных средств, в том числе трансграничные переводы и переводы с использованием электронных средств платежа, от Отправителя:

- для выплаты наличными денежными средствами физическим лицам без открытия счета;

- для зачисления на счета Получателей в кредитных организациях, иностранных банках, в том числе в счет оплаты услуг, выполнения обязательств.

Электронное средство платежа - 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.

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.

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 (далее - операционные услуги).

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 (далее – услуги платежного клиринга).

Функции центрального платежного контрагента (ЦПКК): функции ПКЦ, выступающего в соответствии с Законом о НПС, плательщиком и получателем средств по переводам денежных средств Участников.

Функции Расчетного центра (РЦ): обеспечение в рамках Системы исполнения поступивших от ПКЦ распоряжений Участников посредством списания и зачисления денежных средств по банковским счетам Участников и (или) банковскому счету ЦПКК, направление подтверждений, касающихся исполнения распоряжений Участников (далее – расчетные услуги).

Расчетный центр также выполняет функции **Удостоверяющего центра**: в соответствии с федеральным законом 63-ФЗ «Об электронной подписи».

Функции Участников – предоставление Услуг Системы Клиентам.

Полный перечень ОУПИ доступен для ознакомления на сайте www.cpretail.ru.

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 их соблюдения 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. Выявлять организации, предоставляющие Участникам, их клиентам услуги платежной инфраструктуры, привлекать указанные организации в качестве операторов услуг платежной инфраструктуры.

4.1.6. При наличии в Системе двух и более расчетных, платежных клиринговых или операционных центров обеспечивать взаимозаменяемость операторов соответствующих услуг платежной инфраструктуры и (или) возможность для Участников Системы осуществить переход в течение не более 10 рабочих дней на обслуживание к другому (резервному) оператору услуг платежной инфраструктуры, в случае нарушения обслуживающим их оператором услуг платежной инфраструктуры требований к БФПС , в том числе приостановления (прекращения) оказания услуг платежной инфраструктуры. В случае такого перехода на обслуживание в резервный Расчетный центр используется технология расчетов, применяемая в данном Расчетном центре.

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

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

4.1.9. Обеспечить возможность досудебного и (или) судебного рассмотрения споров с Участниками платежной системы, Операторами услуг платежной инфраструктуры в соответствии с Правилами.

4.1.10. 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.

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

4.1.12. Организовывать взаимодействие Оператора, ОУПИ и Участников Системы по обеспечению БФПС и контроль за соблюдением ОУПИ и Участниками Системы порядка обеспечения БФПС.

4.1.13. Оператор информирует о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры:

- Участников в день такого приостановления (прекращения) любым из указанных ниже способов:
  - размещение информации на официальном сайте Системы www.cpretail.ru,
  - размещение информации в Личных кабинетах Участников,
  - направление уведомления по согласованным каналам связи.
- Банк России (Департамент национальной платежной системы) посредством направления сообщения на бумажном носителе или электронного сообщения, снабженного кодом аутентификации, в течение двух рабочих дней со дня приостановления (прекращения) оказания услуг платежной инфраструктуры. При этом Оператор в день приостановления (прекращения) оказания услуг платежной инфраструктуры незамедлительно направляет в Банк России (Департамент национальной платежной системы) уведомление о приостановлении (прекращении) оказания услуг платежной инфраструктуры с использованием способа связи, информация о котором доведена до него Банком России (Департаментом национальной платежной системы).

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 настоящих Правилах.

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

4.2.3. Размещать в публичном доступе перечень Участников Системы.

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

4.2.5. Уведомлять Участников платежной системы о необходимости смены Расчетного центра или иного ОУПИ в более сокращенные сроки, чем установлены в настоящих Правилах, в случае наличия объективной информации о наличии риска невыполнения Расчетным центром или иным ОУПИ своих обязательств по бесперебойности функционирования.

4.2.6. С согласия Клиента, передавать поручение на осуществление перевода Участнику, с которым заключено письменное соглашение об организации отправки/выдачи переводов через иные платежные системы и операторов по переводу денежных средств, с которыми у Участника заключен отдельный договор.

4.2.7. Устанавливать, изменять предельные размеры (лимиты) обязательств Участников Системы.

4.2.8. Организовывать продвижение услуг Системы.

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

4.2.10. Устанавливать обменный курс, применяемый в Системе при осуществлении расчетов с Участниками, а также при осуществлении Клиентами Бивалютных переводов. Курс фиксируется в ПК «КП Ритейл», доводится до сведения Клиентов в местах их обслуживания, в т.ч. в пунктах обслуживания, на дисплеях терминалов самообслуживания, с помощью систем ДБО.

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

4.3. Права Участников.

4.3.1. Участвовать в других платежных системах.

4.3.2. Определять количество, месторасположение, режим работы Пунктов обслуживания, а также порядок и способ предоставления денежных средств Отправителями.

4.3.3. Привлекать третьих лиц в целях предоставления Услуг Системы в соответствии с законодательством страны своего месторасположения, в т.ч. Банковских Платежных Агентов в соответствии с законодательством Российской Федерации. При этом Участник несет ответственность перед Субъектами Системы за действия указанных третьих лиц.

4.3.4. Полностью или частично приостановить оказание Услуг Системы.

4.3.5. Осуществлять клиринг и расчеты вне рамок Системы на основании договоров, заключаемых между Участниками Системы.

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

4.4. Обязанности Участников.

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

4.4.2. Оплачивать услуги, предоставляемые Операторами услуг платежной инфраструктуры в сроки и в порядке, определенном Правилами (Приложение № 1 к Правилам).

4.4.3. Открыть счет в Расчетном центре Системы. Контролировать достаточность денежных средств на счете в одном из них или нескольких одновременно Расчетных центрах для бесперебойности расчетов и выполнения своих обязательств.

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

4.4.5. Обеспечить получение согласия на обработку (включая автоматизированную обработку) данных физических лиц (отправителей и получателей денежных переводов) всеми Субъектами Системы, участвующими в обработке данных.

4.4.6. Выполнять требования по обеспечению безопасности в Платежной системе в соответствии с Правилами.

4.4.7. В случае внесения изменений в учредительные документы, а также при изменении других данных Участника, предоставить указанные изменения не позднее 5 (пяти) рабочих дней со дня их государственной регистрации.

4.4.8. 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.

4.4.9. Гарантировать соблюдение банковской тайны.

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

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

4.4.12. Направлять по запросу Оператора (поступившему в том числе с почтового ящика ответственного подразделения Оператора cpretail@cpretail.ru) 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.

4.4.13. Соблюдать Правила Системы.

4.4.14. Соблюдать порядок обеспечения БФПС в рамках выполняемого функционала.

4.4.15. Предоставлять внутренние документы по обеспечению БФПС на контроль Оператору Системы.

4.4.16. Выполнять другие обязательства в соответствии с настоящими Правилами.

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. 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.

4.5.5. Нести ответственность за реальный ущерб, причиненный Субъектам Системы вследствие неоказания (ненадлежащего оказания) операционных услуг в размере разовой неустойки, составляющей 0,03% от суммы неисполненных и/или исполненных с нарушением срока обязательств, за исключением случаев умышленного неоказания (ненадлежащего оказания) операционных услуг.

4.5.6. Изготавливать сертификаты ключей проверки электронных подписей.

4.5.7. Выдавать сертификаты ключей проверки электронных подписей в форме электронных документов с информацией об их действии.

4.5.8. Аннулировать выданные сертификаты ключей проверки электронной подписи.

4.5.9. Вести реестр сертификатов ключей проверки электронных подписей, обеспечивать его актуальность.

4.5.10. Обеспечивать уникальность ключей проверки электронных подписей в реестре сертификатов ключей проверки подписей и архиве Удостоверяющего центра.

4.5.11. Проводить по обращениям Участников проверку электронных подписей

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

4.5.13. Осуществлять оценку качества функционирования операционных и технологических средств и информационных систем путем привлечения независимой организации не реже 1 раза в два года. Предоставлять результаты проверки Оператору.

4.5.14. Соблюдать порядок обеспечения БФПС в рамках выполняемого функционала.

4.5.15. Предоставлять внутренние документы по обеспечению БФПС на контроль Оператору Системы.

4.5.16. 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.

4.6.2. Отказать Участнику в выдаче сертификата ключа проверки электронной подписи в случае нарушения им Правил Системы.

4.6.3. Самостоятельно разрабатывать внутренние документы по обеспечению БФПС в пределах выполняемого функционала в целях управления рисками и управления непрерывностью 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 платежные клиринговые позиции Участников.

4.7.3. Осуществляя функции ЦПКК:

- обладать денежными средствами, достаточными для исполнения своих обязательств, либо обеспечивать исполнение своих обязательств, в размере наибольшего обязательства, по которому ЦПКК становится плательщиком, за период, определяемый Правилами Системы: один Операционный день Оператора Системы;

- ежедневно осуществлять контроль рисков неисполнения (ненадлежащего исполнения) Участниками своих обязательств по переводу денежных средств, применять в отношении Участников, анализ финансового состояния которых свидетельствует о повышенном риске, ограничительные меры, в том числе установление максимального размера платежной клиринговой позиции, предъявление требования о повышенном размере обеспечения исполнения обязательств Участников по переводу денежных средств, а также ограничения по совершаемым операциям вплоть до их полного приостановления.

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

4.7.5. Нести ответственность за убытки, причиненные Участникам и Расчетному центру вследствие неоказания (ненадлежащего оказания) услуг платежного клиринга в размере разовой неустойки, составляющей 0,03% от суммы неисполненных и/или исполненных с нарушением срока обязательств, за исключением случаев умышленного неоказания (ненадлежащего оказания) услуг платежного клиринга.

4.7.6. Осуществлять оценку качества функционирования операционных и технологических средств и информационных систем путем привлечения независимой организации не реже 1 раза в два года. Предоставлять результаты проверки Оператору.

4.7.7. Соблюдать порядок обеспечения БФПС в рамках выполняемого функционала.

4.7.8. Предоставлять внутренние документы по обеспечению БФПС на контроль Оператору Системы.

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 требованиям.

4.8.2. Выступать, являясь кредитной организацией, в качестве Центрального платежного клирингового контрагента (ЦПКК).

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

4.9. Обязанности Расчетного центра.

4.9.1. Не изменять без согласования с Оператором положения, определяющие порядок, условия и сроки предоставления расчетных услуг.

4.9.2. Уведомлять Оператора, а также Участников о намерении изменения тарифов предоставления услуг по ведению банковского счета, не менее чем за 45 (Сорок пять) календарных дней до даты вступления в силу таких изменений.

