УТВЕРЖДЕНЫ
Приказом Генерального директора
ООО «КП Ритейл»
№ 13-06-2023/1 от 13.06.2023 г.
Вступают в силу с 12.07.2023 г.

Правила Платежной системы «КП Ритейл»

Редакция 7

г. Москва - 2023 г.

Оглавление

1. Введение

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

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

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

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

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

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

Правила, а также тарифы, являющиеся частью Правил, публикуются в открытом доступе на официальном сайте оператора платежной системы в информационно-телекоммуникационной сети «Интернет» по адресу: https://cpretail.ru.

2. Термины и определения

Для целей Правил используются следующие термины и определения:

Авторизация – разрешение, на осуществление операций с использованием электронного средства платежа.

Авторизационный запрос – запрос плательщика на осуществление Авторизации.

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

Банковская карта (либо Карта) – эмитированная участником платежной системы для Плательщика карта в электронном виде, в том числе таможенная карта, или её реквизиты, используемые для составления расчетных и иных документов к счету плательщика, открытому у участника платежной системы, подлежащих оплате за счет плательщика, являющаяся электронным средством платежа.

БФПС – бесперебойность функционирования Системы.

Инцидент – событие, которое привело к нарушению оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, в том числе вследствие нарушений требований к обеспечению защиты информации при осуществлении переводов денежных средств, в результате которых приостанавливалось оказание услуг платежной инфраструктуры и/или нарушался регламент выполнения процедур (время начала, время окончания, продолжительность и последовательность процедур, выполняемых операторами услуг платежной инфраструктуры при оказании операционных услуг, услуг платежного клиринга и расчетных услуг).

Конфигурация Участника – регистрация участника платежной системы в перечне участников платежной системы, заведение сведений об участнике платежной системы в базы

данных программного комплекса «КП Ритейл», установление параметров участника платежной системы для целей оказания операционных услуг и услуг платежного клиринга, присвоение идентификационного кода.

Лимит по Банковской карте/Лимит ЭСП – максимальная сумма операций, которые могут быть совершены с использованием Банковской карты (ЭСП).

Кабинет Участника – интерфейс для информационного обмена между Оператором и Участниками Системы. Доступ к Кабинету Участника организован на официальном сайте Оператора в информационно-телекоммуникационной сети «Интернет» с использованием индивидуального логина и пароля.

Межсистемная Операция – операция, в осуществлении которой участвуют Субъекты Системы и/или устройство приема платежа разных платежных систем.

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

Оператор по переводу денежных средств (участник платежной системы) - организация, которая в соответствии с законодательством Российской Федерации вправе осуществлять перевод денежных средств.

Операторы услуг платежной инфраструктуры (Операторы УПИ) – операционный центр Системы, платежный клиринговый центр Системы и расчетный центр Системы.

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

Операция - операция по переводу денежных средств или иная операция, в том числе совершенная с использованием Устройства приема платежей.

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

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

План ОНиВД - план действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности субъекта Системы в случае возникновения нестандартных и чрезвычайных ситуаций, в том числе направленный на обеспечение БФПС.

Платежный клиринговый центр (ПКЦ) – организация, созданная в соответствии с законодательством Российской Федерации, обеспечивающая в рамках Системы прием к исполнению распоряжений участников платежной системы об осуществлении перевода денежных средств и выполнение иных действий, предусмотренных Законом о НПС.

Плательщик (Клиент участника платежной системы) – физическое или юридическое лицо, имеющее банковский счет, открытый у Участника платежной системы, и осуществляющее в рамках Системы Операции в целях перевода денежных средств.

Получатель – физическое или юридическое лицо, для перевода денежных средств которому совершена Операция по переводу денежных средств. При совершении Операций по переводу денежных средств с использованием таможенных карт - организация, определяемая в соответствии с законодательством Российской Федерации как получатель таможенных платежей.

Пользователь ЭСП (Клиент участника платежной системы) - физическое лицо или уполномоченный представитель Клиента - юридического лица, которые имеют доступ к электронному средству платежа.

Предельный размер (лимит) обязательств Участника – установленная в соответствии с Правилами максимальная сумма денежных средств, в пределах которой в Системе принимаются к исполнению распоряжения Участника платежной системы, включая Операции по переводу денежных средств, инициированные Клиентами Участника.

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

Реестр ПКЦ - формируемый Оператором, выполняющим функции ПКЦ, и направляемый участнику платежной системы документ в электронной форме, содержащий информацию по принятым к исполнению распоряжениям на проведение Операций.

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

Стандарты Системы – документы Системы, включающие описание продуктов, используемых в Системе, методику анализа и оценки риска информационной безопасности в Системе, методику реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Системе, порядок электронного документооборота между Субъектами Системы, порядок эмиссии и обслуживания банковских карт в Системе, а также иные условия и документы, необходимые для функционирования Системы, принимаемые Оператором в одностороннем порядке и обязательные для соблюдения Субъектами Системы. Стандарты Системы размещаются Оператором на Официальном сайте Оператора в сети интернет.

Согласованный канал связи – средства и способы, определенные совместно Оператором и участником платежной системы, Оператором и привлеченными Операторами УПИ для информационного обмена и расчетов, указанные в заключенных между ними договорах и/или Правилах.

Субъекты Системы – Оператор, Операторы УПИ и Участники платежной системы.

Счет Участника – банковский счет участника платежной системы, открытый в РЦ, используемый для перевода денежных средств и/или расчетов в рамках Системы.

Система электронного документооборота (СЭДО) – транспортная система обмена документами по защищенным каналам связи, позволяющие при информационном обмене между Оператором и Субъектами Системы передавать документы в зашифрованном виде, подписанные электронной подписью стороны, сформировавшей документ. Электронный документооборот между Участниками и Операционным центром, Платежным клиринговым центром, между Расчетным центром и Операционным центром, Платежным клиринговым центром, осуществляется в порядке и на условиях, определенных в Стандартах Системы.

Таможенная Карта «Мир» - платежная карта, выпущенная участником платежной системы «Мир» в соответствии с правилами платежной системы «Мир», предназначенная исключительно для совершения перевода денежных средств в целях уплаты таможенных платежей, совершенных с использованием устройств приема платежей.

Таможенные платежи – таможенные пошлины, авансовые платежи, налоги, пени, проценты, штрафы и иные платежи, взимание которых возложено на таможенные органы в соответствии с законодательством Российской Федерации.

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

Управление непрерывностью функционирования Системы – выявление оказания услуг платежной инфраструктуры, не соответствующих требованиям к оказанию услуг, обеспечению функционирования Системы в случае нарушения оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, и восстановлению оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, включая восстановление оказания услуг платежной инфраструктуры в случае приостановления их оказания в течение периодов времени, установленных Оператором в Правилах.

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

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

Услуги платежной инфраструктуры (УПИ) - операционные услуги, услуги платежного клиринга, расчетные услуги.

Устройство приема платежей – программное и/или аппаратно-программное устройство, осуществляющее информационное взаимодействие с ОЦ и предназначенное для совершения Операций с использованием Электронных средств платежа, без возможности приема (выдачи) наличных денежных средств.

Участник платежной системы (Участник) – Оператор по переводу денежных средств, присоединившийся к Правилам, в целях оказания услуг по переводу денежных средств в рамках Системы.

Электронное средство платежа (**ЭСП**) - средство и (или) способ, позволяющие Клиенту Участника 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 Банковских карт, а также иных технических устройств.

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

3. Субъекты Системы и их функции

Функции Оператора: определение Правил Системы, а также выполнение иных обязанностей, предусмотренных Законом о НПС и Правилами, в том числе привлечение Участников, Операторов УПИ, контроль соблюдения Правил Участниками и Операторами УПИ.

Функции ОЦ: обеспечение в рамках Системы Участникам, их Клиентам доступа к Системе, Услугам Системы, в том числе с использованием ЭСП, а также обмена электронными сообщениями (операционные услуги).

Функции ПКЦ: обеспечение в рамках Системы приема к исполнению распоряжений Участников на перевод денежных средств и выполнение иных действий, предусмотренных Законом о НПС, в том числе дальнейшей передачи РЦ подлежащих исполнению распоряжений для осуществления РЦ его функций (услуги платежного клиринга).

Функции РЦ: обеспечение в рамках Системы исполнения поступивших от ПКЦ Реестров распоряжений или распоряжений, поступивших от Участника, посредством списания и зачисления денежных средств по Счетам Участников, направление

подтверждений, касающихся исполнения Реестров распоряжений и распоряжений Участников (расчетные услуги).

В Системе может действовать более чем один РЦ.

Функции Участников: предоставление Клиентам Услуг Системы.

Субъекты Системы при осуществлении своих функций в рамках Системы обязаны руководствоваться Правилами, а в части, неурегулированной Правилами, Законом о НПС, нормативными актами Банка России, иными нормативно-правовыми актами.

Оператор выполняет функции ОЦ и ПКЦ Системы. Полный перечень Операторов УПИ доступен для ознакомления на Официальном сайте Оператора в сети интернет.

4. Права и обязанности Субъектов Системы

4.1. Обязанности Оператора

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

4.1.2. Определять Правила, организовывать и осуществлять контроль за их соблюдением Участниками и Операторами УПИ.

4.1.3. Осуществлять привлечение Операторов УПИ (за исключением случаев, когда Оператор совмещает функции ОЦ и ПКЦ), которые находятся на территории Российской Федерации и соответствуют требованиям, установленным законодательством Российской Федерации и Правилами, обеспечивать контроль оказания УПИ, вести перечень Операторов УПИ.

4.1.4. Устанавливать требования к Операторам УПИ, с которыми могут заключаться договоры при их привлечении Оператором, в том числе в части их финансового состояния, технологического обеспечения.

4.1.5. Определять Стандарты Системы, организовывать и осуществлять контроль за их соблюдением Участниками и Операторами УПИ. Уведомлять Участников и Операторов УПИ по согласованным каналам связи о внесении изменений в Стандарты Системы за 2 (два) месяца до вступления изменений в силу.

4.1.6. При наличии в Системе двух и более РЦ обеспечивать взаимозаменяемость РЦ и (или) возможность для Участников осуществить переход в течение не более 20 (Двадцати) рабочих дней на обслуживание к другому (резервному) РЦ, в случае нарушения обслуживающим их РЦ требований к БФПС, в том числе приостановления (прекращения) оказания УПИ.

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

4.1.8. Обеспечить прием и обработку обращений Участников по вопросам БФПС.

4.1.9. Обеспечить возможность досудебного рассмотрения споров с Участниками и Операторами УПИ в соответствии с Правилами.

4.1.10. Обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных, информации при осуществлении переводов денежных средств, иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации и требованиями к защите указанной информации, установленными Правительством Российской Федерации, Банком России и Правилами, в том числе реализовывать мероприятия по противодействию осуществлению переводов денежных средств без согласия Клиента Участника (Участника).

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

4.1.12. Обеспечивать бесперебойность оказания УПИ Участникам и управление непрерывностью функционирования Системы.

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

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

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

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

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

4.1.17. Информировать Участников о случаях и причинах приостановления (прекращения) оказания УПИ в порядке, установленном пунктом 10.7.6. Правил.

4.2. Права Оператора

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

4.2.2. В одностороннем порядке вносить изменения в Стандарты Системы.

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

4.2.4. Совмещать свою деятельность с деятельностью Оператора УПИ (за исключением РЦ) и с иной деятельностью, если это не противоречит законодательству Российской Федерации.

4.2.5. Размещать в публичном доступе перечень Участников.

4.2.6. Приостанавливать и прекращать участие Участников в Системе в порядке и по основаниям, установленным Правилами.

4.2.7. Уведомлять Участников о необходимости смены РЦ в более сокращенные сроки, чем установлены в Правилах, в случае наличия объективной информации о наличии риска невыполнения РЦ своих обязательств по обеспечению БФПС.

4.2.8. Устанавливать, изменять Предельные размеры (лимиты) обязательств Участников.

4.2.9. Организовывать продвижение Услуг Системы.

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

4.3. Обязанности Участников

4.3.1. Соблюдать Правила.

4.3.2. Соблюдать порядок обеспечения БФПС в рамках выполняемого функционала.