4.9.3. Обеспечивать в рамках Системы исполнение распоряжений посредством списания и зачисления денежных средств по Счетам Участников.

4.9.4. Обеспечивать направление подтверждений исполнения распоряжений Участников.

4.9.5. В случае внесения изменений в учредительные документы, а также при изменении других данных, предоставить указанные изменения **не позднее 5 (пяти) рабочих дней с даты их государственной регистрации.**

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

4.9.7. 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.

4.9.8. Осуществлять оценку качества функционирования операционных и технологических средств и информационных систем путем привлечения независимой организации не реже 1 раза в два года. Предоставлять результаты проверки Оператору.

4.9.9. Соблюдать порядок обеспечения БФПС в рамках выполняемого функционала.

4.9.10. Предоставлять внутренние документы по обеспечению БФПС на контроль Оператору Системы.

4.9.11. Выполнять иные обязательства в соответствии с настоящими Правилами.

4.10. Права Расчетного центра.

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

4.10.2. Осуществлять кредитование Счетов Участников путем заключения соглашения между Расчетным центром и Участником.

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

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

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

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

5.1.5. Оператор поддерживает перечень ОУПИ в актуальном состоянии:

- перечень публикуется на сайте Системы www.cpretail.ru;
- Оператор в течение 5 (Пяти) рабочих дней с момента возникновения оснований для внесения изменений вносит изменения в перечень и уведомляет об этом Банк России.

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 РФ, 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 РФ.

5.2.2. Требования к Операционному центру.

- Операционным центром платежной системы может выступать юридическое лицо, созданное в соответствии с законодательством РФ, находящееся на территории РФ.
- Организация обладает программно-аппаратным комплексом, персоналом, имеющим соответствующую компетенцию, необходимыми для обеспечения технического функционирования Системы.
- Организация обеспечивает защиту информации в соответствии с требованиями действующего Законодательства.

5.2.3. Требования к Платежному клиринговому центру.

- Платежным клиринговым центром платежной системы может выступать юридическое лицо, созданное в соответствии с законодательством РФ, находящееся на территории РФ.
- При выполнении функций ЦПКК Платежным клиринговым центром может выступать только кредитная организация, созданная в соответствии с законодательством РФ, в том числе небанковская кредитная организация.
- Организация обладает программно-аппаратным комплексом, персоналом, имеющим соответствующую компетенцию, необходимыми для обеспечения технического функционирования Системы, а также для возможности обработки сообщений Участников, иных Субъектов Системы, проведения расследований по операциям, осуществленным в рамках Системы.

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 существующих ОУПИ самостоятельно, в том числе используя общедоступную информацию, а также при необходимости запрашивая от ОУПИ дополнительную информацию о текущей деятельности, осуществляет мониторинг деятельности ОУПИ на момент соответствия требованиям, описанным в п.5.2.1.-5.2.3.

6. Порядок взаимодействия между Субъектами Системы.

6.1. Взаимодействие Оператора с Участниками.

6.1.1. Взаимодействие Оператора с Участниками осуществляется на основании настоящих 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.

6.1.2. Оператор:

- инициирует предложение об участии в Системе либо принимает обращения с намерением юридического лица присоединиться к Правилам Платежной системы;
- 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.

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

- Личный кабинет Участника.
- Электронные адреса Оператора. Информационные рассылки, осуществляемые с адресов, являются официальными сообщениями Оператора Системы.
- Электронный адрес Участника:
  - указанный в договоре участия.
  - указанный при регистрации в Личном кабинете.
  - указанный в официальном письме Оператору или в сообщении на электронный адрес Оператора.

6.2. Критерии участия в Системе.

6.2.1. 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;
- соблюдение требований законодательства Российской Федерации, страны своей юрисдикции по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, а также иного применимого к деятельности организации законодательства;

- обеспечение защиты информации в соответствии с требованиями законодательства Российской Федерации, страны своей юрисдикции, нормативных актов Правительства Российской Федерации и Банка России, Правил.

6.2.2. Участник считается присоединившимся к Системе после открытия счета в Расчетном центре и подписания договора участия в платежной системе с Оператором. Присоединение к Системе является бесплатным для Участника.

6.2.3. Соответствие критериям проверяется в процессе открытия счетов в Расчетном центре. Подписывая договор участия, Участник гарантирует выполнением им мер по защите информации, соблюдение требований применимого законодательства.

6.2.4. Датой начала участия в Системе в целях уведомления об этом уполномоченного органа является одна из следующих дат, более поздняя из них:

- дата заключения договора участия в Платежной системе «КП Ритейл»;
- дата открытия счета в Расчетном центре Системы.

6.2.5. Оператор устанавливает виды участия в Системе:

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

6.2.6. Присоединяясь к Правилам Участник принимает их в целом без каких-либо изъянов и исключений.

6.3. Порядок присвоения идентификационного номера.

6.3.1. Участнику присваивается идентификационный цифровой или буквенный номер, позволяющий однозначно установить Участника.

6.3.2. Идентификационный код присваивается Операционным центром автоматически при регистрации Участника в Системе в момент создания Личного кабинета Участника.

6.4. Критерии приостановления и прекращения участия в Системе.

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

- случаи несоблюдение Участником своих обязательств, установленных Правилами;
- зафиксированные случаи утраты соответствия критериям участия;
- имеющиеся в распоряжении Оператора, Расчетного центра, ЦПКК сведения, позволяющие сделать вывод о высокой вероятности возникновения рисков, ведущих к невозможности осуществления расчетов, в том числе неисполнения обязанности по обеспечению достаточности денежных средств на Счете Участника в сроки и порядке, установленные Правилами;
- 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.

6.4.2. В случае наличия критериев 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 платежной системы, а также ограничить в иных правах и не оказывать иные услуги, предусмотренные Правилами и договором участия. Мониторинг соответствия Участников критериям, указанным в п. 6.4.1 производится на регулярной основе. Документальное оформление мониторинга соответствия Участникам критериям, указанным в п. 6.4.1 производится в случае, если установлен факт невыполнения одного или нескольких критериев соответствия. Ответственное подразделение Оператора доводит соответствующую информацию до органов управления Оператора для принятия решения о приостановлении/прекращении участия.

6.4.3. 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. Взаимодействие между Оператором и ОУПИ.

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

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

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

- Личный кабинет (при наличии).
- Адреса электронной почты Оператора. Информационные рассылки, осуществляемые с адресов Оператора (с доменного имени @cpretail.ru), указанных в заключенных договорах или иным образом официально доведенных до ОУПИ, являются официальными сообщениями Оператора Системы.
- Адреса электронной почты ОУПИ:
  - указанный в договоре с Оператором.
  - указанный при регистрации в Личном кабинете.
  - указанный в официальном письме Оператору или в сообщении на электронный адрес Оператора.

6.6. Взаимодействие между ОУПИ и Участниками.

6.6.1. Взаимодействие ОУПИ с Участниками осуществляется в соответствии с Правилами. Дополнительно Участниками заключается договор с Расчетным центром на открытие и ведение счетов Участника для осуществления расчетов в рамках Системы.

6.6.2. Взаимодействие Участников с ОУПИ осуществляется автоматизированным технологическим взаимодействием с ОЦ. ОЦ самостоятельно осуществляет маршрутизацию сообщений между Субъектами Системы, участвующими в обработке и исполнении распоряжений.

6.6.3. Списание и зачисление денежных средств по счетам Участников и ЦПКК осуществляется Расчетным центром на основании полученного от ПКЦ распоряжения. При этом получение дополнительного распоряжения Участников на списание денежных средств не требуется. Расчетный центр не несет ответственности за правомерность и содержание включенных в состав реестра распоряжений о переводе денежных средств и, указанных реквизитов.

6.6.4. Исполнение распоряжений по списанию денежных средств со счетов, 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 реестра ПКЦ.

6.7. Контроль соблюдения Правил, ответственность за их несоблюдение.

6.7.1. Контроль соблюдения настоящих Правил Участниками и 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 ОУПИ, анализа жалоб и обращений Участников в отношении деятельности ОУПИ.

6.7.2. В рамках указанного мониторинга Оператор обязывает ОУПИ вести автоматизированный контроль выполнения Участниками обязательств по осуществлению расчетов, выполнения ПКЦ технологических процедур, предусмотренных процессами взаимодействия, в т.ч. поддержания бесперебойности функционирования в рамках Системы.

6.7.3. Оператор анализирует поступающие жалобы, обращения, результаты автоматизированного контроля, на ежеквартальной основе. По результатам анализа могут осуществляться мероприятия для устранения имеющихся некорректных действий: обращение к Участнику, ОУПИ в рабочем режиме (в т.ч. по согласованным каналам связи), организация встреч с Участником, ОУПИ, направление им официальных писем, в т.ч. содержащих требования об уплате неустойки в соответствии с условиями заключенных договоров.

6.7.4. Участники, ОУПИ несут ответственность за несоблюдение Правил. Несоблюдение Правил является одним из критериев прекращения участия в Системе, а также критерием прекращения выполнения функций оператора услуг платежной инфраструктуры.

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

6.7.6. Контроль соблюдения Участниками, 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 РФ или страны нахождения Участника.

6.8. Порядок изменения Правил платежной системы.

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

6.8.2. Для внесения изменений и/или дополнений в Правила Оператор обязан обеспечить Участникам возможность предварительного ознакомления с предлагаемыми изменениями и/или дополнениями и направления своего мнения Оператору в установленный им срок, который не может быть менее одного месяца. Возможность предварительного ознакомления с предлагаемыми изменениями и/или дополнениями обеспечивается путем размещения предлагаемых изменений и/или дополнений на официальном сайте Оператора в информационно - телекоммуникационной сети «Интернет»: www.cpretail.ru.

6.8.3. Изменения и/или дополнения в Правила вносятся в срок не менее одного месяца со дня окончания срока, указанного в п.6.8.2 Правил.

6.8.4. Изменения в Правила могут быть внесены по соглашению всех сторон – Субъектов Системы.

6.8.5. В случае изменения Правил по соглашению всех сторон Оператор размещает на официальном сайте Системы:

- проект Правил или предлагаемых изменений с указанием срока вступления изменений в силу;
- информацию о сроке, в течение которого Субъекты могут направить Оператору уведомления о согласии или несогласии с вносимыми изменениями, и адрес для сбора уведомлений.

6.8.6. Субъекты обязаны ознакомиться с вносимыми изменениями и направить в адрес Оператора уведомление о согласии или несогласии с ними по указанному Оператором адресу и в срок, указанный Оператором.

6.8.7. Субъект, направивший уведомление, содержащее несогласие с вносимыми изменениями, обязан привести аргументы своего несогласия. Неаргументированный отказ от принятия изменений не признается таковым. Считается, что Субъект не направил уведомление о согласии или несогласии с вносимыми изменениями.

6.8.8. Субъекты, не направившие уведомления о согласии или несогласии с вносимыми изменениями по указанному Оператором адресу и в срок, указанный Оператором, а также направившие несогласие и совершившие любую операцию в рамках Системы после срока, указанного Оператором, признаются принявшими предлагаемые изменения Правил.

6.8.9. Правила считаются согласованными всеми Субъектами Системы в случае, если в срок, указанный Оператором, не поступило ни одного уведомления о несогласии с вносимыми изменениями либо ни одним Субъектом не прекращены операции в рамках Системы.

6.8.10. В случае если Правила не согласованы всеми сторонами, Оператор имеет право инициировать повторную процедуру внесения изменений в Правила по соглашению всех сторон либо инициировать внесение изменений в одностороннем порядке в соответствии с пп.6.8.1 – 6.8.3 Правил.

6.8.11. Оператор обязан представлять в Банк России изменения и/или дополнения в Правила, изменения перечня Операторов услуг платежной инфраструктуры не позднее 10 (десяти) дней со дня внесения соответствующих изменений.

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

6.9.1. 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.

6.9.2. Каналы связи:

- По вопросам, связанным с ключами защиты информации skzi@cpretail.ru;
- адрес электронной почты cpretail@cpretail.ru.

6.9.3. 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.

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

6.9.5. Оператор разрабатывает, тестирует и пересматривает план действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности (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:

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

- при наличии в Системе одного Операционного, и (или) Платежного клирингового центра - мероприятия по привлечению другого ОУПИ и по переходу Участников Платежной системы на обслуживание к вновь привлеченному ОУПИ в течение 10 рабочих дней в случаях:

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

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

Оператор обеспечивает реализацию указанных выше мероприятий.

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

В случае, если ОУПИ является кредитной организацией, разработка, тестирование и пересмотр плана ОНиВД осуществляется в порядке, предусмотренном Положением Банка России от 16.12.2003 года № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»,

Оператор анализирует эффективность мероприятий по восстановлению оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, и использует полученные результаты при управлении рисками в Системе.

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

6.10. Порядок изменения операционных и технологических средств и процедур.

6.10.1. 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.

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

6.10.2. 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 РФ, настоящих 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.

6.10.3. 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 ОУПИ направляет Участникам уведомление об изменении операционных и технологических средств и процедур с описанием таких изменений не позднее, чем за 30 (тридцать) календарных дней до даты вступления в силу соответствующих изменений.

6.10.4. Участник, ОУПИ вправе самостоятельно вносить изменения в операционные и технологические средства и процедуры по взаимодействию с Системой на стороне Участника, ОУПИ, если внесение таких изменений не противоречит законодательным, нормативным документам соответствующих регуляторов и настоящим Правилам и не приводит к изменению порядка оказания услуг по переводам денежных средств, предусмотренного настоящими Правилами, а также к объему и характеру их оказания Участником, ОУПИ.

6.11. Порядок взаимодействия с платежными системами.

6.11.1. В настоящее время Система не взаимодействует с другими платежными системами.

6.11.2. Оператор при заключении договора о взаимодействии Системы с иными платежными системами отражает порядок взаимодействия в Правилах.

6.11.3. В случае начала взаимодействия с другими платежными системами Оператор начнет вести перечень платежных систем, с которыми осуществляется взаимодействие,

разместит указанный перечень на официальном сайте Оператора в информационно-телекоммуникационной сети «Интернет».

6.12. Порядок досудебного разрешения споров между Субъектами Системы.

6.12.1. Спорные ситуации, включая системные сбои, между Оператором и Участниками, между Оператором и ОУПИ, между Участниками и 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).

6.12.2. 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.

6.12.3. При возникновении спорной ситуации, связанной с применением электронного документооборота, Субъекты Системы действуют в соответствии с Инструкцией по работе с ключевой информации.

6.12.4. Участники в случае возникновения обстоятельств, свидетельствующих о возникновении и/или наличии спорной ситуации, в т.ч. при взаимодействии с ОУПИ, направляют сообщения Оператору по согласованным каналам связи, в т.ч. в порядке, описанном в п.6.9 Правил. Оператор осуществляет дальнейшее взаимодействие с ОУПИ.

6.12.5. Оператор организует рассмотрение обращения в оперативном режиме, претензии в течение 30 календарных дней.

6.12.6. 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.

7. Порядок осуществления платежного клиринга и расчетов.

7.1. Применяемые формы безналичных расчетов.

7.1.1. Переводы денежных средств в Системе осуществляются в рамках следующей формы безналичных расчетов - расчеты платежными поручениями.

7.2. Платежный клиринг.

7.2.1. В целях обеспечения исполнения обязательств Участников операции в рамках Системы осуществляются исходя из доступного остатка каждого Участника, размер которого контролируется и изменяется Платежным клиринговым центром при приеме распоряжений Участников.

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 выданных/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 Платежным клиринговым центром, 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;

- передачи Расчетному центру для исполнения принятых распоряжений Участников.

7.2.4. Определение платежной клиринговой позиции Участника осуществляется на нетто-основе по каждой из валют расчета. Платежная клиринговая позиция на нетто-основе определяется в течение операционного дня в размере разницы между общей суммой подлежащих исполнению распоряжений, по которым Участник является плательщиком, включая комиссии, и общей суммой распоряжений, по которым Участник является получателем средств, включая комиссии.

7.2.5. После определения платежной клиринговой позиции Платежный клиринговый центр формирует и направляет в Расчетный центр реестр, содержащий распоряжения на списание или зачисление денежных средств по счету Участника.

7.2.6. Реестр может быть сформирован и направлен в Расчетный центр до окончания операционного дня в рамках процедур управления рисками в Системе, в т.ч. в случае приостановления участия в Системе Участником, либо в рамках схемы с промежуточными расчетами.

7.2.7. Платежный клиринговый центр направляет Участникам Системы извещения (подтверждения), касающиеся приема к исполнению распоряжений Участников Системы, а также передачи извещений (подтверждений), касающихся исполнения распоряжений Участников Системы.

7.3. Расчеты.

7.3.1. Расчеты в рамках Системы осуществляются по счетам Участников, открытым в Расчетном центре.

7.3.2. Расчеты осуществляются Расчетным центром посредством списания и зачисления (без дополнительного распоряжения Участника) денежных средств со/на Счета на основании поступившего от Платежного клирингового центра реестра в размере сумм платежных клиринговых позиций.

7.3.3. При расчетах по Адресным переводам списание/зачисление денежных средств осуществляется по счетам Участников-отправителей и Участников-исполнителей.

7.3.4. При расчетах по Безадресным переводам списание/зачисление денежных средств осуществляется по счетам Участников и ЦПКК.

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

7.3.6. Для подтверждения правильности определения платежной клиринговой позиции и расчетов ПКЦ высылает Участникам реестр/справку, содержащие расшифровку каждой из вошедших в клиринговую позицию соответствующего Участника операции по согласованным каналам связи по итогам каждого операционного дня, соответствующего рабочему дню, установленному законами РФ и Постановлениями Правительства РФ. Операции Участников за операционные дни, соответствующие выходным и праздничным дням, включаются в реестры/справки следующего рабочего дня и направляются Участникам по окончании операционного дня, соответствующего рабочего дня.

7.3.7. Реестр/справка, содержащие расшифровку каждой из вошедших в клиринговую позицию соответствующего Участника, также являются подтверждением исполнения распоряжений 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 ОЦ Системы. Время приема

распоряжений представлено в Таблице №1, регламенты обработки распоряжений и проведения расчетов представлены в Таблице №2.

7.4.2. Операционный день в Системе – календарный день.

7.4.3. Время приёма к исполнению распоряжений Участников.

Таблица №1

Событие	**Время по Московскому времени**
Прием к исполнению распоряжений Участников	Круглосуточно

7.4.4. Регламент обработки распоряжений и осуществления расчетов.

Таблица №2

Событие	**Время по Московскому времени**
Начало (открытие) операционного дня – приёма распоряжений Участников (операционные услуги, услуги платежного клиринга).	00:00:00 ежедневно.
Завершение (закрытие) операционного дня - приёма распоряжений Участников (операционные услуги, услуги платежного клиринга).	23:59:59 ежедневно.
Обмен электронными сообщениями, расчёт платежных клиринговых позиций и направление подтверждений Участникам (операционные услуги, услуги платежного клиринга).	С 00:00:00 до 23:59:59.
Составление реестров, передача в Расчетный центр (операционные услуги, услуги платежного клиринга).	С 00:00 до 06:00 следующего за операционным днем рабочего дня.
Осуществление расчётов по счетам Участников Расчетным центром.	С момента получения реестра до 23:59:29 дня получения реестра.

7.4.5. В случае разового изменения времени операционного дня Оператор либо ОЦ/ПКЦ доводит данную информацию до Участников по согласованным каналам связи.

7.4.6. О проведении плановых технических, профилактических и ремонтных работ, проводимых не чаще, чем ежемесячно, Оператор либо ОЦ/ПКЦ заранее, не позднее, чем за один рабочий день до даты начала проведения работ, уведомляет Участников по согласованным каналам связи или путем опубликования на сайте Системы. В уведомлении указываются дата и время начала проведения работ, предполагаемые дата и время окончания проведения работ.

Допускаются технологические перерывы в оказании операционных и клиринговых услуг, которые устанавливаются на основании оценки допустимого уровня рисков, общая продолжительность технологических перерывов 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 с использованием ДБО.

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 (контрольный номер перевода).

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) производятся 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.

8.2. Моменты наступления безотзывности, безусловности и окончательности Перевода.

8.2.1. По переводам в пользу физических лиц для выплаты наличными денежными средствами:

- Безусловность наступает в момент обращения Получателя в Пункт обслуживания Участника-исполнителя и указания им контрольного номера перевода с одновременным совпадением данных Получателя в Переводе и данных, полученных в ходе идентификации Получателя,
- Окончательность наступает в момент выплаты наличных денежных средств Получателю.

8.2.2. По Переводам 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:

- при использовании технологии проверки выполнения условий осуществления операции в режиме он-лайн на этапе введения данных операции в программное обеспечение Участника-отправителя (при не прохождении проверки перевод не принимается в обработку);
- при использовании технологии проверки выполнения условий осуществления операции в режиме оф-лайн на этапе обработки перевода ПКЦ (в этом случае при не прохождении проверки Перевод возвращается Участнику - отправителю ПКЦ).