4.3.3. Открыть Счет Участника в РЦ. Контролировать достаточность денежных средств на Счете Участника в РЦ для бесперебойности расчетов и выполнения своих обязательств в рамках Системы.

4.3.4. Предоставлять услуги по переводу денежных средств в строгом соответствии с требованиями законодательства Российской Федерации и Правил. Участник несет финансовую ответственность перед Оператором за неисполнение, несвоевременное исполнение своих обязательств в рамках Системы.

4.3.5. Соблюдать применимые к участнику Стандарты Системы.

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

4.3.7. Оплачивать услуги, предоставляемые Оператором и привлеченными Операторами УПИ, в сроки и в порядке, определенные Правилами и договорами, заключенными в рамках Системы.

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

4.3.9. Сообщать Оператору обо всех Инцидентах, включая инциденты информационной безопасности.

4.3.10. Самостоятельно нести ответственность за соблюдение требований применимого законодательства Российской Федерации, в том числе законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения, о защите персональных данных.

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

4.3.12. Обеспечивать защиту информации при осуществлении переводов денежных средств в соответствии с требованиями, установленными законодательством Российской Федерации, Правительством Российской Федерации, Банком России и Правилами, в том числе реализовывать мероприятия по противодействию осуществлению переводов денежных средств без согласия Клиента Участника в соответствии с требованиями Правил.

4.3.13. Выполнять другие обязательства в соответствии с Правилами.

4.4. Права Участников

4.4.1. Участвовать в других платежных системах.

4.4.2. Полностью или частично приостановить участие в Системе.

4.5. Обязанности ОЦ

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

4.5.2. Обеспечивать обмен электронными сообщениями.

4.5.3. Обеспечивать защиту обрабатываемой в соответствии с выполняемыми функциями ОЦ информации.

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

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

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

4.5.7. Соблюдать порядок обеспечения БФПС в рамках выполняемого функционала.

4.5.8. Выполнять иные обязательства в соответствии с Правилами.

4.6. Права ОЦ

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

4.7. Обязанности ПКЦ

4.7.1. Выполнять процедуры приема к исполнению распоряжений на перевод денежных средств, переданных Участниками, включая проверку соответствия распоряжений установленным требованиям.

4.7.2. Определять достаточность денежных средств для исполнения распоряжений Участников.

4.7.3. Определять платежные клиринговые позиции Участников на валовой основе.

4.7.4. Направлять Участнику Реестры ПКЦ в сроки и в порядке, определенные Правилами.

4.7.5. Передавать РЦ от имени Участников подлежащие исполнению распоряжения Участников на перевод денежных средств в виде Реестра распоряжений.

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

4.7.7. Не раскрывать третьим лицам сведения об Операциях, о Счетах Участников и Клиентах Участников, полученные при оказании УПИ, за исключением передачи информации в рамках Системы, а также случаев, предусмотренных федеральными законами.

4.7.8. Соблюдать порядок обеспечения БФПС в рамках выполняемого функционала.

4.7.9. Выполнять иные обязательства в соответствии с Правилами.

4.8. Права ПКЦ

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

4.9. Обязанности РЦ

4.9.1. Соблюдать Правила.

4.9.2. Уведомлять Оператора об открытии/закрытии Счетов Участников в течение 3 (Трех) рабочих дней с момента их открытия/закрытия.

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

4.9.4. Обеспечивать в рамках Системы своевременное и полное исполнение Реестра распоряжений, полученного от Оператора, выполняющего функции ПКЦ, распоряжений, полученных от Участников в рамках заключенного с РЦ договора на оказание расчетных услуг, посредством списания/зачисления денежных средств со/на Счетов/Счета Участников и перечисления денежных средств Получателю соответственно.

4.9.5. Обеспечивать направление Оператору, выполняющему функции ПКЦ, подтверждений, касающихся исполнения Реестра распоряжений, и Участникам извещений об исполнении распоряжений Участников, полученных в соответствии с заключенным договором на оказание в рамках Системы расчетных услуг.

4.9.6. Передавать Оператору, выполняющему функции ПКЦ, сведения об остатках на Счетах Участников и проведенных по Счетам Участников платежах, связанных с осуществлением расчетов по Операциям, совершенным в рамках Системы, в сроки, определенные Правилами и/или договором между Оператором, выполняющим функции ПКЦ, и РЦ.

4.9.7. Обеспечивать защиту информации при осуществлении переводов денежных средств в соответствии с требованиями, установленными законодательством Российской

Федерации, Правительством Российской Федерации, Банком России и Правилами, в том числе реализовывать мероприятия по противодействию осуществлению переводов денежных средств без согласия Клиента Участника (Участника).

4.9.8. Обеспечивать бесперебойность оказания расчетных услуг, самостоятельно организовывать управление рисками, присущими деятельности РЦ – кредитной организации.

4.9.9. Соответствовать требованиям финансовой устойчивости и к управлению рисками, установленным Банком России, технологическим требованиям к работе в Системе, позволяющим обеспечить выполнение требований законодательства Российской Федерации, нормативных актов Правительства Российской Федерации, Банка России и Правил в части обеспечения БФПС, обеспечения защиты информации в собственных информационных системах, а также при взаимодействии с Субъектами Системы.

4.9.10. Самостоятельно нести ответственность за соблюдение требований применимого законодательства Российской Федерации, в том числе законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения, о защите персональных данных.

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

4.9.12. Соблюдать применимые к РЦ Стандарты Системы.

4.9.13. Соблюдать порядок обеспечения БФПС в рамках выполняемого функционала.

4.9.14. Незамедлительно информировать Оператора обо всех событиях, которые привели к нарушению оказания расчетных услуг, соответствующих требованиям к оказанию услуг, в том числе об Инцидентах, включая инциденты информационной безопасности в порядке, установленном в пункте 6.12.1. Правил.

4.9.15. Предоставлять по запросу Оператора План ОНиВД РЦ.

4.9.16. Выполнять иные обязательства в соответствии с Правилами.

4.10. Права РЦ

4.10.1. Совмещать свою деятельность с деятельностью Участника. В случае совмещения деятельности открывать Счет Участника в РЦ не требуется.

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

4.10.3. Вводить плату за предоставление услуг по ведению Счета Участника.

5. Порядок привлечения Операторов УПИ, ведение перечня Операторов УПИ, требования к Операторам УПИ

5.1. Порядок привлечения Операторов УПИ, ведение перечня Операторов УПИ

5.1.1. В Системе Оператор совмещает свою деятельность с деятельностью Операторов УПИ, за исключением деятельности РЦ.

5.1.2. Оператор, в том числе с целью обеспечения БФПС, принимает решение о необходимости привлечения Операторов УПИ и об объеме выполняемых ими функций.

5.1.3. Привлечение Операторов УПИ осуществляется Оператором на основании договора, заключаемого между Оператором и Оператором УПИ.

5.1.4. Привлечение осуществляется на условиях обеспечения равноправного доступа Операторов УПИ в Систему и отсутствия условия об исключительном оказании УПИ.

5.1.5. Ведение перечня Операторов УПИ осуществляется Оператором самостоятельно путем включения в него информации об Операторе УПИ с указанием его типа.

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

5.2. Требования к Операторам УПИ

5.2.1. Требования к РЦ:

- РЦ может выступать кредитная организация, созданная в соответствии с законодательством Российской Федерации, в том числе небанковская кредитная организация, которая не менее 1 (Одного) года осуществляет переводы денежных средств по открытым в этой кредитной организации банковским счетам;
- РЦ должен соответствовать требованиям к финансовой устойчивости, установленным Банком России;
- РЦ должен выполнять обязательные требования Банка России, в том числе требования по обеспечению мер по противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения;
- РЦ должен обеспечивать банковскую тайну, защиту информации при осуществлении переводов денежных средств и персональных данных Плательщиков (в случае их получения и обработки) в соответствии с законодательством Российской Федерации.

5.2.2. Требования к ОЦ:

- Оператор самостоятельно осуществляет функции ОЦ и не привлекает сторонние организации в качестве Операционных центров, за исключением случаев, указанных в пункте 10.6.3.4. Правил;
- Оператор обязан соответствовать требованиям, предъявляемым действующим законодательством Российской Федерации к организациям, осуществляющим деятельность в качестве ОЦ.

5.2.3. Требования к ПКЦ:

- Оператор самостоятельно осуществляет функции ПКЦ и не привлекает сторонние организации в качестве ПКЦ, за исключением случаев, указанных в пункте 10.6.3.4. Правил;
- Оператор обязан соответствовать требованиям, предъявляемым законодательством Российской Федерации к организациям, осуществляющим деятельность в качестве ПКЦ;
- Оператор, оказывая услуги платежного клиринга, обязуется передавать РЦ от имени Участников подлежащие исполнению распоряжения Участников на перевод денежных средств в виде Реестра распоряжений.

5.2.4. Операторы УПИ не вправе в одностороннем порядке приостанавливать (прекращать) оказание УПИ Участникам.

5.2.5. Оператор в отношении привлеченных Операторов УПИ самостоятельно, в том числе используя общедоступную информацию, а также при необходимости запрашивая от привлеченных Операторов УПИ дополнительную информацию о текущей деятельности, осуществляет мониторинг деятельности привлеченных Операторов УПИ на соответствие требованиям, установленным в пунктах 5.2.1- 5.2.3 Правил. Мониторинг деятельности привлеченных Операторов УПИ осуществляет структурное подразделение (работник) Оператора, ответственное(ый) за управление рисками, присущими деятельности Системы. Результаты мониторинга ежегодно оформляются в виде отчета и направляются не позднее последнего числа первого месяца года, следующего за отчетным, на рассмотрение единоличному исполнительному органу Оператора.

6. Порядок взаимодействия между Субъектами Системы

6.1. Организация взаимодействия Субъектов Системы

6.1.1. Операции по переводу денежных средств в Системе инициируются Клиентами Участников. Для проведения перевода денежных средств в Системе могут использоваться ЭСП и Устройства приема платежей.

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

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

6.2. Взаимодействие Оператора с Участниками

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

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

6.2.3. Взаимодействие Оператора с Участниками осуществляется на основании Правил и Договора участия.

6.2.4. После подписания Договора участия и оплаты Конфигурации Участника в Системе Оператор в срок, не превышающий 2 (Две) недели, осуществляет Конфигурацию Участника в Системе.

6.2.5. Оператор, в соответствии с Правилами:

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

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

- Официальный сайт Оператора в сети интернет;
- Кабинет Участника;
- СЭДО;
- электронная почта Оператора: адреса, принадлежащие домену @cpretail.ru или доведенные до Участника уполномоченными должностными лицами Оператора (информационные рассылки, осуществляемые с таких адресов, являются официальными сообщениями Оператора);
- обмен сообщениями на бумажных носителях, направляемых сторонами друг другу с привлечением организаций почтовой связи, компаний экспресс-доставки документов, курьеров, а также осуществляемый уполномоченными представителями сторон;
- электронная почта Участника: адреса представителей Участника, указанные в Договоре участия, в официальном сообщении Участника, направленном Оператору на бумажном носителе или на электронный адрес Оператора.

6.2.7. Порядок электронного документооборота между Оператором и Участником при использовании СЭДО устанавливается Оператором в виде Стандарта Системы и доводится до Участника по Согласованным каналам связи.

6.2.8. Оператор вправе устанавливать Предельные размеры (лимиты) обязательств Участника с учетом уровня риска. Предельный размер (лимит) обязательств Участника состоит из остатка на Счете Участника и суммы превышения остатка на Счете Участника, определенной Оператором и согласованной с Участником.

Сумма допустимого превышения остатка на Счете Участника, включенная в Предельный размер (лимит) обязательств Участника, устанавливается в соответствии с внутренними процедурами Оператора на основании комплексной оценки Участника и анализа его финансовой устойчивости.

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

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

6.3. Критерии участия в Системе

6.3.1. Взаимодействие в рамках Системы возможно только при условии присоединения Участника к Правилам.

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

6.3.3. Участником может стать кредитная организация при соответствии следующим критериям:

- наличие действующей лицензии на осуществление банковских операций, выданной Банком России;
- кредитная организация не находится в стадии ликвидации, банкротства, является финансовой устойчивой;
- обеспечено наличие технической возможности интеграции в Систему.

6.3.4. Участник считается присоединившимся к Системе после подписания с Оператором Договора участия.

6.3.5. Подписывая Договор участия, Участник гарантирует соблюдение требований применимого законодательства Российской Федерации и выполнением им мер по защите информации при осуществлении переводов денежных средств.

6.3.6. Датой начала участия в Системе является дата заключения Договора участия в Системе.

6.3.7. Оператор устанавливает виды участия в Системе:

- прямое участие, предусматривающее обязательное открытие Счета Участника в РЦ.

6.4. Порядок присвоения идентификационного номера

6.4.1. Участнику присваивается идентификационный цифровой четырехразрядный код, позволяющий однозначно определить Участника в Системе.

6.4.2. Идентификационный код присваивается Участнику в процессе Конфигурации Участника.

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

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

- случаи несоблюдения Участником своих обязательств, установленных Правилами;
- зафиксированные случаи утраты соответствия критериям участия;
- случаи приостановления государственным органом операций Участника, включая отзыв лицензии, или наложения ареста на денежные средства Участника, находящиеся на счете в РЦ;
- 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 том числе в связи с отзывом у Участника необходимых для его деятельности лицензий или иных разрешений либо приостановления их действия, если Участник объявляет о своей ликвидации, либо в отношении него инициирована процедура банкротства.

6.5.2. В случае несоблюдения Участником своих обязательств, условий осуществления расчетов, установленных Правилами, а также в иных случаях, установленных в Правилах, Оператор вправе до дня устранения Участником допущенного нарушения в одностороннем порядке приостановить его участие в Системе, а именно: приостановить возможность совершения Операций Клиентами Участника, а также ограничить в иных правах и не оказывать иные услуги, предусмотренные Правилами и Договором участия. Оператор производит на регулярной основе мониторинг соответствия Участников критериям, установленным пунктом 6.3.1 Правил, и возникновения оснований приостановления и/или прекращения участия в Системе, указанных в пункте 6.5.1. Правил.

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

6.5.4. Оператор не позднее 2 (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), направленному по Согласованным каналам связи.

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

- по заявлению о прекращении участия Участника в Системе, составленному в письменной форме на бумажном носителе, подписанному уполномоченным лицом Участника и скрепленному печатью Участника, поданному Оператору. Со дня получения заявления о прекращении участия Оператор приостанавливает участие Участника в Системе. Оператор предпринимает меры по прекращению обработки ОЦ Операций с использованием ЭСП, выпущенных Участником, в день получения заявления о прекращении участия в Системе. Не позднее, чем на второй рабочий день после получения заявления о прекращении участия, Оператор уведомляет Участника об объеме неисполненных обязательств Участника, связанных с участием в Системе, включая обязательства по осуществлению расчетов по операциям, совершенным Клиентами Участника для целей перевода денежных средств, и оплаты оказанных Участнику услуг. Участник обязан в срок, не превышающий 3 (Трех) рабочих дней, с даты получения уведомления от Оператора осуществить расчеты по всем своим обязательствам, после чего его участие в Системе прекращается, о чем Оператор уведомляет Участника в письменной форме. Оператор вправе направить уведомление, содержащее информацию о дате прекращения участия в Системе как на бумажном носителе, так и в электронном виде (по используемому сторонами при обмене в рамках Системы электронному каналу связи);
- по решению Оператора в случаях, предусмотренных в Правилах. При этом участие Участника приостанавливается, Оператор уведомляет Участника о приостановлении с последующим прекращением участия Участника в Системе, об объеме неисполненных обязательств Участника, связанных с участием в Системе, включая обязательства по осуществлению расчетов по операциям, совершенным Клиентами Участника для целей перевода денежных средств, и оплаты оказанных Участнику услуг. Оператор предпринимает меры по прекращению обработки ОЦ Операций с использованием ЭСП, выпущенных Участником, в день уведомления Участника о приостановлении с последующем прекращением участия в Системе. Участник обязан в срок, не превышающий 3 (Трех) рабочих дней, с даты получения уведомления от Оператора осуществить расчеты по всем своим обязательствам, после чего его участие в Системе прекращается, о чем Оператор уведомляет Участника в письменной форме. Оператор вправе направить уведомление, содержащее информацию о дате прекращения участия в Системе как на бумажном носителе, так и в электронном виде (по используемому сторонами при обмене в рамках Системы электронному каналу связи);
- в случаях, предусмотренных законодательством Российской Федерации, в том числе, когда Участник лишается права осуществлять деятельность по переводу денежных средств, включая отзыв (аннулирование) лицензии на осуществление банковских операций. Со дня, когда Оператору стало известно об указанных обстоятельствах, участие Участника в Системе приостанавливается, Оператор уведомляет Участника о приостановлении с последующим прекращением участия Участника в Системе, об объеме неисполненных обязательств Участника, связанных с участием в Системе, включая обязательства по осуществлению расчетов по операциям, совершенным Клиентами Участника для целей перевода денежных средств, и оплаты оказанных Участнику услуг по всем своим обязательствам, после чего его участие в Системе прекращается. Оператор предпринимает меры по прекращению обработки ОЦ Операций с использованием ЭСП, выпущенных Участником, в день отзыва лицензии. Участник обязан осуществить расчеты по всем своим обязательствам, после чего его участие в Системе прекращается, о чем Оператор уведомляет Участника в письменной форме. Оператор вправе направить уведомление, содержащее информацию о дате прекращения участия в Системе как на бумажном носителе, так и в

электронном виде (по используемому сторонами при обмене в рамках платежной системы электронному каналу связи).

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

6.6. Взаимодействие между Оператором и привлеченными Операторами УПИ

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

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

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

6.6.4. Для обеспечения взаимодействия Оператора и привлеченного Оператора УПИ используют следующие Согласованные каналы связи:

- Официальный сайт Оператора в сети интернет;
- СЭДО;
- электронная почта Оператора: адреса, принадлежащие домену @cpretail.ru или доведенные до привлеченного Оператора УПИ уполномоченными должностными лицами Оператора (информационные рассылки, осуществляемые с таких адресов, являются официальными сообщениями Оператора);
- обмен сообщениями на бумажных носителях, направляемых сторонами друг другу с привлечением организаций почтовой связи, компаний экспресс-доставки документов, курьеров, а также осуществляемый уполномоченными представителями сторон;
- электронная почта привлеченного Оператора УПИ: адреса представителей привлеченного Оператора УПИ, указанные в
  - договоре с Оператором;
  - официальном сообщении привлеченного Оператора УПИ, направленном Оператору на бумажном носителе или на электронный адрес Оператора.

6.6.5. Порядок электронного документооборота между Оператором и привлеченным Оператором УПИ при использовании СЭДО устанавливается Оператором в и доводится до привлеченного Оператора УПИ по Согласованным каналам связи.

6.7. Взаимодействие между Операторами УПИ

6.7.1. Взаимодействие Оператора, выполняющего функции ОЦ и ПКЦ, с РЦ осуществляется в соответствии с Правилами и на условиях договора, заключаемого между Оператором и РЦ.

6.7.2. РЦ в порядке и сроки, установленные Правилами и договором, заключаемым с Оператором, уведомляет Оператора об открытии и закрытии Счетов Участников, передает Оператору сведения об остатках на Счетах Участников и проведенных по Счетам Участников платежах, связанных с осуществлением расчетов по операциям, совершенным в рамках Системы, а также осуществляет иные функции, установленные договором, заключаемым с Оператором.

6.7.3. РЦ обязан принимать и соответствующим образом обрабатывать полученные от Оператора, выполняющего функции ОЦ и ПКЦ, Реестры распоряжений.

6.7.4. Оператор, выполняющий функции ОЦ и ПКЦ, обязан принимать и соответствующим образом обрабатывать полученные от РЦ уведомления и подтверждения исполнения Реестра распоряжений.

6.8. Взаимодействие между РЦ и Участниками

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

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

6.8.3. Списание денежных средств по Счетам Участников осуществляется РЦ на основании полученного от Оператора, выполняющего функции ПКЦ, Реестра распоряжений. При этом получение дополнительного распоряжения Участников на списание денежных средств со Счета Участника не требуется. На основании распоряжений, включенных в Реестр распоряжений, РЦ составляет распоряжения на перевод денежных средств со Счета Участника Получателям. РЦ не несет ответственности за правомерность и содержание распоряжений на перевод денежных средств, включенных в состав Реестра распоряжений, а также указанных в них реквизитов.

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

6.8.5. Средства, поступающие в РЦ в пользу Участника, зачисляются на Счет Участника датой проведения платежа обслуживающим РЦ подразделением расчетной сети Банка России, днем получения РЦ выписок других кредитных организаций либо, в случае отсутствия приложений к выписке, в день поступления этих документов в РЦ.

6.9. Контроль соблюдения Правил

6.9.1. Контроль соблюдения Правил Участниками и привлеченными Операторами УПИ осуществляется Оператором на постоянной основе путем мониторинга деятельности Участников в процессе оказания Услуг Системы, анализа жалоб и обращений Клиентов, а также мониторинга деятельности привлеченных Операторов УПИ, анализа жалоб и обращений Субъектов Системы.

6.9.2. Оператор вправе для целей осуществления контроля за соблюдением Правил обязать Участников (как всех, так и любого в отдельности), привлеченных Операторов УПИ предоставлять отчет о соблюдении ими Правил, о спорных и конфликтных ситуациях между Участником и его Клиентами, связанных с оказанием услуг, предусмотренных Правилами, и иную информацию относительно деятельности в качестве Участника или привлеченного Оператора УПИ. Периодичность предоставления указанного отчета не может быть чаще, чем 1 (Один) раз в месяц.

6.9.3. Оператор регулярно анализирует поступающие жалобы и обращения. По результатам анализа Оператором может быть принято решение о разработке мероприятия по устранению имеющихся некорректных действий, в том числе обращение к Участнику, привлеченному Оператору УПИ в рабочем режиме (в том числе по Согласованным каналам связи), организация встреч с Участником, привлеченными Операторами УПИ, направление им официальных писем, в том числе содержащих требования об уплате неустойки в соответствии с Правилами и/или условиями заключенных договоров.

6.10. Порядок предоставления Участниками и привлеченными Операторами УПИ информации о своей деятельности Оператору

6.10.1. Участники и Операторы УПИ ежегодно, не позднее последнего числа первого месяца календарного года, следующего за отчетным годом, предоставляют Оператору:

6.10.1.1. Перечень средств криптографической защиты информации, применяемых Участниками и Операторами УПИ при осуществлении технологических процедур, выполняемых при оказании услуг по переводу денежных средств и УПИ, соответственно, в рамках Системы по форме, определяемой Оператором.

6.10.1.2. Информацию о своей деятельности в рамках Системы, предусмотренную Правилами, в том числе:

- о результатах оценки соответствия уровням защиты информации, установленным Положением Банка России от 04.06.2020 № 719-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 № 719-П), в соответствии с национальным стандартом Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 28.03.2018 № 156-ст «Об утверждении национального стандарта Российской Федерации» (М., ФГУП «Стандартинформ», 2018);
- о реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств, в том числе о разработанных и реализованных на практике организационных и технических мерах по защите информации при осуществлении переводов денежных средств в рамках Системы с учетом Постановления Правительства Российской Федерации от 13.06.2012 № 584 «Положение о защите информации в платежной системе» (далее – Постановление № 584): перечень мер и перечень локальных нормативных актов Субъекта Системы, регламентирующих порядок реализации мер;
- о результатах проведенных оценок соответствия установленным требованиям, когда в соответствии с Правилами такая оценка должна быть проведена или проводилась по собственной инициативе, в том числе результаты оценки качества функционирования операционных и технологических средств, информационных систем, применяемых Субъектом Системы;
- о выявленных угрозах и уязвимостях в обеспечении защиты информации, предоставляемых в составе сведений о проведении тестирования на

проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры в соответствии с требованиями Положения Банка России № 719-П: период проведения тестирования и анализа, наименование организации, проводившей тестирование и анализ, перечень выявленных угроз и уязвимостей, предпринятые меры.