8.2.3. По Переводам, указанным в п.8.2.2, окончательность наступает в момент зачисления перевода на счет Участника-исполнителя.

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

8.3. Порядок сопровождения перевода денежных средств сведениями о Плательщике.

8.3.1. Система предоставляет техническую возможность сопровождения Перевода сведениями о Плательщике в соответствии с требованиями Федерального закона от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон №115-ФЗ).

8.3.2. Участники самостоятельно несут ответственность за реализацию комплекса мер, направленных на предотвращение легализации (отмывания) доходов, полученных преступным путем, и финансированию терроризма, в т.ч. при сопровождении перевода денежных средств

сведениями о Плательщике, а также ответственность за достоверность и полноту передаваемых сведений.

8.3.3. В случае, если в распоряжении Участника не содержатся сведения о Плательщике в соответствии с требованиями Федерального закона № 115-ФЗ, ПКЦ имеет право отказать в приеме в обработку распоряжения Участника.

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

8.4.1. Порядок внесения изменений при совершении Операции Участником - Отправителем с использованием средств ДБО, со счетов Отправителя определяется и доводится до сведения Отправителя Участником - Отправителем самостоятельно.

8.4.2. Внесение изменений в Перевод, направленный в пользу физического лица для выплаты наличными денежными средствами, возможно осуществить по требованию Отправителя при условии, что на момент внесения изменений или передачи их в Операционный центр денежные средства не были выплачены Получателю. Внесение изменений возможно только в реквизиты Получателя – физического лица или дополнительную информацию.

8.4.3. Для внесения изменений в Перевод, направленный для зачисления на счет физического лица или для выплаты чеком или в пользу юридического лица - Клиента Оператора Системы, Отправитель обращается к соответствующему юридическому лицу – Получателю или к кредитной организации/иностранному банку, в котором открыт счет Получателя, или к организации, обеспечивающей выплату чеком, напрямую. В случае невозможности такого обращения Отправитель может подать в офис Участника-Отправителя 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 данным юридическим лицом/организацией, обеспечивающей выплату по чеку, или кредитной организацией/иностранным банком, в которых открыт счет Получателя.

8.4.4. Условием осуществления Операции является предъявление Отправителем документа, подтверждающего факт совершения отправки, и, при необходимости, документов, подтверждающих его личность, что он является Отправителем.

8.4.5. Порядок взаимодействия Участника – Отправителя с Отправителями, утерявшими документы, являющиеся подтверждением совершения Операции, определяется и доводится до сведения Отправителей Участником – Отправителем самостоятельно.

8.4.6. Участник - Отправитель, принявший заявление Отправителя на внесение изменений, обязан незамедлительно с момента его принятия направить запрос на изменение Оператору Системы. В случае невозможности внесения изменений в Перевод по причине его выдачи или в соответствии с условиями осуществления Перевода, установленными Участником-Получателем, Оператор обеспечивает невозможность передачи такого запроса программным способом.

8.4.7. Участник - Отправитель уведомляет Отправителя о результатах обработки запроса.

8.4.8. 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.

8.5. Отзыв, возврат (аннулирование) Переводов.

8.5.1. 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.

8.5.2. Аннулирование Переводов возможно до наступления их окончательности.

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

8.5.4. Заявление об отзыве адресного перевода подается через тот же пункт Участника-отправителя, что и заявление на осуществление перевода.

8.5.5. При возврате Бивалютного перевода сумма Перевода пересчитывается по курсу, установленному на день отправки Бивалютного перевода.

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

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

9.1. Порядок оплаты услуг.

9.1.1. Порядок оплаты услуг по переводу денежных средств, услуг платежной инфраструктуры в рамках Системы является единообразным.

9.1.2. Комиссионное вознаграждение в Системе уплачивает Клиент, получающий Услуги Системы.

9.1.3. Уплачиваемое Клиентом вознаграждение за услуги по переводу денежных средств включает в себя комиссионное вознаграждение всех Субъектов Системы: Участника – отправителя, Оператора, ОУПИ, Участника – исполнителя, а также посредников в переводе (при их наличии).

9.1.4. Комиссия взимается сверх суммы Перевода.

9.1.5. Комиссия может быть выражена:

- в процентном отношении к сумме перевода;
- в процентном отношении к сумме перевода плюс фиксированная сумма;
- в фиксированной сумме.

9.1.6. Размер комиссии может варьироваться, в том числе в зависимости:

- от суммы перевода;
- от валюты перевода, валюты выдачи/зачисления;
- от используемых средств осуществления перевода и форм безналичных расчетов;
- от выбранного Отправителем места осуществления/получения перевода;
- наличия/отсутствия дополнительных сопутствующих переводу услуг;
- наличия/отсутствия посредников в осуществлении перевода;
- способа доставки денежных средств Получателю.

9.1.7. Сумма комиссии округляется по правилам, установленным Оператором.

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

9.1.9. Тарифы Системы (Приложение 1 к Правилам) признаются Тарифами для обслуживания физических лиц каждого Участника, оказывающего Услуги Системы Клиентам.

9.1.10. Тарифы Расчетного центра за ведение банковских счетов не являются Тарифами Системы.

9.1.11. Если действующее законодательство иностранного государства или его местных органов, резидентом которого является Участник, предусматривает какие бы то ни было удержания с вознаграждений, подлежащих перечислению Субъектам Системы, то такое вознаграждение подлежит увеличению таким образом, чтобы сумма, подлежащая перечислению Субъектам Системы, соответствовала вознаграждению, предусмотренному Тарифами, которое получили бы Субъекты Системы в случае отсутствия таких вычетов и удержаний.

9.1.12. При обслуживании Клиента вознаграждение 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.

9.1.13. Оператор осуществляет дальнейшее распределение комиссионного вознаграждения:

- ОУПИ за услуги платежной инфраструктуры;
- Участнику-исполнителю вознаграждение за осуществление перевода денежных средств.

9.1.14. Оператор вправе проводить маркетинговые акции путем установления комиссионного вознаграждения 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.

9.1.15. Оператор имеет право вносить изменения в Тарифы Системы. При внесении изменений, предусматривающих введение новых Тарифов или увеличение размера Тарифов, Оператор обязан уведомить об этом Банк России в срок не менее чем за 30 календарных дней до дня введения в действие изменений с предоставлением обоснования указанных изменений.

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

9.1.17. При использовании Участником при обслуживании Клиентов различных средств ДБО, банковских счетов, 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 согласования с Оператором.

9.1.18. Индивидуальные комиссии, устанавливаемые Участником сверх Тарифов, не являются Тарифами Системы.

9.1.19. Установление индивидуальных комиссий сверх Тарифов Системы без согласования с Оператором признается нарушением Правил Системы.

9.1.20. При установлении индивидуальных комиссий ниже Тарифов Системы без внесения изменений в Тарифы Системы Участник обязан уплачивать услуги платежной инфраструктуры и перечислять часть комиссионного вознаграждения Участника-исполнителя в полном объеме, предусмотренном Тарифами Системы.

9.1.21. Участник имеет право направить Оператору предложения с обоснованием внесения изменений в Тарифы Системы с уменьшением ставок комиссионного вознаграждения.

9.1.22. Тарифы Системы, а также самостоятельно установленное Участником в соответствии с п.**9.1.17** Правил комиссионное вознаграждение доводятся до сведения Клиентов, обслуживаемых Участником в порядке, устанавливаемом Участником самостоятельно, но обязательно до момента совершения операции.

9.1.23. Процедуры расчета и уплаты комиссии осуществляются ОУПИ в рамках общих процедур клиринга и расчетов, в частности, комиссии включаются в платежную клиринговую позицию по каждому Участнику.

10. Управления рисками в Системе.

10.1. Система управления рисками.

10.1.1. При обеспечении БФПС, которая достигается при условии оказания Участникам услуг платежной инфраструктуры соответствующих требованиям к оказанию услуг и (или) восстановления оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, в течение 6 часов и восстановления оказания услуг платежной инфраструктуры в случае приостановления их оказания в течение 6 часов, к Оператору применяются следующие требования.

Оператор обеспечивает БФПС путем осуществления скоординированной с ОУПИ и Участниками Системы деятельности:

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

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 за соблюдением ОУПИ и Участниками Системы порядка обеспечения БФПС.

10.1.2. 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, перечень мероприятий, проводимых в рамках Системы, и способов управления рисками.

10.2. Модель управления рисками.

10.2.1. Оператор организует систему управления рисками в Системе с учетом организационной модели управления рисками в Системе, определенной в соответствии с требованиями части 2 статьи 28 Закона о НПС: функции по оценке и управлению рисками в Системе распределяются между Участниками, Оператором, ОУПИ.

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

10.2.3. Участники, ОУПИ самостоятельно осуществляют деятельность:

- по управлению рисками, присущими их виду деятельности, и несут ответственность за последствия реализации указанных рисков;
- 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), законодательных требований;
- по контролю соблюдения привлеченными БПА, БПС условий их привлечения, а также законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- по разработке необходимых внутренних документов по управлению рисками и обеспечению непрерывности функционирования Системы в соответствии с требованиями законодательных, нормативных документов, настоящих Правил и рекомендаций Оператора.

10.2.4. Оператор предъявляет следующие требования к управлению рисками Участниками, 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, ОУПИ соблюдают требования к защите информации, указанные в п.13 настоящих Правил.
- Участники, ОУПИ обеспечивают надлежащее функционирование операционных и технологических средств, устройств, информационных систем, используемых ими при работе с Системой.
- Участники, ОУПИ самостоятельно обеспечивают управление рисками в собственной деятельности, в том числе разрабатывают необходимые методики в соответствии с требованиями Законодательства.
- Участники, ОУПИ разрабатывают и соблюдают планы по обеспечению непрерывности и восстановлению непрерывности своей деятельности.
- Участники, ОУПИ соблюдают порядок информационного взаимодействия в соответствии с Правилами.
- Участники, 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 настоящих 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 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 платежной системы о нарушении оказания 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 РФ 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 КО);
- выполнения Правил;
- выполнения требований законодательства, в т.ч. в сфере противодействия легализации преступных доходов и финансированию терроризма.

10.3.5. Участники, ОУПИ при возникновении событий, не связанных с БФСП, но способных повлиять на уровень рисков Системы, предоставляют информацию Оператору по каждому инциденту в соответствии с п.11.2.2. настоящих Правил.