6.10.1.3. Сводную информацию, направленную Оператору в течение отчетного года, либо подтверждение об отсутствии указанных ниже обстоятельств в отчетном году:

- о событиях, вызвавших спорные, нестандартные, потребовавшие расследования указанных событий и проведения анализа их причин и последствий;
- об инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- о чрезвычайных ситуациях, в том числе, событиях, вызвавших операционные сбои, системные сбои, потребовавшие расследования указанных событий и анализа их причин и последствий;
- о жалобах и обращениях Клиентов Участника (конфликтные ситуации), связанных с операциями по переводу денежных средств в Системе;
- о выявленных случаях нарушения БФПС;
- о случаях неисполнения или ненадлежащего исполнения обязательств Субъектом Системы, предусмотренных Правилами;
- о случаях и (или) попытках осуществления переводов денежных средств без согласия Клиента Участника и компьютерных атак, направленных на объекты информационной инфраструктуры Субъектов Системы и (или) Клиентов Участника, которые могли привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия Клиента Участника.

  Предоставление информации, указанной в настоящем пункте, осуществляется по Согласованным каналам связи.

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

6.10.3. Привлеченные Операторы УПИ информируют Оператора 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, в порядке, установленном для информирования в чрезвычайных ситуациях.

6.10.4. Дополнительно, по запросу Оператора Участники и Операторы УПИ обязаны в срок, не превышающий 5 (Пяти) рабочих дней со дня получения указанного запроса, предоставлять Оператору информацию о своей деятельности, связанной с выполнением возложенных на них функций и обязанностей в рамках Системы, а также в целях анализа Оператором обеспечения защиты информации иные документы и данные об обеспечении в Системе защиты информации при осуществлении переводов денежных средств.

6.11. Порядок изменения Правил

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

6.11.2. Для внесения изменений в Правила Оператор обязан обеспечить Участникам возможность предварительного ознакомления с предлагаемыми изменениями и направления своего мнения Оператору в установленный им срок, который не может быть менее 1 (Одного) месяца. Возможность предварительного ознакомления с предлагаемыми изменениями

обеспечивается путем размещения предлагаемых изменений на Официальном сайте Оператора в сети интернет.

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

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

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

6.11.5. По истечению срока, установленного пунктом 6.11.2. Правил, единоличный исполнительный орган Оператора утверждает новую редакцию Правил с указанием срока начала действия изменений. Изменения в Правила вносятся в срок не менее 1 (Одного) месяца со дня окончания срока, указанного в пункте 6.11.2. Правил.

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

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

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

6.12. Порядок взаимодействия в спорных, чрезвычайных, нестандартных ситуациях, включая случаи системных сбоев

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

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

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

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

6.13. Порядок взаимодействия с иными платежными системами

6.13.1. Оператор вправе заключать с операторами иных платежных систем договоры/соглашения о взаимодействии платежных систем в целях осуществления Межсистемных Операций.

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

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

6.13.4. Перечень платежных систем, с которыми осуществляется взаимодействие на основании заключенных межсистемных договоров (соглашений):

6.13.4.1. Платежная система «Мир», оператор платежной системы Акционерное общество «Национальная система платежных карт», (ОГРН 1147746831352) (далее – НСПК).

6.13.4.2. Порядок взаимодействия платежных систем определяется в договоре о взаимодействии Системы и Платежной системы «Мир» (далее – договор взаимодействия платежных систем):

1) Оператор обеспечивает прием Таможенных Карт «Мир» в Устройствах приема платежей в целях осуществления операции по перечислению Таможенных платежей.
2) Оператор обеспечивает формирование Устройством приема платежей Авторизационного запроса и передачу указанного запроса в НСПК.
3) НСПК обеспечивает обработку Авторизационного запроса в порядке, предусмотренном правилами и стандартами Платежной системы «Мир», и направление ответа на Авторизационный запрос Оператору в порядке, предусмотренном правилами и стандартами Платежной системы «Мир».
4) Оператор обеспечивает формирование и передачу в НСПК реестра операций, совершенных в Устройствах приема платежей, в форме, порядке и сроки, установленные правилами и стандартами Платежной системы «Мир».
5) Платежный клиринг в целях осуществления межсистемных расчетов по Межсистемным Операциям осуществляет НСПК в порядке, предусмотренном правилами и стандартами Платежной системы «Мир».
6) Расчет в целях осуществления межсистемных расчетов по Межсистемным Операциям осуществляет расчетный центр Платежной системы «Мир» - Банк России в порядке, предусмотренном правилами и стандартами Платежной системы «Мир». Расчеты осуществляются в валюте Российской Федерации.
7) Оператор, после поступления на корреспондентский счет РЦ денежных средств от участников Платежной системы «Мир» в счет оплаты по Межсистемным Операциям, обеспечивает перечисление Таможенных платежей в сроки, предусмотренные действующим законодательством Российской Федерации.

6.14. Порядок досудебного разрешения споров между Субъектами Системы

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

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

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

6.14.4. Субъекты Системы, которым было направлено извещение о спорной ситуации, участвующие в разрешении спорной ситуации (далее – ответчики), обязаны не позднее чем в течение следующих 2 (Двух) рабочих дней проверить наличие указанных в извещении обстоятельств, и, при необходимости, принять меры по разрешению спорной ситуации со своей стороны. В тот же срок ответчики извещают доступными способами инициатора о результатах проверки и, при необходимости, о мерах, принятых для разрешения спорной ситуации.

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

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

6.14.7. Если спорная ситуация не была разрешена в рабочем порядке, инициатор должен не позднее чем в течение 3 (Трех) рабочих дней после возникновения спорной ситуации направить уведомление о спорной ситуации (далее - уведомление) и предложение о создании комиссии по разрешению спорной ситуации ответчику и Оператору (если Оператор не является инициатором или ответчиком). Уведомление, подписанное уполномоченным представителем инициатора, направляется по Согласованному каналу связи.

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

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

6.14.9. Оператор не позднее чем в течение 2 (Двух) рабочих дней после получения от инициатора уведомления направляет по Согласованному каналу связи инициатору и ответчику информацию о предлагаемом месте, дате и времени сбора комиссии, список предлагаемых для участия в работе комиссии представителей Оператора с указанием фамилий, имен, отчеств, должностей, их контактной информации (телефон, электронная почта), а также предлагает инициатору и ответчикам не позднее чем в течение 2 (Двух) рабочих после получения указанной информации сообщить список предлагаемых для участия в работе комиссии их представителей с указанием фамилий, имен, отчеств, должностей, их контактной информации (телефон, электронная почта).

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

6.14.10. Если стороны не договорятся об ином, в состав комиссии входит по 3 (Три) уполномоченных лица Оператора, инициатора и каждого из ответчиков, участвующих в разрешении спорной ситуации в соответствии с полученными и направленными списками представителей инициатора, ответчиков и Оператора.

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

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

Комиссия рассматривает спорную ситуацию и выносит решение в течении 30 (Тридцати) календарных дней. В исключительных случаях срок работы комиссии по решению членов комиссии может быть дополнительно продлен не более чем на 30 (Тридцать) календарных дней. Любой из членов комиссии вправе выступить с инициативой о привлечении для проведения технической экспертизы независимого эксперта. Решение о привлечении независимого эксперта комиссия принимает простым большинством голосов, при этом сторона, чей представитель выступил с инициативой привлечения независимого эксперта, самостоятельно решает вопрос об оплате экспертных услуг.

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

- состав комиссии с указанием сведений о фамилиях, именах, отчествах, местах работы, занимаемых должностях, контактной информации каждого из членов комиссии;
- краткое изложение обстоятельств, свидетельствующих, по мнению инициатора, о возникновении и/или наличии спорной ситуации;
- установленные комиссией фактические обстоятельства;
- мероприятия, проведенные комиссией для установления наличия, причин возникновения и последствий возникшей спорной ситуации, с указанием даты времени и места их проведения;
- выводы, к которым пришла комиссия в результате проведенных мероприятий;
- подписи всех членов комиссии.

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

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

6.14.13. По итогам работы комиссии составляется акт, при этом акт должен содержать следующую информацию:

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

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

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

6.14.14. В срок не более 3 (Трех) рабочих дней со дня окончания работы комиссии, стороны на основании выводов комиссии принимают меры по разрешению спорной ситуации и извещают другие заинтересованные стороны о принятых мерах.

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

В случае, если спорная ситуация признается сторонами разрешенной, то в срок не позднее 5 (Пяти) рабочих дней со дня окончания работы комиссии стороны оформляют решение об урегулировании спорной ситуации.

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

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

Претензия должна содержать:

- изложение существа требований инициатора;
- при возможности денежной оценки претензии - ее сумму и расчет;
- изложение фактических обстоятельств, на которых основываются требования инициатора и доказательства, подтверждающие их, со ссылкой на соответствующие нормы законодательства Российской Федерации и нормативных правовых актов, а также Правил;
- сведения о работе комиссии и, в случае если комиссия работала в связи с рассматриваемой спорной ситуацией, копии материалов работы комиссии, независимо от выводов комиссии, согласия или несогласия с этими выводами инициатора;
- иные документы, имеющие значение, по мнению инициатора;
- перечень прилагаемых к претензии документов и других доказательств, а также иные сведения, необходимые для урегулирования разногласий по претензии.

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

Ответчик, в адрес которого направлена претензия, обязан в срок не позднее 5 (Пяти) рабочих дней удовлетворить требования претензии или представить инициатору мотивированный отказ в их удовлетворении, одновременно направив копию отказа Оператору. Непредставление ответа на претензию в течение указанного срока является нарушением установленного Правилами претензионного порядка и может рассматриваться в качестве отказа в удовлетворении требований претензии.

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

6.15. Ответственность за несоблюдение Правил

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

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

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

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

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

6.15.4. Субъекты Системы освобождаются от ответственности за неисполнение или ненадлежащее исполнение своих обязательств, если оно явилось следствием непреодолимой силы при условии, что эти обстоятельства непосредственно повлияли на исполнение обязательств.

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

Субъект Системы, подвергшийся действию обстоятельств непреодолимой силы и оказавшийся вследствие этого не в состоянии выполнить свои обязательства, должен сообщить об этом Оператору в течение 1 (Одного) рабочего дня с момента возникновения указанных обстоятельств в устной форме и в течение 3 (Трех) рабочих дней в письменной форме. В противном случае Субъект Системы, нарушивший обязательство, не вправе ссылаться на обстоятельства непреодолимой силы. Уведомление должно содержать данные о характере обстоятельств, оценку их влияния на возможность исполнения своих обязательств и срок исполнения обязательств с приложением подтверждения официальных органов о действии обстоятельств непреодолимой силы.

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

7.1. Общий порядок осуществления перевода денежных средств в Системе и применяемые формы безналичных расчетов

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

7.1.2. Перевод денежных средств осуществляется со Счета Участника на основании Реестра распоряжений, поступающего в РЦ в электронном виде (по Ссогласованным каналам связи, на отчуждаемых машинных носителях информации) или на бумажном носителе.

7.1.3. На основании Реестра распоряжений, переданного РЦ Оператором, выполняющим функции ПКЦ, в случаях и в порядке, предусмотренных Правилами, РЦ составляет распоряжения и осуществляет перевод денежных средств со Счета Участника Получателю средств.

7.1.4. Перевод денежных средств в Системе осуществляется в рамках следующих форм безналичных расчетов: расчеты платежными поручениями.

7.1.5. Участники осуществляют перевод денежных средств по операциям, инициированным Пользователем ЭСП в Устройствах приема платежей.

7.1.6. В целях обеспечения исполнения обязательств Участников Операции в рамках Системы осуществляются исходя из Предельного размера (лимита) обязательств, который контролируется и изменяется Оператором, выполняющим функции ПКЦ. При приеме распоряжений Участников в соответствии с порядком, установленным Правилами, доступный Предельный размер (лимит) обязательств соответствующего Участника уменьшается на сумму Операций, инициированных Клиентами Участника и комиссий, подлежащих уплате в соответствии с Тарифами.

7.1.7. По завершении Операции с использованием ЭСП составляется документ в электронной форме. Документ по Операции является основанием для осуществления расчетов по указанной Операции и (или) служит подтверждением ее совершения.

7.1.8. Переводы денежных средств в Системе с использованием ЭСП через Устройства приема платежей в целях осуществления Таможенных платежей осуществляются в следующем порядке:

- уполномоченное лицо Клиента Участника (в случае, если Клиент – юридическое лицо) или Клиент Участника (в случае, если Клиент – физическое лицо), являющееся Пользователем ЭСП, инициирует Операцию с использованием Устройства приема платежей;
- на основании инициированной Операции Устройством приема платежей формируется и передается Оператору, выполняющему функции ОЦ, Авторизационный запрос на разрешение проведения Операции;
- Оператор, выполняющий функции ОЦ, обрабатывает запрос на разрешение проведения Операции, в том числе определяет Участника, эмитировавшего ЭСП и его Клиента, инициировавшего Операцию;
- Оператор, выполняющий функции ПКЦ, осуществляет процедуры платежного клиринга, в том числе проводит проверку достаточности лимитов;
- в случае если Предельный размер (лимит) обязательств Участника, а также Лимит ЭСП, являются достаточными для совершения Операции, Оператор, выполняющий функции ПКЦ, в зависимости от вида Устройства приема платежей либо подтверждает осуществление инициированной Пользователем ЭСП Операции, либо формирует положительный ответ на запрос и уменьшает доступный Лимит ЭСП и доступный Предельный размер (лимит) обязательств Участника на сумму Операции, в противном случае формируется отказ в проведении Операции;
- расчет размера и проверка достаточности Лимита ЭСП и Предельного размера (лимита) обязательств Участника осуществляется в порядке, определенном Правилами;
- в случае, если Устройством приема платежей предусмотрено получение предварительного ответа на запрос проведения Операции после получения

положительного ответа на запрос Пользователь ЭСП подтверждает намерение совершить Операцию и совершает действия, направленные на завершение Операции с использованием Устройства приема платежей, направляющего сообщение Оператору, выполняющему функции ОЦ, о положительном завершении Операции;

- по результатам положительного завершения Операции Пользователю ЭСП Устройством приема платежей формируется документ в электронном виде, подтверждающий осуществление Операции, что определяет момент наступления безусловности и безотзывности перевода денежных средств;
- по итогам операционного дня Оператор обрабатывает информацию об Операциях, совершенных Плательщиками, в течение операционного дня, формирует в порядке, определенном Правилами, реестры ПКЦ для Участников и Реестр распоряжений для списания денежных средств со Счетов Участников;
- на основании Реестра распоряжений РЦ осуществляет списание денежных средств со Счетов Участников в пользу Получателей.

7.2. Порядок осуществления платежного клиринга и расчетов в Системе

7.2.1. Платежный клиринг в Системе осуществляется Оператором, выполняющим функции ПКЦ, посредством:

- выполнения процедур приема к исполнению распоряжений Участников, включая проверку соответствия распоряжений Участников установленным требованиям, определение достаточности денежных средств для исполнения распоряжений;
- определения размера платежных клиринговых позиций;
- направления Участникам отчетов об Операциях, совершенных Клиентами Участника в целях перевода денежных средств в течение операционного дня, расчеты по которым осуществляются на основании распоряжений и за счет Участника;
- передачи РЦ для исполнения принятых распоряжений Участников в виде Реестра распоряжений;
- направления Участникам извещений (подтверждений), касающихся приема к исполнению распоряжений Участников, а также передачи извещений (подтверждений), касающихся исполнения распоряжений Участников.

7.2.2. Процедуры приема к исполнению распоряжений Участников включает:

- удостоверение права Плательщика распоряжаться денежными средствами;
- удостоверение права Участника распоряжаться денежными средствами;
- контроль целостности распоряжения;
- контроль структуры распоряжения;
- контроль полноты реквизитов распоряжения;
- контроль достаточности денежных средств Плательщика (Лимитов ЭСП) для исполнения распоряжения;
- контроль достаточности денежных средств на Счете Участника (Предельного размера (лимита) обязательств Участника) для исполнения распоряжения.

7.2.3. При положительном результате процедур приема распоряжения Плательщика, Оператор, выполняющий функции ПКЦ, принимает к исполнению распоряжение Участника и направляет Участнику по Согласованному каналу связи Реестр ПКЦ, который содержит расшифровку каждой Операции, вошедшей в платежную клиринговую позицию соответствующего Участника, и является подтверждением приема к исполнению распоряжения.

7.2.4. Определение платежной клиринговой позиции Участника осуществляется на валовой основе. Платежная клиринговая позиция определяется в размере суммы операций,

совершенных Клиентами Участника, расчеты по которым осуществляются за счет Участника, на основании информации об указанных Операциях, полученной за операционный день Оператором, выполняющим функции ОЦ и ПКЦ, с Устройств приема платежей и зафиксированной в отчетах, передаваемых Оператором Участнику (Реестры ПКЦ). Указанная информация является основанием для передачи Оператором, выполняющим функции ОЦ и ПКЦ, РЦ от имени Участника подлежащих исполнению распоряжений о списании денежных средств со Счета Участника.

7.2.5. После определения платежной клиринговой позиции Оператор, выполняющий функции ПКЦ, формирует Реестры ПКЦ для Участников и Реестр распоряжений для РЦ, и направляет сформированные реестры адресатам по согласованным каналам связи.

7.2.6. Реестр распоряжений может быть сформирован и направлен в РЦ до окончания операционного дня в рамках процедур управления рисками в Системе в случае приостановления или прекращения участия Участника в Системе. В случае направления Реестра распоряжений в связи с приостановлением или прекращением участия Участника в Системе, Реестр распоряжений формируется на основании полученной с начала операционного дня и до момента приостановления участия информации, указанной в пункте 7.2.4. Правил, и/или содержит сведения о комиссиях за услуги, оказанные Участнику за период с начала календарного месяца оказания услуг по дату приостановления или прекращения участия в Системе.

7.2.7. Операции Участников за операционные дни, соответствующие выходным и праздничным дням, включаются в Реестры ПКЦ, направляемые Участникам до 12:00 часов по московскому времени первого рабочего дня, следующего за ними.

7.2.8. Форматы Реестра ПКЦ, Реестра распоряжений, используемых в Системе, размещаются на Официальном сайте Оператора в сети интернет в доступном Участникам специальном разделе.

7.2.9. Расчеты в Системе по Операциям, совершенным Клиентом Участника в целях перевода денежных средств с использованием ЭСП, эмитированных Участником, являющимися обязательствами Участника, осуществляются со Счета Участника.

7.2.10. Расчеты осуществляются РЦ посредством списания (без дополнительного распоряжения Участника) денежных средств со Счета Участника на основании поступившего от Оператора, выполняющего функции ПКЦ, Реестра распоряжений в размере сумм определенных платежных клиринговых позиций.

7.2.11. РЦ обеспечивает направление извещений (подтверждений), касающихся исполнения распоряжений Участников, включенных в Реестр распоряжений.

7.2.12. Участник обязан до 15:00 часов по московскому времени рабочего дня, следующего за днем совершения Клиентами Участника операций по переводу денежных средств, обеспечить поступление денежных средств на Счет Участника в размере, достаточном для осуществления расчетов по Операциям, принятым к исполнению Оператором, выполняющим функции ОЦ и ПКЦ.

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

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

- предоставлением РЦ Оператору, выполняющему функции ОЦ и ПКЦ, данных об остатках денежных средств на Счетах Участников для осуществления контроля за рисками неисполнения (ненадлежащего исполнения) Участниками обязательств по переводу денежных средств;
- обязательствами РЦ осуществлять расчетные услуги в порядке, установленном Правилами, а также Договором счета, заключенным между РЦ и соответствующим Участником;

- осуществлением расчетов со Счета Участника;
- совершением Операций с использованием Устройств приема платежей только в случае получения в режиме реального времени сведений о достаточности Предельного размера (лимита) обязательств Участника и Лимита ЭСП (Лимит по Банковской карте) его Клиента.

7.2.15. Направление Участникам отчетов об операциях, совершенных Клиентами в целях перевода денежных средств в течение операционного дня, расчеты по которым осуществляются за счет Участника, осуществляется Оператором, выполняющим функции ПКЦ, в порядке и сроки, определенные в Порядке эмиссии и обслуживания банковских карт, размещенном на официальном сайте оператора платежной системы в сети интернет.

7.3. Временной регламент функционирования Системы

7.3.1. В качестве единой шкалы времени признается московское время. Контрольным является время системных часов аппаратных средств ОЦ.

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

7.3.3. Система функционирует круглосуточно без выходных и праздничных дней, за исключением времени, необходимого для осуществления технических, профилактических, ремонтных работ, а также работ, вызванных необходимостью устранения чрезвычайных обстоятельств, повлиявших на работоспособность Системы. В случае разового изменения времени операционного дня Оператор, выполняющий функции ОЦ и ПКЦ, доводит соответствующую информацию по Согласованным каналам связи до Участников.

7.3.4. Допускается отклонение в пределах 30 (Тридцати) минут от времени завершения (закрытия) операционного дня. В указанном случае, время начала (открытия) следующего операционного дня сдвигается на величину отклонения времени закрытия предыдущего операционного дня в соответствующую сторону. Отклонение времени начала и/или завершения операционного дня в пределах установленного значения является нормальным, не требует специального уведомления Участников.

7.3.5. О проведении плановых технических, профилактических и ремонтных работ Оператор, уведомляет Участников и привлеченных Операторов УПИ заранее, не позднее, чем за 1 (Один) рабочий день до даты начала проведения работ, путем информирования по Согласованным каналам связи или путем опубликования на Официальном сайте Оператора в сети интернет. В уведомлении указываются дата и время начала проведения работ, дата и время окончания проведения работ.

7.3.6. О проведении внеплановых ремонтных работ, а также работ, вызванных необходимостью устранения чрезвычайных обстоятельств, повлиявших на работоспособность Системы, Оператор уведомляет Участников и привлеченных Операторов УПИ не позднее 1 (Одного) рабочего дня с даты начала проведения работ, путем информирования по Согласованным каналам связи или путем опубликования на Официальном сайте Оператора в сети интернет. В уведомлении указываются предполагаемые дата и время окончания проведения работ.

7.4. Регламент выполнения процедур в Системе

7.4.1. Время приема распоряжений представлено в Таблице №1, регламентное время обработки распоряжений и проведения расчетов представлены в Таблице №2.

Время приёма к исполнению распоряжений Участников

Таблица №1

Процедура	Время (по московскому времени)
Прием к исполнению распоряжений на перевод денежных средств (операционные услуги, услуги платежного клиринга)	Круглосуточно (24/7)

Регламент обработки распоряжений и осуществления расчетов

Таблица №2

Процедура	Время (по московскому времени)
Обработка ОЦ запроса на разрешение проведения Операции (операционные услуги)	Не более 30 секунд
Формирование и направление ПКЦ Участникам отчетов об Операциях, совершенных Клиентами Участников в целях перевода денежных средств в течение операционного дня, расчеты по которым осуществляются за счет Участника (Реестры ПКЦ) (услуги платежного клиринга)	до 12:00 часов рабочего дня, следующего за операционным днем совершения Операций с использованием ЭСП
Расчет платежной клиринговой позиции, формирование и направление ПКЦ в РЦ Реестра распоряжений за операционный день (услуги платежного клиринга)	до 19:00 часов рабочего дня, следующего за операционным днем совершения Операций с использованием ЭСП
Осуществление РЦ списания денежных средств со Счетов Участников (расчетные услуги)	с момента получения Реестра распоряжений до 24:00 часов дня получения Реестра распоряжений в случае его поступления до 15:00 часов, либо не позднее 24:00 часов следующего за днем получения Реестра распоряжений рабочего дня, в случае поступления Реестра распоряжений после 15:00 часов
Пополнение Участниками Счетов Участников в РЦ	до 15:00 часов рабочего дня, следующего за операционным днем совершения Операций с использованием ЭСП (день получения Реестра ПКЦ)

7.5. Моменты наступления безотзывности, безусловности и окончательности перевода денежных средств

7.5.1. При переводе денежных средств в Системе с использованием ЭСП момент наступления безусловности и безотзывности перевода денежных средств наступает при формировании Устройством приема платежей документа в электронном виде, подтверждающего осуществление Операции.