10.3.6. Участники, 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. Информация предоставляется по согласованным каналам связи незамедлительно при возникновении угрозы нарушения бесперебойности функционирования в рамках Системы, при отсутствии указанной угрозы не позднее 3 (трех) рабочих дней после наступления события. При этом дополнительно возможно руководствоваться порядком информирования и взаимодействия, описанным в п.6.9 Правил.

10.3.8. Участники, 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).

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

10.3.10. Оператор вправе использовать информацию:

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

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

10.3.12. Информация предоставляется по запросу Оператора, но не реже 1 раза в два года.

10.3.13. Форма предоставления информации определяется Оператором самостоятельно.

10.4. Мероприятия по управлению рисками.

10.4.1. Система управления рисками включает следующие мероприятия 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;
- доведение до органов управления Оператора соответствующей информации о рисках;
- показателей бесперебойности функционирования Системы (показатели БФПС);
- управление непрерывностью и порядок обеспечения бесперебойности функционирования Системы, отраженных в п. 11 настоящих Правил;
- методики анализа рисков в Системе, включая определение профиля рисков;
- порядка обмена информацией, необходимой для управления рисками;
- порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев;
- 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.

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. Система управления рисками предусматривает следующие способы управления рисками:

- осуществление расчета в пределах, предоставленных Участником денежных средств (в пределах доступного остатка);
- страхование рисков (при необходимости);
- ограничение объемов операций вне зависимости от остатка денежных средств Участника исходя из позиции уровня рисков по конкретным операциям;
- автоматизированное управление очередностью исполнения распоряжений Участников - по времени поступления распоряжений (распоряжения исполняются в момент поступления при достаточности предоставленных денежных средств);
- осуществление расчета между Субъектами системы в Системе до конца рабочего дня.

10.6. Ограничение объемов операций вне зависимости от остатка денежных средств Участника исходя из уровня риска работы с конкретным Участником Системы. Организационная структура системы управления рисками.

10.6.1. Оператор определяет собственную структуру управления рисками и функциональные обязанности лиц в соответствующих структурных подразделениях, ответственных за управление рисками. По осуществлению управления рисками

устанавливается разграничение ответственности и полномочий между Субъектами Платежной системы.

10.6.2. Организационная структура органов управления рисками Оператора включает:

- Генеральный директор;
- Структурное подразделение (работник) Оператора, ответственное за управление рисками;
- Структурное подразделение (работник) Оператора, ответственное за информационную безопасность;
- Другие структурные подразделения (работники) Оператора в рамках выполняемого функционала.

10.6.3. Функциональные обязанности и компетенция органов управления рисками Оператора включает, в том числе, следующее:

- разработка и утверждение внутренних документов, регулирующих систему управления рисками, в том числе «Порядка бесперебойности функционирования и анализа рисков платежной системы «КП Ритейл», в которых, в том числе, рассматривается методика анализа рисков в платежной системе;
- установление предельных размеров (лимитов) обязательств Участников с учетом уровня рисков;
- установление допустимого уровня рисков нарушения бесперебойности функционирования Системы;
- принятие мер по обеспечению бесперебойности функционирования Системы и минимизации уровня рисков;
- осуществление контроля уровня рисков;
- оценка 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 настоящих Правилах; проведение оценки эффективности системы управления рисками Системы и ее совершенствование.

10.6.4. Участники и ОУПИ определяют должностных лиц и/или структурные подразделения, к обязанностям которых относится обеспечение мониторинга и проведение мероприятий, связанных с управлением рисками. Информация о вышеуказанных лицах (фамилия, имя, отчество, должность, контактные данные) предоставляется ОУПИ и Участниками в письменном (на бумажном/электронном носителе информации) или устном виде Оператору.

10.7. Доведение до органов управления Оператора информации о рисках.

10.7.1. В целях доведения до органов управления Оператора сведений о рисках информация о выявленных рисках незамедлительно предоставляется должностным лицом, ответственным за управление рисками, Генеральному директору Оператора.

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

10.7.3. Участники, ОУПИ самостоятельно разрабатывают процедуры доведения информации, необходимой для управления рисками до своих органов управления и Оператора.

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

11. Управление непрерывностью и порядок обеспечения бесперебойности функционирования Системы.

11.1. Показатели бесперебойности функционирования Системы.

11.1.1. 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.

11.1.2. 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).

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

11.1.4. Показатели бесперебойности:

Наименование показателя	**Формат**	**Пороговые уровни показателей бесперебойности функционирования платежной системы**	**Процедура/методика формирования**
Продолжительность восстановления оказания УПИ (П1):			
период времени восстановления оказания услуг операторами УПИ в случае приостановления оказания УПИ, в том числе вследствие нарушения требований к обеспечению защиты информации при	в часах/ минутах/ секундах	П1 ≤ 6 часов Приостановление оказания УПИ длительностью не более 6 часов 00 мин. 00 секунд	Рассчитывается по каждому из ОУПИ и по каждому из инцидентов, повлекших приостановление оказания УПИ. При возникновении инцидентов, повлекших

осуществлении переводов денежных средств. Определяется как период времени с момента приостановления оказания УПИ вследствие инцидента, произошедшего у оператора УПИ, и до момента восстановления оказания УПИ.			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 О УПИ, у которых возникли инциденты
Непрерывность оказания УПИ (П2):			
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	в часах/ минутах/ секундах	П2 ≥ 6 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 Федерального закона от 27 июня 2011 года N 161-ФЗ	Рассчитывается по каждому из ОУПИ при возникновении каждого из инцидентов, повлекших приостановление оказания УПИ. Если ОУПИ оказывает более одного вида УПИ одновременно, показатель П2 должен рассчитываться одновременно по всем видам УПИ, оказываемым данным ОУПИ
Соблюдение регламента (П3):			
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	% с точностью до двух знаков после запятой (с округлением по математическому методу).	П3 ≥ 98,00 % - для операционного центра и платежного клирингового центра, П3 ≥ 99,00 % - для расчетного центра, рассчитывается ежемесячно по каждому оператору УПИ по формулам п.3. Приложения 1 к Положению ЦБ РФ № 607-П от 03.10.2017. Значение показателя П3 по платежной системе в целом принимается равным наименьшему из значений	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

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		данного показателя, рассчитанных по всем ОУПИ в отношении всех видов оказываемых ими услуг. При этом если оператор УПИ оказывает более одного вида УПИ одновременно, показатель П3 должен рассчитываться по данному оператору УПИ в отношении всех видов оказываемых им услуг.	участников платежной системы (их клиентов), по которым были оказаны услуги платежного клиринга в течение календарного месяца
Доступность операционного центра ПС (П4):			
характеризует оказание операционных услуг операционным центром платежной системы как среднее значение коэффициента доступности операционного центра платежной системы за календарный месяц	% с точностью до двух знаков после запятой (с округлением по математическому методу).	П4 ≥ 96,00 %, рассчитывается ежемесячно по каждому оператору УПИ по формуле п.4. Приложения 1 к Положению ЦБ РФ № 607-П от 03.10.2017. Значение показателя П4 по платежной системе в целом принимается равным наименьшему из значений данного показателя, рассчитанных по всем операционным центрам платежной системы	Для платежных систем с несколькими операционными центрами показатель П4 должен рассчитываться для каждого операционного центра платежной системы
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).	П5 ≤ 400%, рассчитывается ежемесячно по платежной системе в целом и для каждого оператора УПИ в отдельности по формуле п.5. Приложения 1 к Положению ЦБ РФ № 607-П от 03.10.2017. В случае если за предыдущие 12 календарных месяцев, включая оцениваемый месяц, инцидентов не было, значение показателя признается равным нулю	В платежных системах, в которых оператор УПИ оказывает более одного вида УПИ одновременно, показатель П5 должен рассчитываться по данному оператору УПИ в отношении всех видов оказываемых им услуг.

11.2. Управление непрерывностью и порядок осуществления деятельности по обеспечению бесперебойности.

11.2.1. В 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 настоящих Правилах. В соответствии с Правилами организационная модель управления рисками в Системе предусматривает распределение функций между Участниками, Оператором, ОУПИ.

11.2.2. Оператор организует сбор и обработку сведений, в том числе от привлеченных Операторов услуг платежной инфраструктуры, используемых для расчета показателей БФПС, указанных в п.11.1.2 настоящих 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 сведений по Платежной системе и сведений об инцидентах не менее трех лет с даты получения указанных сведений.

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

11.2.3. 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.

11.2.4. 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.

11.2.5. Оператор координирует деятельность Субъектов Системы по обеспечению БФПС.

11.2.6. Оператор, Участники и ОУПИ организуют деятельность по реализации порядка обеспечения БФПС в рамках внутренних систем управления рисками своей деятельности.

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

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

11.2.9. Правила содержат общие принципы функционирования Системы и ее Субъектов, управления рисками, обеспечения бесперебойности и защиты информации, содержат порядок разрешения споров, взаимодействия в чрезвычайных ситуациях, а также порядок взаимодействия в Системе в целом, в т.ч. в целях управления рисками, обеспечения защиты информации и бесперебойности.

11.3. Методика анализа рисков.

11.3.1. 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 настоящих 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.

11.3.2. Методики анализа рисков в Системе обеспечивают:

- выявление и анализ рисков в Системе, включая выявление событий, реализация которых может привести к возникновению инцидента (далее - риск-события), и определение для каждого из выявленных риск-событий величины риска, характеризуемого 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, соответствующих 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).

11.3.3. Методики анализа рисков в Системе предусматривают выполнение следующих мероприятий:

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

- разработку 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 Операторов услуг платежной инфраструктуры и других факторов, влияющих на БФПС;

- формирование перечня возможных риск-событий для каждого бизнес-процесса с указанием причин риск-событий и их последствий;

- 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;

- 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 (далее - профили

рисков).

11.3.4. Оператор составляет профили рисков в соответствии с требованиями, предусмотренными в нормативных документах Банка России, и пересматривает (актуализирует) их не реже одного раза в год.

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

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

11.3.7. 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.

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

11.4. **Порядок информационного взаимодействия Субъектов платежной системы и документационного обеспечения из деятельности по обеспечению БФПС.**

11.4.1. Оператор организует взаимодействие Субъектов Системы по обеспечению БФПС с учетом следующих 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 настоящих Правил.

Оператор определяет функции, выполняемые 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.

11.4.2. С целью обеспечения БФПС Оператор, ОУПИ, и Участники осуществляют информационное взаимодействие. Обмен информацией осуществляется посредством электронной почты, а также по согласованным каналам связи. Порядок обмена информацией указан в п.10.3 настоящих Правил.

11.4.3. 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 .6.9 настоящих Правил, в котором также предусмотреть план восстановления деятельности после сбоев.