7.5.2. Списание РЦ денежных средств со Счетов Участников в пользу Получателей по Операциям определяет момент наступления окончательности переводов денежных средств, совершенных в рамках Системы.

7.5.3. Возврат ошибочно уплаченных денежных средств осуществляется в Системе в порядке, предусмотренном законодательством Российской Федерации.

7.6. Порядок сопровождения перевода денежных средств сведениями о Плательщике

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

7.6.2. Участники самостоятельно несут ответственность за реализацию комплекса мер, направленных на предотвращение легализации (отмывания) доходов, полученных

преступным путем, финансирования терроризма и финансирования распространения оружия массового уничтожения.

7.6.3. Участник, у которого открыт банковский счет Плательщика:

- обязан обеспечить контроль за наличием, полноту, передачу Оператору, выполняющему функции ОЦ и ПКЦ, в составе расчетных документов или иным способом, а также хранение информации, предусмотренной законодательством Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения;
- несет ответственность за достоверность и полноту сведений о Плательщике, передаваемых Оператору.

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

7.6.5. В случае, если в распоряжении Участника не содержатся сведения о Плательщике в соответствии с требованиями законодательства Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения, Оператор, выполняя функции ПКЦ, имеет право отказать в приеме к исполнению распоряжения Участника.

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

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

8. Порядок оплаты Услуг Системы

8.1. Тарифы на оплату Услуг Системы и порядок оплаты являются едиными для всех Участников.

8.2. Участники оплачивают Услуги Системы в размере, предусмотренном в Тарифах. Дополнительно к сумме вознаграждения, указанного в Тарифах, уплачивается НДС в установленном законодательством Российской Федерации размере, в случае если оказание услуги является объектом налогообложения НДС.

8.3. Оплата Конфигурации Участника осуществляется Участником в соответствии с Тарифами после подписания им Договора участия в течение 5 (Пяти) рабочих дней с даты получения Участником соответствующего счета на оплату, выставляемого Оператором.

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

8.5. Оператор имеет право вносить изменения в порядок оплаты услуг и Тарифы в порядке, предусмотренном для внесения изменений в Правила. При внесении изменений, предусматривающих введение новых Тарифов или увеличение размера Тарифов, Оператор обязан уведомить об этом Банк России с соблюдением срока, установленного Законом о НПС.

8.6. Оплата предоставленных Участнику услуг, указанных в Тарифах, осуществляется не позднее 5 (Пятого) рабочего дня месяца, следующего за месяцем оказания услуг, путем перевода РЦ денежных средств в сумме стоимости оказанных Участнику услуг со Счета Участника, на счет Оператора на основании распоряжения, передаваемого в РЦ Оператором, выполняющим функции ПКЦ, на что Участник дает свое безусловное согласие. Получение дополнительного распоряжения Участника на осуществление указанного перевода денежных средств не требуется. Расчетный месяц оказания услуг устанавливается с начала операционного дня в Системе, соответствующего первому календарному дню месяца и заканчивается с окончанием операционного дня в Системе, соответствующего последнему календарному дню месяца.

8.7. Для осуществления расчетов за оказанные услуги в установленные в пунктах 8.3 и 8.6 Правил сроки Участник обязан обеспечить на своем Счете Участника достаточность денежных средств, доступных для целей расчетов за оказанные услуги.

8.8. Расшифровка сумм, списанных со Счета Участника в качестве оплаты стоимости оказанных Участнику услуг, приводится в акте об объеме предоставленных услуг, который предоставляется Оператором Участнику в срок не позднее 5 (Пятого) рабочего дня месяца, следующего за месяцем оказания услуг.

9. Система управления рисками в Системе

9.1. Общие положения

9.1.1. Оператор совместно с Операторами УПИ и Участниками организует систему управления рисками в Системе.

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

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

Порядок обеспечения БФПС определен в Правилах.

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

- управление рисками в Системе;

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

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

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

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

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

9.2. Организационная модель управления рисками

9.2.1. Оператор самостоятельно управляет рисками в Системе. Модель управления рисками выбирается с учетом выполнения Оператором функций ОЦ и ПКЦ, и представляет собой централизованную систему управления рисками, в которой Оператор самостоятельно определяет виды рисков, способы их мониторинга, анализа, оценки и управления.

9.2.2. Привлеченные Операторы УПИ и Участники в целях обеспечения БФПС осуществляют мониторинг рисков и обеспечивают реализацию определенных Оператором мер по управлению рисками, присущими их виду деятельности, в рамках внутренних систем управления рисками и несут ответственность за оперативное информирование Оператора о реализации указанных рисков и их последствиях, оказывающих непосредственное влияние на функционирование Системы.

9.2.3. В целях управления рисками Оператор обладает следующими полномочиями:

- разрабатывать методики анализа рисков в Системе, включая профили рисков;
- составлять профили рисков, присущих деятельности Системы, включая риск нарушения БФПС;
- осуществлять мониторинг, анализ, оценку и управление рисками в Системе;
- устанавливать уровни оказания УПИ и определять показатели БФПС;
- определять мероприятия по управлению рисками нарушения БФПС в Системе;
- определять и внедрять способы управления рисками в Системе;
- определять меры, направленные на предупреждение и минимизацию риска нарушения БФПС;
- устанавливать допустимый уровень риска нарушения БФПС;
- принимать меры, необходимые для достижения или поддержания допустимого уровня рисков, включая риск нарушения БФПС;
- утверждать комплекс мероприятий для кризисных ситуаций, в случае длительного нахождения Системы под влиянием какого-либо риска;
- принимать решения в области управления рисками в Системе;
- определять требования в части бесперебойности оказания им УПИ Участникам и обеспечивать контроль за исполнением указанных требований;

- вносить изменения в систему управления рисками в Системе в случае, если действующая система управления рисками в Системе не позволила предотвратить нарушение оказания УПИ, соответствующего требованиям к оказанию услуг;
- восстановить оказание УПИ, соответствующее требованиям к оказанию услуг, и (или) восстановить оказание УПИ в случае приостановления их оказания в течение периодов времени, установленных в Правилах;
- организовывать взаимодействие Субъектов Системы в целях управления рисками;
- осуществлять контроль за выполнением Субъектами Системы требований к управлению рисками, присущими их деятельности и оказывающими влияние на БФПС;
- осуществлять контроль за выполнением Субъектами Системы требований по обеспечению бесперебойности оказания услуг;
- определять соответствие действий, осуществляемых Субъектами Системы в рамках Системы, требованиям Правил;
- приостанавливать в одностороннем порядке участие Участника в Системе до устранения допущенного участником нарушения;
- приостанавливать в одностороннем порядке участие Участника в Системе, если имеющиеся в распоряжении Оператора сведения позволяют сделать вывод о высокой вероятности возникновения рисков, ведущих к невозможности осуществления расчетов по Операциям, совершенным Плательщиками для целей перевода денежных средств, в том числе неисполнения обязанности по обеспечению достаточности денежных средств на Счете Участника в сроки и порядке, установленные Правилами;
- лишать организацию статуса Участника;
- осуществлять иные меры, установленные Правилами для обеспечения Оператором управления рисками, возникающими в деятельности Системы.

9.2.4. В обязанности РЦ в части управления рисками входят следующие:
- создание внутренней системы управления рисками, присущими деятельности Субъекта Системы, включая риск нарушения БФПС;
- соблюдение регламента выполнения процедур;
- соблюдение уровней оказания УПИ;
- осуществление анализа и оценки рисков, присущих деятельности Субъекта Системы;
- осуществление мониторинга рисков и уведомление Оператора о реализации рисков, оказывающих влияние на БФПС;
- принятие мер, направленных на предупреждение и минимизацию рисков, присущих деятельности Субъекта Системы;
- поддержание ликвидности в объемах, необходимых для обеспечения обязательств по переводу денежных средств;
- поддержание работоспособности операционных и технологических средств, информационных систем, обеспечивающих проведение переводов денежных средств в Системе;
- обеспечение информационного взаимодействия с Оператором, согласно порядку, установленному Правилами;
- обеспечение взаимодействия с Оператором при реализации мероприятий по управлению рисками;
- соблюдение продолжительности временных периодов, в течение которых должно быть восстановлено надлежащее функционирование Системы в случае его нарушения, в том числе в случае приостановления (прекращения) оказания УПИ.

9.2.5. В обязанности Участников в части управления рисками входят следующие:

- создание внутренней системы управления рисками, присущими деятельности Субъекта Системы, включая риск нарушения БФПС;
- соблюдение регламента выполнения процедур;
- осуществление анализа и оценки рисков, присущих деятельности Субъекта Системы;
- осуществление мониторинга рисков и уведомление Оператора о реализации рисков, оказывающих влияние на БФПС;
- принятие мер, направленных на предупреждение и минимизацию рисков, присущих деятельности Субъекта Системы;
- поддержание на Счете Участника остатка денежных средств, достаточного для своевременного выполнения своих обязательств;
- поддержание работоспособности операционных и технологических средств, информационных систем, обеспечивающих проведение переводов денежных средств в Системе;
- обеспечение информационного взаимодействия с Оператором, согласно порядку, установленному Правилами;
- обеспечение взаимодействия с Оператором при реализации мероприятий по управлению рисками.

9.3. Мероприятия по управлению рисками

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

- организационной структуры управления рисками, обеспечивающей контроль за выполнением Субъектами Системы требований к управлению рисками, установленных Правилами;
- функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений Оператора;
- порядка доведения до органов управления Оператора соответствующей информации о рисках;
- показателей бесперебойности функционирования Системы (далее - показатели БФПС) и значений их пороговых уровней;
- порядка обеспечения БФПС;
- методик анализа рисков в Системе, включая определение профилей рисков, а также способы управления рисками;
- порядка обмена информацией между Субъектами Системы, необходимой для управления рисками;
- порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев;
- уровней оказания УПИ, характеризующих качество функционирования операционных и технологических средств платежной инфраструктуры (далее – уровни оказания УПИ);
- 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.

9.4. Организационная структура системы управления рисками

9.4.1. Оператор определяет собственную структуру управления рисками и функциональные обязанности лиц в соответствующих структурных подразделениях, ответственных за управление рисками в Системе. Структура управления рисками в Системе

обеспечивает контроль за выполнением Участниками и Операторами УПИ требований к управлению рисками, установленных Правилами.

9.4.2. Организационная структура управления рисками включает:

- единоличный исполнительный орган Оператора;
- структурное подразделение (работник) Оператора, ответственное (ответственный) за управление рисками, присущими деятельности Системы.
- структурное подразделение (работник) Оператора, ответственное (ответственного) за организацию и контроль обеспечения защиты информации.

9.4.3. Функциональные обязанности и компетенция единоличного исполнительного органа Оператора включают, в том числе, следующие:

- утверждение Стандартов Системы;
- утверждение Правил, включая систему управления рисками в Системе, порядок обеспечения БФПС, взаимодействия ОЦ, ПКЦ и Участников, ОЦ, ПКЦ и РЦ, внутренних документов, регулирующих систему управления рисками, и Плана ОНиВД;
- обеспечение условий для эффективной реализации политики в сфере управления рисками;
- определение структурного подразделения (работника) Оператора, ответственного за управление рисками, присущими деятельности Системы;
- определение структурного подразделения (работника) Оператора, ответственного за организацию и контроль обеспечения защиты информации;
- утверждение комплекса мероприятий для кризисных ситуаций, в случае нахождения Системы под влиянием какого-либо риска;
- принятие организационных решений по вопросам управления рисками в Системе;
- утверждение критериев оценки системы управления рисками, в том числе используемых методов оценки рисков;
- утверждение профилей рисков, присущих деятельности Системы;
- утверждение допустимых уровней рисков, присущих деятельности Системы;
- принятие мер по обеспечению БФПС и минимизации уровня рисков;
- установление предельных размеров (лимитов) суммы превышения остатка на Счете Участника, определяемой для установления Предельного размера (лимита) обязательств Участников с учетом уровня риска;
- контроль за выполнением мероприятий по управлению рисками;
- рассмотрение отчетов о состоянии рисков, присущих деятельности Системы, и системы управления рисками в целом;
- утверждение отчета об оценке системы управления рисками в Системе, в том числе, используемых методов оценки рисков в Системе, результатов применения способов управления рисками в Системе;
- внесение изменений, совершенствование системы управления рисками в Системе;
- иные функции, установленные законодательством Российской Федерации, нормативными актами Банка России и Правилами.