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

-политика информационной безопасности;

-политика защиты от вредоносного кода;

-политика использования сети Интернет;

- политика резервного копирования.

11.4.4. Оператор, 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 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 клиринговых позиций и остатках денежных средств на банковских счетах Участников Системы, открытых в расчетном центре;

-иная информация о функционировании Системы, предусмотренная настоящими Правилами.

11.4.5. Оператор информирует о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры:

- Банк России и Участников Системы в порядке, установленном Указанием Банка России от 11 июня 2014 года № 3280-У «О порядке информирования оператором платежной системы Банка России, участников платежной системы о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры» (далее - Указание Банка России N 3280-У);

- ОУПИ в порядке, аналогичном установленному Указанием Банка России N 3280-У для Участников Системы.

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

11.5.1. 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.

11.5.2. 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 ОУПИ, а также Участников, которым установлен лимит на операции;
- осуществляет контроль соблюдения Правил в соответствии с п.6.7 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 п.11.2.2 настоящих Правил.

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

Оператор определяет следующий порядок проведения контроля за соблюдением ОУПИ и Участниками порядка обеспечения БФПС.

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

Оператор при выявлении нарушения порядка обеспечения БФПС ОУПИ и Участниками:

- информирует 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 Операторов услуг платежной инфраструктуры и Участников Платежной системы, в деятельности которых выявлены нарушения, о результатах проведенной проверки.

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

11.6. Обязанности ОУПИ по обеспечению бесперебойности оказания услуг платежной инфраструктуры.

11.6.1. Расчетный центр, Операционный центр, Платежный клиринговый центр 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.

11.6.2. Операционный центр, Платежный клиринговый центр дополнительно обязаны осуществлять в части организации управления рисками нарушения БФПСС следующие мероприятия:

- сбор, систематизацию, накопление информации о переводах денежных средств (при выполнении функций ОЦ);
- обеспечение собственной финансовой устойчивости (при выполнении функций ЦПКК), а именно – поддержание ликвидности, соблюдения экономических нормативов, поддержания финансовых показателей в соответствии с требованиями Банка России, обеспечение достаточности денежных средств на счетах ЦПКК в Расчетном центре.

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

11.7. Права и обязанности Оператора.

11.7.1. Оператор имеет право и обязан:

- координировать деятельность Субъектов Системы по обеспечению БФПС;
- определять мероприятия по управлению рисками;
- определять и внедрять способы управления рисками;
- контролировать соблюдение субъектами Системы порядка обеспечения БФПС;
- определять показатели БФПС;
- устанавливать требования к содержанию деятельности по обеспечению БФПС, осуществляемой Субъектами Системы;
- устанавливать допустимый уровень рисков нарушения БФПС;
- осуществлять анализ рисков 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 платежной системе и при оценке влияния инцидентов на БФПС;
- осуществлять мероприятия по минимизации риска, необходимые для достижения или поддержания допустимого уровня рисков нарушения БФПС;
- выявлять текущие изменения присущего уровня риска нарушения БФПС (далее - мониторинг рисков нарушения БФПС);
- проводить оценку системы управления рисками в платежной системе, в том числе используемых методов оценки рисков в платежной системе, результатов применения способов управления рисками в платежной системе, не реже одного раза в год и документально оформлять результаты указанной оценки;
- вносить изменения в систему управления рисками в платежной системе в случае, если действующая система управления рисками в платежной 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 в настоящих Правилах платежной системы;
- осуществлять информационное взаимодействие Субъектов Системы в целях управления рисками нарушения БФПС;
- проверять соблюдение операторами УПИ и участниками платежной системы порядка обеспечения БФПС, в том числе контролировать соответствие документов операторов УПИ порядку обеспечения БФПС, и при выявлении несоответствия документов операторов УПИ порядку обеспечения БФПС направлять рекомендации операторам УПИ по устранению выявленных несоответствий;
- при выявлении нарушения порядка обеспечения БФПС операторами УПИ и участниками платежной системы Оператор должен информировать операторов УПИ и участников платежной системы о выявленных в их деятельности нарушениях и устанавливать сроки устранения нарушений, а также осуществлять проверку результатов устранения нарушений и информировать операторов УПИ и

участников платежной системы, в деятельности которых выявлены нарушения, о результатах проведенной проверки;

- определить ответственность Операторов УПИ и участников ПС за неисполнение порядка обеспечения БФПС;
- разрабатывать, проверять (тестировать) и пересматривать план ОНиВД Оператора, а также организовать проведение Операторами УПИ проверки (тестирования) и пересмотра планов ОНиВД с периодичностью не реже 1 раза в два года.

11.8. Права и обязанности Участников.

11.8.1. 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 своих банковских счетах, используемых для расчетов в рамках Системы.

11.9. Права и обязанности ОУПИ.

11.9.1. ОУПИ имеют право и обязаны обеспечивать:

- соблюдение заключенного с Оператором договора, Правил, законодательных требований;
- надлежащее функционирование операционных и технологических средств, устройств, информационных систем, используемых при расчетах в работе с Системой;
- осуществлять мониторинг рисков нарушения БФПС;
- надлежащую защиту информации.

11.9.2. 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.

11.9.3. 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 ОУПИ и Участниками;
- проведения регулярных проверок Участников на предмет соблюдения условий осуществления переводов денежных средств, требований настоящих 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 настоящих 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 10 рабочих дней на обслуживание к другому ОУПИ, включая РЦ в случае нарушения обслуживающим их РЦ требований к бесперебойности оказания услуг платежной инфраструктуры, в том числе приостановления (прекращения) оказания услуг.

11.9.3.1. Обеспечение БФПС ОУПИ осуществляется путем:

- выполнения функций по управлению риском нарушения БФПС в соответствии с организационной моделью управления рисками в Системе;
- сбора и обработки доступной 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 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 клиринговых услуг 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.

11.9.3.2. 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, настоящих Правил, договоров и условий осуществления переводов денежных средств;
- осуществления контроля использования наименования и товарных знаков Системы исключительно в рамках заключенных договоров и настоящих Правил.

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

11.10.1. ОУПИ проводят оценку качества функционирования операционных и технологических средств и информационных систем путем привлечения независимой организации не реже 1 раза в два года.

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

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

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

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

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

12.1.1. Субъекты Системы используют при осуществлении деятельности по обеспечению БФПС настоящие Правила.

12.1.2. Участники, ОУПИ дополнительно разрабатывают, утверждают и реализуют в своей деятельности планы по обеспечению непрерывности и восстановлению непрерывности своей деятельности.

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

12.1.4. ОЦ, РЦ осуществляет 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 клиринговых позиций, состоянии лимитов, о доступном остатке, о выполнении распоряжений КЦ;
- информацию о статусе перевода в любой момент времени.

12.1.6. Сбор, документирование и обработка информации осуществляется автоматизированным способом с использованием специализированного программного обеспечения, применяемого ОЦ, РЦ.

13. Обеспечение защиты информации в Системе.

13.1. Общие правила осуществления защиты информации.

13.1.1. Обязанности по определению порядка защиты информации распределяются между Оператором, Участниками и ОУПИ.

13.1.2. Оператор в Правилах устанавливает общие требования к защите информации, обрабатываемой Субъектами Системы, подлежащей обязательной защите.

13.1.3. Защита информации осуществляется Участниками и ОУПИ в соответствии с требованиями, установленными Правилами, а также требованиями, предусмотренными нормативными актами и законодательством Российской Федерации, в том числе с учетом специфики деятельности Субъекта Системы.

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 платежной системы, а также в извещениях (подтверждениях), касающихся исполнения распоряжений Участников платежной системы;
- информация об остатках денежных средств на банковских счетах;
- информация, содержащаяся в оформленных в рамках применяемой формы безналичных расчетов распоряжениях клиентов операторов по переводу денежных средств, распоряжениях Участников платежной системы, распоряжениях платежного клирингового центра;
- информация о платежных клиринговых позициях;
- информация, необходимая для удостоверения клиентами права распоряжения денежными средствами;
- информация о конфигурации, определяющей параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается оператором по переводу денежных средств, оператором 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 документы, устанавливающие порядок реализации требований Оператора, законодательства к защите информации.

13.1.7. 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.

13.1.8. 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.

13.2. Требования к обеспечению защиты информации.

13.2.1. Субъекты Системы обязаны обеспечивать защиту информации при осуществлении переводов денежных средств в соответствии с требованиями Постановления Правительства Российской Федерации от 13 июня 2012 года №584 «Положение о защите информации в платежной системе» и Положения Банка России от 09 июня 2012 года №382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (далее – Положение Банка России 382-П).

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, поддержкой программ управления уязвимостями, созданием и поддержанием безопасной сетевой инфраструктуры, мониторингом сетевой инфраструктуры, а также мерами по управлению доступом к защищаемой информации.

13.3.2. 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.

13.3.3. 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.

13.3.4. В рамках реализации мер по внедрению и поддержание мер по управлению доступом к защищаемой информации Субъекты Системы обеспечивают ограничение доступа и учет лиц, имеющих доступ к защищаемой информации, в том числе обеспечивают:

- предоставление доступа к Системе только тем лицам, которым такой доступ необходим для выполнения возложенных на них функций, 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;
- немедленный отзыв доступа при прекращении полномочий лица на доступ к защищаемой информации;
- ограничение доступа к техническим средствам АС Системы;

- невозможность 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.

13.3.5. 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.

13.3.6. 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.

13.3.7. 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.

13.3.8. 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.

13.3.9. 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. Требования по защите АРМ Участника Системы от несанкционированного доступа

13.4.1. Защита АРМ Участника Системы и носителей ключевой информации от несанкционированного доступа осуществляется с целью исключения возможностей:

13.4.2. появления в компьютерах, на которых установлено программного обеспечение Системы, программ, направленных на разрушение, нарушение работоспособности или модификацию ПО Системы, либо на перехват информации;

13.4.3. внесения несанкционированных изменений в технические и программные средства Системы, а также в их состав;

13.4.4. внесения несанкционированных изменений в электронные документы.

13.4.5. Программное обеспечение автоматизированного рабочего места участника Системы рекомендуется устанавливать на отдельный, специально выделенный для этих целей компьютер. В обязательном порядке должна быть обеспечена защита данного компьютера от сетевых атак и антивирусная защита.

13.4.6. Следует принять меры, препятствующие несанкционированному вскрытию системных блоков компьютеров, входящих в состав АРМ Участника Системы.

13.4.7. На компьютере должна быть установлена только одна ОС.

13.4.8. Средствами BIOS компьютера следует исключить возможность загрузки операционной системы, отличной от установленной на жестком диске, т.е. должна быть отключена возможность загрузки с дискет, CD/DVD приводов, USB flash дисков, загрузка по сети и т.п.

13.4.9. Доступ к изменению настроек BIOS должен быть защищен паролем.

13.4.10. Пользователям операционной системы должны быть назначены пароли. Длина паролей должна составлять не менее восьми символов, содержащих в обязательном порядке буквы разных регистров и спецсимволы. Срок действия паролей должен быть ограничен не более чем 6 месяцами.

13.4.11. На АРМ Участника Системы не должны устанавливаться средства разработки ПО и отладчики.

13.4.12. Доступ к АРМ Участника из сети, не являющейся локальной сетью Участника, должен быть полностью блокирован средствами межсетевых экранов. Рекомендуется полностью блокировать сетевой доступ к АРМ Участника средствами персонального межсетевого экрана.

13.4.13. Использование сети Интернет на АРМ Участника должно быть ограничено заранее определенным перечнем доверенных сайтов. Рекомендуется ограничить перечень ресурсов только сайтами Системы. Рекомендуется ограничить или полностью отказаться от

приема внешней (из Сети Интернет) электронной почты. В обязательном порядке получаемая почта должна проверяться антивирусными средствами.

13.4.14. Должно быть установлено и регулярно обновляться антивирусное программное обеспечение. Рекомендуется установить по умолчанию уровень политик безопасности, блокирующий вредоносный и подозрительный код без запроса пользователя АРМ.

13.4.15. Должна производиться установка обновлений безопасности операционных систем на АРМ Участника. Рекомендуется использовать обновление в автоматическом режиме.

13.4.16. Пользователи АРМ, работающие с системой, не должны иметь прав администратора, с целью ограничения возможностей установки под этими учетными записями программного обеспечения на компьютере. Рекомендуется на уровне политики ОС ограничить список запускаемых приложений только известными установленными приложениями. Рекомендуется ограничить список пользователей, имеющих возможность входа в операционную систему, на уровне политики ОС.

13.4.17. В целях защиты АРМ Участника Системы от несанкционированного доступа, дополнительно, рекомендуется установить программно-аппаратный комплекс защиты от несанкционированного доступа. Рекомендуется сформировать с помощью этого комплекса функционально замкнутую среду, обеспечивающую контроль целостности ПО и допускающую работу пользователей строго в рамках, предоставляемых им возможностей и полномочий. Защите с помощью этого комплекса подлежат системные и загрузочные файлы, а также файлы, связанные с работой средств криптографической защиты информации (СКЗИ). Права администратора этого комплекса предоставляются сотруднику подразделения, ответственного за организацию и контроль обеспечения защиты информации в Системе.

13.5. Использование средств криптографической защиты информации.

13.5.1. В рамках Системы для защиты информации используются средства криптографической защиты информации (шифрования) либо программно-аппаратные средства, содержащие модули криптографической защиты информации.

13.5.2. 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 РФ;
- средства криптозащиты, входящие в состав операционных систем, реализующие электронную подпись по алгоритму RSA с длиной ключа не менее 2048 бит.

13.5.3. 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.

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

13.5.5. Для выработки сертификатов ключей работников Субъектов Системы, Оператор определяет корпоративный Удостоверяющий центр. В Системе может быть определено более одного Удостоверяющего центра. Допускается совмещение ролей Удостоверяющего Центра и Операционного Центра.

13.5.6. С целью признания электронных подписей в Системе:

- Субъекты Системы самостоятельно вырабатывают криптографические ключи и обеспечивают работу с ключевой информацией;

- Субъекты запрашивают выработку (изготовление) сертификата ключа электронной подписи в Удостоверяющем Центре;
- в запросе на изготовление сертификата ключа электронной подписи указывается работник Субъекта - Владелец ключа электронной подписи, уполномоченный подписывать расчетные и/или иные документы на бумажных носителях от имени Субъекта Системы;
- Субъект Системы несёт ответственность за достоверность сведений о Владельце, которые были предоставлены им при выпуске сертификата ключа электронной подписи;
- Удостоверяющий центр проводит проверку уникальности ключа электронной подписи до выпуска (изготовления) сертификата ключа;
- Удостоверяющий Центр осуществляет выпуск (изготовление) сертификатов ключей электронной подписи по запросам Субъектов Системы, в том числе, представленных в электронном виде;
- Удостоверяющий Центр ведет архив изготовленных сертификатов ключей электронной подписи;
- Операционный центр Системы закрепляет (регистрирует) выпущенные Удостоверяющим центром сертификаты ключей электронной подписи за Субъектами Системы;
- при компрометации ключа электронной подписи Владелец ключа, или Администратор безопасности Субъекта Системы, незамедлительно оповещает Удостоверяющий Центр с использованием специального одноразового кода оповещения;
- Удостоверяющий Центр, после получения оповещения, вносит изменения в справочник отозванных сертификатов и оповещает Операционный Центр;
- временем с которого перестает действовать ключ электронной подписи, считается время внесения записи в справочник отозванных сертификатов Удостоверяющего Центра;
- Субъекты Системы не обрабатывают электронные сообщения, подписанные с помощью ключей электронной подписи, которые внесены в справочник отозванных сертификатов на момент их отправки.

13.5.7. Регистрация в Операционном центре сотрудников Субъектов, осуществляющих закрепление работников за выполняемыми ролями и/или точками (Администраторов безопасности), и осуществляющих контроль и установку лимитов (Администраторов лимитов), осуществляется только по распоряжению Оператора, на основании письменной заявки Субъекта, подписанной лицом, уполномоченным подписывать документы Системы от имени Субъекта.

13.5.8. Для обеспечения непрерывности деятельности Субъекта, для каждой выделенной роли запрашивается регистрация ключей электронной подписи минимум двух сотрудников Субъекта.

13.5.9. Регистрация иных ключей подписи за работниками Субъекта может проводиться на основании электронного документа, переданного в Операционный центр от имени Администратора безопасности.

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

13.6.1. Субъекты Системы в целях снижения возможных потерь от воздействия вредоносного кода обязаны обеспечить выполнение следующих требований:

- использование технических средств защиты информации, предназначенных для выявления вредоносного кода и для предотвращения воздействия вредоносного кода на объектах информационной инфраструктуры (далее - антивирус);
- регулярное обновление версий антивируса и баз данных, используемых в работе антивируса и содержащих описание вредоносных кодов и способы их обезвреживания;
- функционирование антивируса в автоматическом неотключаемом режиме;
- использование антивирусов различных производителей и их раздельную 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.
- предварительную проверку антивирусом программного обеспечения, устанавливаемого или изменяемого на средствах вычислительной техники, включая банкоматы и платежные терминалы.

13.6.2. Субъекты Системы обеспечивают использование технических средств защиты информации от воздействия вредоносного кода различных производителей и их раздельную 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 банкоматы и платежные терминалы, выполняемой после установки или изменения программного обеспечения.

13.6.3. 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.

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

13.6.5. В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Участник, ОУПИ обеспечивают информирование Оператора; Оператор обеспечивает информирование ОУПИ и Участников.

13.6.6. 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 событий.

13.6.7. Субъект Системы информирует стороны информационного обмена в электронном виде о возобновлении указанного вида информационного обмена после восстановления нормального функционирования средств, используемых в электронном обмене.

13.7. Обеспечение защиты персональных данных в Системе.

13.7.1. 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.

13.8. Информационное взаимодействие при выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.

13.8.1. 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 Системе, 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.

13.8.2. Оператор информирует ОУПИ и Участников о выявленных в Системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, носящих системный характер, а также о рекомендуемых методиках анализа и реагирования на указанные инциденты путем размещения соответствующей информации, направляя информацию по согласованным каналам связи.

13.8.3. Оператор услуг платежной инфраструктуры обеспечивает регистрацию самостоятельно выявленных инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств.

13.8.4. Оператор по переводу денежных средств обеспечивает регистрацию ставших ему известными инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, выявленных клиентами данного оператора по переводу денежных средств.

13.8.5. Оператор по переводу денежных средств обеспечивает регистрацию ставших ему известными инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, выявленных банковскими платежными агентами (субагентами).

13.8.6. Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры определяют во внутренних документах порядок регистрации и хранения сведений об инцидентах, указанных в абзацах первом - третьем подпункта 2.13.4 Положения Банка России 382-П.

13.8.7. ОУПИ и Участники в составе информации о своей деятельности, представляемой в порядке и сроки, определенные Правилами, представляют данные для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств. При этом состав указанных данных должен соответствовать требованиям нормативных актов Банка России (Положение Банка России 382-П), регламентирующих

требования к обеспечению защиты информации в Системе при осуществлении переводов денежных средств.

13.8.8. Информирование оператора платежной системы о выявленных операторами по переводу денежных средств, являющимися участниками платежной системы, и операторами услуг платежной инфраструктуры, привлекаемыми для оказания услуг платежной инфраструктуры в платежной системе, инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, осуществляется ежемесячно.

13.9. Информационное взаимодействие для целей анализа обеспечения в Системе защиты информации

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

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

13.9.3. Информация предоставляется по запросу Оператора не реже 1 раза в два года.

13.9.4. Форма предоставления информации определяется Оператором в соответствующем запросе.

14. Приложения, которые входят в состав настоящих Правил:

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

14.2. Приложение №2. Регламент электронного документооборота.

14.3. Приложение №3. Договор участия в Платежной системе «КП Ритейл».

Приложение №1 к Правилам. Тарифы

Т А Р И Ф Ы

Платежной системы «КП Ритейл»

Категория перевода денежных средств	Тип операции	Тарифы для клиентов (ТДК)	Тарифы для Участников отправляющих (ТУО) и выдающих (ТУИ) переводы
	Отправка Переводов денежных средств без открытия счета по территории Российской Федерации	- от 0% до 4% от суммы Перевода денежных средств; - и/или фиксированная сумма от 0 рублей до 1500 рублей	- от 0% до 45% от суммы комиссии, уплачиваемой Клиентом в соответствии с Тарифами для Клиентов; - и/или от 0% до 1% от суммы Перевода денежных средств; - и/или фиксированная сумма от 0 рублей до 750 рублей.