9.4.4. Функциональные обязанности структурного подразделения (работника) Оператора, ответственного за управление рисками, присущими деятельности Системы включают, в том числе, следующие:

- контроль за выполнением Субъектами Системы требований к управлению рисками, установленных Правилами;
- разработка внутренних документов, регулирующих систему управления рисками в Системе и порядка обеспечения БФПС;

- сбор, документирование и статистическая обработка информации о функционировании Системы;
- сбор и документирование сведений об инцидентах;
- анализ информации о функционировании Системы;
- анализ показателей уровней оказания УПИ;
- анализ сведений об инцидентах, в целях определения их влияния на БФПС;
- анализ нестандартных ситуаций с целью выявления возможных дополнительных рисков в Системе;
- расчет, анализ и мониторинг показателей БФПС;
- проведение мониторинга и оценки рисков, присущих деятельности Системы, включая системный риск (риск нарушения БФПС);
- проведение оценки рисков в Системе с использованием методик анализа рисков в Системе, включая профили рисков;
- проведение оценки системы управления рисками в Системе, в том числе, используемых методов оценки рисков в Системе, результатов применения способов управления рисками в Системе и документальное оформление результатов указанной оценки;
- разработка мер по минимизации рисков в Системе;
- информирование единоличного исполнительного органа Оператора о выявлении факторов, указывающих на реализацию риска нарушения БФПС;
- информирование единоличного исполнительного органа Оператора о состоянии рисков;
- контроль актуальности состояния перечней бизнес-процессов;
- контроль актуальности состояния классификаторов (структурированных перечней) рисков в Системе, событий, реализация которых может привести к возникновению инцидентов (далее – риск-событие), причин риск-событий;
- вынесение на рассмотрение единоличным исполнительным органом Оператора предложений по предупреждению возникновения, устранению и минимизации риск-событий, могущих повлечь реализацию риска нарушения БФПС;
- анализ подверженности рискам бизнес-процессов Системы - взаимосвязанных, последовательных технологических процедур, выполняемых при оказании УПИ (далее тексту – бизнес-процесс);
- составление и пересмотр (актуализация) профилей рисков, присущих деятельности Системы;
- разработка и вынесение на обсуждение единоличным исполнительным органом Оператора мер, необходимых для достижения допустимых уровней рисков, включая риск нарушения БФПС;
- расчет суммы превышения остатка на Счете Участника, определяемой для установления Предельного размера (лимита) обязательств Участника, с учетом уровня рисков;
- участие в разработке новых продуктов, внедрении новых технологий, освоении новых направлений деятельности с целью своевременного отслеживания возникновения рисков на стадии внедрения и принятия мер по их минимизации;
- инициирование внесения изменений в систему параметров, на основании которых производится оценка функционирования Системы;
- организация обмена информацией о рисках и мерах по управлению ими между структурными подразделениями Оператора, Участниками и привлеченными Операторами УПИ;
- иные функции, установленные законодательством Российской Федерации, нормативными актами Банка России и Правилами.

9.4.5. Функциональные обязанности структурного подразделения (работника) Оператора, ответственного за организацию и контроль обеспечения защиты информации:

- осуществление мониторинга и учета событий информационной безопасности;
- повышение осведомленности работников Оператора, выполняющего функции Операционного центра и Платежного клирингового центра, в области обеспечения защиты информации;
- выявление риск информационной безопасности в Системе;
- проведение анализа и оценка риска информационной безопасности;
- организация реагирования на Инциденты защиты информации и организация восстановления штатного функционирования объектов информационной инфраструктуры Оператора, выполняющего функции Операционного центра и Платежного клирингового центра, в случае реализации Инцидентов защиты информации;
- осуществление обмена информацией об Инцидентах защиты информации с привлеченными Операторами УПИ и Участниками;
- участие в противодействии осуществлению в рамках Системы переводов денежных средств без согласия Клиента Участника (Участника).

9.4.6. Участники и привлеченные Операторы УПИ определяют должностных лиц и/или структурные подразделения, к обязанностям которых относится обеспечение мониторинга и проведение мероприятий, связанных с управлением рисками, присущими их деятельности.

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

9.4.8. Информационная система состояния рисков в Системе базируется на:

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

9.5. Виды рисков, присущих деятельности Системы

9.5.1. Деятельности Системы присущи следующие виды рисков:

- **правовой риск** – риск нарушения БФПС и ненадлежащего оказания УПИ вследствие несоблюдения Субъектами Системы требований законодательства Российской Федерации, Правил, договоров, заключенных между Субъектами Системы, внутренних нормативных документов Оператора и внутренних нормативных документов привлеченных Операторов УПИ либо вследствие наличия правовых коллизий и (или) правовой неопределенности в законодательстве Российской Федерации, нормативных актах Банка России, Правилах и договорах, заключенных между Субъектами Системы, а также вследствие нахождения привлеченных Операторов УПИ и Участников под юрисдикцией различных государств;
- **операционный риск, одним из видов которого является риск информационной безопасности** – риск нарушения БФПС и ненадлежащего оказания УПИ вследствие возникновения у Субъектов Системы сбоев, отказов и аварий в работе информационных и технологических систем, недостатков в организации и выполнении технологических и управленческих процессов, ошибок или противоправных действий персонала Субъектов Системы либо

вследствие воздействия событий, причины возникновения которых не связаны с деятельностью Субъектов Системы, включая чрезвычайные ситуации, ошибочные или противоправные действия третьих лиц;

- **кредитный риск** – риск нарушения БФПС и риск ненадлежащего оказания УПИ РЦ вследствие невыполнения Участником или Участниками договорных обязательств перед РЦ в установленный срок или в будущем;
- **риск ликвидности** – риск нарушения БФПС и ненадлежащего оказания УПИ вследствие отсутствия у Участников денежных средств, достаточных для своевременного выполнения их обязательств перед другими Субъектами Системы;
- **общий коммерческий риск** – риск нарушения БФПС и ненадлежащего оказания УПИ вследствие уменьшения доходов и (или) увеличения расходов, ухудшения финансового состояния Оператора и (или) привлеченных Операторов УПИ, не связанного с реализацией кредитного риска Системы и риска ликвидности Системы;
- **риск нарушения БФПС (системный риск)** – риск приостановления (прекращения) осуществления переводов денежных средств или надлежащего функционирования Системы, а также невозможность восстановления оказания УПИ, соответствующего требованиям к оказанию услуг, и восстановления оказания УПИ в случае приостановления их оказания в течение периодов времени, установленных Оператором в Правилах, вследствие неблагоприятного стечения обстоятельств – возникновения инцидентов в деятельности Субъектов Системы.

9.6. Способы управления рисками

9.6.1. 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, вида количества переводов денежных средств и их сумм, времени окончательного расчета.

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

9.6.3. Система управления рисками предусматривает следующие способы управления рисками:

- использование безотзывных банковских гарантий, обеспечивающих своевременное и полное исполнение обязательств по переводу денежных средств Получателю;
- осуществление расчета в пределах, предоставленных Участником денежных средств (в пределах остатка на Счете Участника), если иное дополнительно не установлено Оператором в отношении Участника;
- осуществление расчетов в Системе до конца рабочего дня;
- установление Оператором Предельных размеров (лимитов) обязательств Участников с учетом уровня риска;
- осуществление Оператором мониторинга выполнения Субъектами Системы требований к управлению непрерывностью функционирования Системы, и разработка в случае необходимости рекомендаций, в целях повышения ими эффективности такой деятельности;
- управление очередностью исполнения распоряжений Участников, обеспечивающее завершение расчетов по операциям, совершенным в рамках Системы, в приоритетном порядке, в пределах допустимых законодательством Российской Федерации;

- осуществление Оператором мониторинга соответствия деятельности Субъектов Системы законодательству Российской Федерации и Правилам;
- разработка Субъектами Системы Планов ОНиВД, содержащих комплекс мер, реализуемый в повседневной деятельности в целях подготовки к чрезвычайным и нестандартным ситуациям и обеспечения бесперебойности деятельности Системы;
- право Оператора на приостановление, в том числе с последующим прекращением участия Участника в Системе в случаях, предусмотренных Правилами.

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

9.6.5. На основании анализа параметров, с использованием которых Оператор производит оценку функционирования Системы (установлены пунктом 10.4. Правил), и иных данных, аккумулируемых Оператором и получаемых от остальных Субъектов Системы в установленном в Правилах порядке, Оператор:

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

9.7. Методики анализа рисков в Системе

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

- сбор, фиксирование, отслеживание и анализ параметров работы Субъектов Системы, в том числе анализ соблюдения порядка расчетов согласно Правилам;
- 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.

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

- выявление и анализ рисков в Системе, включая выявление риск-событий, и определение для каждого из выявленных риск-событий величины риска, 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 УПИ, соответствующего требованиям к оказанию услуг, включая восстановление оказания УПИ 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).

9.7.3. Методики предусматривают выполнение следующих мероприятий:

а. Идентификация риска – выявление риска, определение его причин и предпосылок, которые включают в себя:
- формирование и поддержание в актуальном состоянии перечней бизнес-процессов;
- разработка и поддержание в актуальном состоянии классификаторов (структурированных перечней) рисков в Системе, риск-событий, причин риск-событий;
- проведение анализа бизнес-процессов в Системе, включая анализ и оценку технологического обеспечения привлеченных Операторов УПИ и других факторов, влияющих на БФПС;
- формирование перечня возможных риск-событий для каждого бизнес-процесса с указанием причин риск-событий и их последствий.

б. Анализ и оценка риска – анализ информации, полученной в результате идентификации риска, определение вероятности наступления и последствий риск-событий, который включает в себя:
- определение уровня присущего риска для каждого из выявленных рисков в Системе и установление уровня допустимого риска;
- сопоставление определенного уровня присущего риска и установленного уровня допустимого риска по каждому из выявленных рисков в Системе для выделения значимых для Системы рисков;
- применение способов управления рисками в Системе для каждого из значимых для Системы рисков и последующее определение уровня остаточного риска для каждого из значимых для Системы рисков;
- сопоставление уровней остаточного риска и допустимого риска для каждого из значимых для Системы рисков и принятие решения о необходимости применения других способов управления рисками в Системе в дополнение к ранее примененным способам.

в. Мониторинг уровня риска – выявление событий, способствующих изменению степени подверженности риску, уровня риска, отслеживание динамики характеризующих уровень риска показателей с целью выявления отклонений и определению тенденций в изменении уровня риска, которые включают в себя:
- мониторинг рисков в Системе, в том числе уровней остаточных рисков в Системе, их соответствия уровню допустимого риска;
- составление и пересмотр (актуализацию) по результатам оценки рисков в Системе и анализа эффективности мероприятий по восстановлению оказания УПИ, соответствующего требованиям к оказанию услуг, профиля каждого из выявленных рисков в Системе, включая профиль риска нарушения БФПС.

9.7.4. Составление профилей рисков, включая профиль риска нарушения БФПС, осуществляется в соответствии с законодательством Российской Федерации и нормативными актами Банка России, а также с учетом следующих требований:
- особенностей структуры Системы;
- условий и способов проведения расчетов;

- количественных характеристик потоков расчетных документов;
- распределения прав, ответственности и обязанностей Субъектов Системы.