Переводы в пределах Российской Федерации	Выплата Переводов денежных средств без открытия счета по территории Российской Федерации	Плата не взимается	- от 0% до 35 % от суммы комиссии, уплачиваемой Клиентом в соответствии с Тарифами для Клиентов; - и/или от 0% до 1% от суммы Перевода денежных средств; - и/или фиксированная сумма от 0 рублей до 750 рублей.
Трансграничные переводы	Отправка Переводов денежных средств без открытия счета из Российской Федерации	- От 0% до 4% от суммы Перевода денежных средств; -и/или фиксированная сумма от 0 рублей/долларов США/ЕВРО до 6000 рублей/300 долларов США/300 ЕВРО	- От 0% до 45 % от суммы комиссии, уплачиваемой Клиентом в соответствии с Тарифами для Клиентов; - и/или от 0% до 1,5% от суммы Перевода денежных средств -и/или фиксированная сумма от 0 рублей/долларов США/ЕВРО до 3000 рублей/150 долларов США/ЕВРО
	Выплата Переводов денежных средств без открытия счета	Плата не взимается	- От 0% до 45 % от суммы комиссии, уплачиваемой Клиентом в соответствии с Тарифами для Клиентов; - и/или от 0% до 1,5% от суммы Перевода денежных средств -и/или фиксированная сумма от 0 рублей/долларов США/ЕВРО до 3000 рублей/150 долларов США/ЕВРО
Транзитные переводы	Отправка Переводов денежных средств без открытия счета за пределами РФ	- От 0% до 4% от суммы Перевода денежных средств; -и/или фиксированная сумма от 0 рублей/долларов США/ЕВРО до 6000 рублей/300 долларов США/300 ЕВРО	- От 0% до 45 % от суммы комиссии, уплачиваемой Клиентом в соответствии с Тарифами для Клиентов; - и/или от 0% до 1,5% от суммы Перевода денежных средств -и/или фиксированная сумма от 0 рублей/долларов США/ЕВРО до 3000 рублей/150 долларов США/ЕВРО
	Выплата Переводов денежных средств без открытия счета	Плата не взимается	- От 0% до 45 % от суммы комиссии, уплачиваемой Клиентом в соответствии с Тарифами для Клиентов; - и/или от 0% до 1,5% от суммы Перевода денежных средств

	за пределами РФ		-и/или фиксированная сумма от 0 рублей/долларов США/ЕВРО до 3000 рублей/150 долларов США/ЕВРО
Оплата в пользу юридических лиц за товары, работы, услуги	- 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	- От 0% до 25% от суммы Перевода денежных средств; -и/или фиксированная сумма от 0 до 1000 рублей	- 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

Тариф Оператора, выполняющего функции ОЦ и ПКЦ рассчитывается по следующей формуле:
ТДК – ТУО – ТУИ = Тариф Оператора

Приложение № 2 к Правилам. Регламент электронного документооборота.

Регламент электронного документооборота (РЭДО)

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

Абонент	Участник.
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)	вырабатываемые 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 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 Абонента или оператора услуг платежной инфраструктуры, и имеющее равную юридическую силу с расчетными и иными документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати.
Электронный документооборот (ЭДО)	Обмен Электронными документами и 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.

1.1 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 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 Оператора Системы.

1.2 Электронные сообщения и документы

1.2.1 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.

3) Все отправляемые Участниками сообщения являются Электронными документами, т.е. относятся к категориям 2, 3 или 4.

1.2.2 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.

1.2.3 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 ответа от Принимающей стороны. Датой и временем приема считаются дата и время получения сообщения Принимающей стороной.

1.2.4 Условия принятия Электронных сообщений в обработку Принимающей стороной

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

1) Для сообщений, обмен которых происходит с использованием шифрования, сообщение успешно расшифровано.

2) Сообщение относится к категории 2, 3 или 4, имеет ЭП и положительный результат ее проверки.

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

1.3 Условия организации и правила осуществления ЭДО

1.3.1 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.

1.3.2 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.

1.3.3 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.

1.3.4 Учет Электронных документов

1) Учет Электронных документов осуществляется путем ведения электронных журналов учета или традиционных бумажных журналов учета. 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) Операторы услуг платежной инфраструктуры и 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.

1.3.5 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.

1.3.6 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.

1.4 Обеспечение информационной безопасности при ЭДО

1.4.1 Общие положения информационной безопасности

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

1.4.2 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 РФ

3) Криптографический протокол TLS

1.4.3 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 по адресу

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 истечение 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.

1.4.4 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.

3) Порядок хранения и использования носителей ключевой информации должен исключать возможность использования ключей лицами, не являющимися их Владельцами.

4) Владельцам не разрешается:

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 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 и Владельцами ключей, и ведётся журнал такого доступа.

13) В иных случаях для хранения носителей ключевой информации должны использоваться надежные металлические сейфы. В этом случае по окончании рабочего дня, а также вне времени сеансов связи с Системой, носители ключевой информации должны храниться в сейфе. 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.

1.4.5 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 цента 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.

1.4.6 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 удается 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. 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. 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 устанавливает на персональный компьютер эталонную операционную систему и эталонное программное обеспечение, хранящееся у Операционного центра. 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 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) При проведении экспертизы при необходимости по электронным документам могут быть изготовлены в установленном порядке их бумажные копии.

23) Экспертная комиссия не дает правовой оценки действиям сторон.

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

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

Приложение №3 к Правилам. Договор

ДОГОВОР УЧАСТИЯ
в Платежной системе «КП Ритейл» №__

г. Москва «___» _____ 201___ г.

Общество с ограниченной ответственностью «КП Ритейл», именуемое в дальнейшем Оператор, в лице _____, действующего на основании _____, с одной стороны, и _____, именуемый в дальнейшем Участник, в лице _____, действующего(ей) на основании_____, с другой стороны, вместе именуемые «Стороны», а по отдельности «Сторона», заключили настоящий договор (далее – Договор) о нижеследующем:

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.
Термины в тексте настоящего Договора имеют значение, изложенное в Правилах Платежной системы «КП Ритейл».

2. ПРЕДМЕТ ДОГОВОРА.
2.1. Участник присоединяется к Правилам Платежной системы «КП Ритейл» (далее – Правила) путем принятия их в целом и на условиях, приведенных в Правилах.
2.2. Правила Системы публикуются на официальном сайте Оператора в сети интернет по адресу www.cpretail.ru

3. ОБЩИЕ ПОЛОЖЕНИЯ.

3.1. Права и обязанности Сторон:
3.1.1. Оператор обязан обеспечить Участнику возможность предоставления клиентам Услуг системы «КП Ритейл» на условиях Правил посредством:
- регистрации Участника в Системе и информирования других Участников о данном включении;
- обеспечения оказания Участнику услуг платежной инфраструктуры путем привлечения третьих лиц – операторов услуг платежной инфраструктуры в соответствии с Правилами.
3.1.2. Оператор обязан информировать Участника об изменении Правил, публикуя новую редакцию на официальном сайте Системы в сети интернет в порядке и сроки, указанные в Правилах.
3.1.3. Оператор вправе вносить изменения в Правила и контролировать выполнение Правил Участниками.
3.1.4. Оператор вправе без предварительного уведомления Участника временно приостановить по собственной инициативе полностью или частично работу Участника в Системе в случаях неисполнения им своих обязательств в рамках настоящего Договора, а также в случае нарушения положений Правил. О данном факте Оператор незамедлительно уведомляет Участника по согласованному каналу связи.
3.1.5. Участник обязуется открыть счет в расчетном центре Системы.
3.1.6. Участник обязуется самостоятельно организовать и поддерживать финансовое, техническое и технологическое обеспечение предоставления Услуг системы «КП Ритейл».
3.1.6. Участник обязуется предоставлять Услуги системы «КП Ритейл» в полном соответствии с Правилами.
3.1.7. Участник обязуется предоставлять услуги Системы в пределах, установленных лицензией на осуществление банковских операций, выданных участнику Банком России, в полном соответствии с Правилами Системы.
3.2. Порядок расчетов регламентируется Правилами Системы.
3.3. За предоставление Услуг системы «КП Ритейл» Участник уплачивает и получает комиссию в размере, указанном в Тарифах Системы.
3.4. Иные права и обязательства Сторон устанавливаются Правилами.

3.5. В качестве согласованных каналов связи Стороны договорились использовать следующие адреса электронной почты:

Оператор	Участник

3.6. Об изменении согласованных каналов связи Стороны уведомляют друг друга посредством сообщений с адресов электронной почты, указанных в п. 3.5 настоящего Договора, либо путем направления письменного уведомления на бумажном носителе, подписанном уполномоченными лицами соответствующей Стороны.

4. КОНФИДЕНЦИАЛЬНОСТЬ.

4.1. Стороны обязуются сохранять конфиденциальность данных, получаемых при работе в Системе, в т.ч. и персональных данных, и предоставлять доступ к информации третьим лицам только с согласия владельца информации, за исключением случаев, когда предоставление информации осуществляется в соответствии с требованиями законодательства страны местонахождения Участника или условиями, изложенными в Правилах.

4.2. В случае расторжения настоящего Договора участия в Платежной системе «КП Ритейл» Стороны обязаны соблюдать требования о конфиденциальности информации и сведений, полученных ими в период срока его действия, в течение пяти лет с даты его расторжения (окончание срока действия.

5. ДЕЙСТВИЕ ДОГОВОРА И ПОРЯДОК ЕГО ПРЕКРАЩЕНИЯ И ИЗМЕНЕНИЯ.

5.1. Договор вступает в силу с даты его подписания обеими Сторонами и действует в течение неопределённого периода времени, до его расторжения по соглашению Сторон, или отказа одной из Сторон от его исполнения, либо до момента прекращения настоящего Договора по иным основаниям.

5.2. Настоящий Договор может быть изменен и/или дополнен по взаимному согласию Сторон, путем подписания дополнительного соглашения.

5.3. Настоящий Договор составлен в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

5.4. Договор может быть расторгнут по соглашению Сторон, или по инициативе одной из Сторон при условии полного урегулирования всех финансовых и иных обязательств до даты расторжения настоящего Договора. О намерении расторгнуть настоящий Договор заинтересованная Сторона обязана предупредить другую Сторону не позднее, чем за 30 (Тридцать) календарных дней до даты предполагаемого расторжения, и полностью урегулировать финансовые обязательства. Предупреждение о намерении расторгнуть настоящий Договор направляется заинтересованной Стороной в письменном виде заказным письмом с уведомлением о вручении и за подписью уполномоченного лица, по адресам, Сторон, указанным в разделе 6 настоящего Договора.

6. АДРЕСА И РЕКВИЗИТЫ СТОРОН.

Пронумеровано, прошито, скреплено печатью
11 (семьдесят один) листа(ов)

Генеральный директор ООО «КП Ритейл»

_____ Г.В. Русов

«12» июня 2019 года

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ ОГРН 1137746174791
"КП Ритейл"
"Ltd. CR Retail"
* МОСКВА *