9.7.4.1. Профили рисков составляются по всем выявленным рискам в Системе и содержат следующие параметры:

- описание риск-событий, выявленных с применением не менее одного метода из числа предусмотренных национальным стандартом Российской Федерации ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 01.12.2011 № 680-ст «Об утверждении национального стандарта» (М., ФГУП «Стандартиформ», 2012) (далее - Стандарт) (риск-события отражаются в профиле каждого из выявленных рисков в платежной системе);
- описание причины возникновения каждого из риск-событий;
- описание бизнес-процессов Оператора и Операторов УПИ, в которых могут произойти риск-события;
- вероятность наступления риск-событий (определение вероятности наступления риск-событий осуществляется с применением не менее одного метода из числа предусмотренных Стандартом);
- описание и оценку возможных неблагоприятных последствий каждого риск-события (если риск-событие имеет несколько возможных неблагоприятных последствий, то указываются все неблагоприятные последствия данного риск-события) (определение неблагоприятных последствий риск-событий осуществляется с применением методов из числа предусмотренных Стандартом с учетом результатов анализа сведений об инцидентах);
- описание бизнес-процессов и перечень Субъектов Системы, на которые влияет риск-событие;
- уровень присущего риска;
- уровень допустимого риска;
- уровень остаточного риска;
- перечень способов управления рисками в Системе, позволяющих снизить уровень присущего или остаточного риска.

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

9.7.4.3. В случае возникновения инцидента, приведшего к приостановлению оказания УПИ, который не отражен в профилях рисков как риск-событие, профили рисков подлежат пересмотру (актуализации) в срок, не превышающий 3 (Трех) месяцев со дня возникновения данного инцидента.

9.7.4.4. Пересмотр (актуализация) профилей рисков производится структурным подразделением (работником) Оператора, ответственным за управление рисками, присущими деятельности Системы по мере необходимости, но не реже 1 (Одного) раза в год.

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

9.8. Порядок проведения оценки рисков, мониторинг рисков в Системе и порядок проведения оценки системы управления рисками

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

- сбор и анализ информации о функционировании Системы, включая информацию об инцидентах;
- расчет показателей БФПС;
- выявление изменений профилей рисков;

- проверка соответствия результатов оценки риска, включая риск нарушения БФПС, фактической информации о риске;
- контроль соблюдения Операторами УПИ уровней оказания УПИ;
- оценку влияния на БФПС инцидентов, возникших в деятельности Субъектов Системы;
- инициирование принятия мер, необходимых для достижения допустимого уровня рисков, включая риск нарушения БФПС.

9.8.2. Оператор проводит оценку рисков в Системе не реже 1 (Одного) раза в год с использованием методик анализа рисков в Системе, включая профили рисков.

9.8.3. Оператор проводит оценку системы управления рисками в Системе, в том числе, используемых методов оценки рисков в Системе, результатов применения способов управления рисками в Системе не реже 1 (Одного) раза в 2 (Два) года.

9.8.4. Критерием оценки системы управления рисками является:

- достижение цели обеспечения непрерывности функционирования Системы в рамках допустимого уровня рисков: обязательства по переводу денежных средств осуществляются в соответствии с регламентом выполнения процедур при гарантированном обеспечении надежности, своевременности и соблюдении информационной безопасности.

При оценке системы управления рисками, в том числе используется система параметров, установленная разделом 10.4. Правил.

9.8.5. Критерием оценки результатов применения способов управления рисками в Системе является нахождение рисков в установленных для них пределах допустимых значений – применение методов приводит к обработке рисков, обеспечивающей достижение допустимого уровня каждым видом риска. Результатом оценки является вывод о правильности организации и эффективности функционирования системы управления рисками, которая должна обеспечивать высокий уровень защиты от возникновения угрозы нарушения БФПС либо необходимости замены неэффективных мероприятий по управлению рисками более эффективными, повышающими общую результативность системы управления рисками.

9.8.6. Критериями оценки применяемых методов оценки рисков являются:

- факты выявления/невыявления риск-событий, ранее неидентифицированных в деятельности Системы, установленные в результате обработки накопленной информации о деятельности Субъектов Системы;
- соответствие характеру и масштабу деятельности Системы;
- соответствие результатов оценки рисков фактической информации о риске;
- отсутствие наличия жалоб и претензий со стороны Участников и их Клиентов к качеству предоставляемых Услуг Системы;
- наличие/отсутствие мер воздействия со стороны надзорных органов.

9.8.7. В случае, если действующая система управления рисками в Системе не позволила предотвратить нарушение оказания УПИ, соответствующего требованиям к оказанию услуг, а также восстановить оказание УПИ, соответствующее требованиям к оказанию услуг, и (или) восстановить оказание УПИ в случае приостановления их оказания в течение периодов времени, установленных в Правилах, Оператор вносит изменения и(или) совершенствует систему управления рисками в Системе.

9.9. Порядок обмена информацией, необходимой для управления рисками

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

9.9.2. Оператор осуществляет контроль за выполнением Участниками и привлеченными Операторами УПИ требований к управлению рисками, установленных Правилами, в рамках осуществления контроля за соблюдением Правил.

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

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

9.9.5. Запрашиваемая информация может касаться вопросов:

- защиты информации;
- мер по поддержанию бесперебойности функционирования Субъекта Системы;
- финансового состояния и выполнения требований Банка России (для кредитных организаций);
- выполнения Правил;
- выполнения требований законодательства Российской Федерации, в том числе в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения.

9.9.6. Участники, привлеченные Операторы УПИ при возникновении событий, вызвавших спорные, нестандартные и чрезвычайные ситуации, включая системные сбои, а также неисполнение или ненадлежащее исполнение своих обязательств доводят до сведения Оператора информацию о таких событиях в соответствии с требованиями пункта 6.12.1. Правил.

9.9.7. Привлеченные Операторы УПИ обязаны незамедлительно информировать и предоставлять Оператору информацию о возникновении угрозы нарушения БФПС и обо всех инцидентах, произошедших в их деятельности, которые привели к нарушению требований регламента выполнения процедур и/или оказали влияние на БФПС в порядке и сроки, определенные пунктом 6.12.1. Правил для взаимодействия в рамках Системы в чрезвычайных ситуациях, и руководствуясь пунктом 10.5.3. Правил.

9.9.8. Участники и РЦ по запросу Оператора предоставляют информацию о своей деятельности в виде отчетности, в том числе: оборотная ведомость по счетам бухгалтерского учета кредитной организации, информация об обязательных нормативах и других показателях деятельности кредитной организации, расчет собственных средств (капитала), отчет о финансовых результатах кредитной организации, годовая (промежуточная) отчетность.

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

9.9.10. Оператор вправе использовать информацию:

- из открытых, доступных на законных основаниях источников, в том числе средства массовой информации, сайт Банка России, сайты Участников, привлеченных Операторов УПИ, систем агрегирования данных, рейтинговых агентств;
- автоматизированного контроля, осуществляемого Оператором.

9.9.11. Оператор обязуется предоставлять Участникам, привлеченным Операторам УПИ информацию, необходимую для управления рисками в Системе как по собственной инициативе, так и по их запросу.

9.9.12. Информация, касающаяся обеспечения защиты информации, пересмотра Плана ОНиВД, привлеченного Оператора УПИ, а также оценки качества функционирования операционных и технологических средств и информационных систем привлеченного

Оператора УПИ, предоставляется по запросу Оператора. Форма предоставления информации определяется Оператором самостоятельно.

9.10. Порядок доведения до органов управления Оператора информации о рисках

9.10.1. Информация о рисках по итогам каждого квартала доводится до сведения единоличного исполнительного органа Оператора структурным подразделением (работником) Оператора, ответственным за управление рисками, присущими деятельности Системы.

9.10.2. Информация об общем уровне рисков Системы доводится до сведения единоличного исполнительного органа Оператора структурным подразделением (работником) Оператора, ответственным за управление рисками, присущими деятельности Системы, не реже 1 (Одного) раза в год.

9.10.3. Результаты оценки эффективности системы управления рисками доводятся до сведения единоличного исполнительного органа Оператора структурным подразделением (работником) Оператора, ответственным за управление рисками, присущими деятельности Системы, не реже 1 (Одного) раза в 2 (Два) года.

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

10. Порядок обеспечения БФПС

10.1. Организация деятельности по управлению непрерывностью функционирования Системы

10.1.1. Оператор совместно с Операторами УПИ и Участниками организует выявление оказания УПИ, не соответствующего требованиям Закона о НПС и принятых в соответствии с ним нормативных актов Банка России, а также положениям Правил, договоров об оказании УПИ, внутренних организационно-распорядительных документов Оператора и привлеченных им Операторов УПИ (далее – требования к оказанию услуг), обеспечению функционирования Системы в случае нарушения оказания УПИ, соответствующего требованиям к оказанию услуг, и восстановлению оказания УПИ, соответствующего требованиям к оказанию услуг, включая восстановление оказания услуг в случае приостановления их оказания в течение периодов времени, установленных Оператором (далее - управление непрерывностью функционирования Системы).

10.1.2. Оператор координирует деятельность Субъектов Системы по обеспечению БФПС.

10.1.3. Участники и РЦ организуют деятельность по реализации порядка обеспечения БФПС в рамках внутренних систем управления рисками, присущими их деятельности.

10.1.4. В Системе БФПС достигается при условии:

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

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

- восстановление надлежащего функционирования платежной системы – не более 72 (Семидесяти двух) часов;

– возобновление осуществления переводов денежных средств в случае его приостановления (прекращения) с момента приостановления (прекращения) – не более 6 (Шести) часов.

10.1.6. Бесперебойным считается функционирование Платежной системы, если вследствие произошедшего инцидента:

– не превышен пороговый уровень показателя продолжительности восстановления оказания УПИ в случае приостановления оказания УПИ;
– отсутствует одновременное нарушение регламента выполнения процедур и порогового уровня показателя непрерывности оказания УПИ;
– не превышено время восстановления надлежащего оказания УПИ.

Неоказание одной из УПИ длительностью более 6 (Шести) часов считается приостановлением функционирования Системы.

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

10.1.8. Участники и РЦ являются кредитными организациями, реализующими меры, направленные на обеспечение непрерывности и (или) восстановление деятельности, в соответствии с требованиями нормативных актов Банка России.

10.1.9. Операторы УПИ обязаны обеспечивать бесперебойность оказания УПИ, предоставляемых им Участникам и их Клиентам, а также соблюдение требований Оператора, связанных с управлением риском нарушения БФПС.

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

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

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

10.1.13. Оператор организует деятельность по управлению непрерывностью функционирования Системы в соответствии с организационной моделью управления рисками в Системе, предусматривающей самостоятельное управлением рисками в Системе Оператором.

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

– распределение обязанностей и прав Субъектов Системы по управлению непрерывностью функционирования Системы;
– установление ответственности за неисполнение порядка БФПС;
– установление системы параметров, на основании которых производится оценка функционирования Системы;
– разработку регламента выполнения процедур и осуществление контроля его соблюдения Субъектами Системы;
– сбор и обработку сведений о функционировании Системы, в том числе от РЦ, используемых для расчета показателей БФПС, а также сведений об инцидентах;
– требования к содержанию деятельности по обеспечению БФПС, осуществляемой Субъектами Системы;
– координацию и контроль деятельности Участников и РЦ по обеспечению БФПС;
– определение подхода к восстановлению оказания УПИ;

- реализацию мероприятий и способов достижения и поддержания допустимого уровня риска нарушения БФПС, включая проведение оценки их эффективности;
- принятие мер по предотвращению, обнаружению, подготовке к чрезвычайным и нестандартным ситуациям, уменьшению степени их воздействия.

10.2. Обязанности и права Субъектов Системы по управлению непрерывностью функционирования Системы

10.2.1. Обязанности и права Субъектов Системы по управлению непрерывностью функционирования Системы разграничиваются в соответствии с применяемой в Системе организационной моделью управления рисками.

10.2.2. Обязанностями Субъектов Системы в части управления непрерывностью функционирования Системы являются:

- осуществление деятельности в соответствии с требованиями законодательства Российской Федерации, нормативных актов Банка России, Правил и договоров, заключенных в рамках Системы;
- осуществление мер, направленных на недопущение нарушений функционирования операционных и технологических средств, информационных систем, обеспечивающих учет информации о переводах денежных средств и состоянии расчетов, в том числе:
  - обеспечение наличия резервирования компонентов сетевой, вычислительной инфраструктуры и систем электроснабжения;
  - дублирование каналов связи;
  - обеспечение регулярного резервного копирования данных по услугам, оказанным в рамках Системы;
  - защита информационных систем от воздействия вредоносного программного кода;
  - обеспечения наличия территориально удаленного резервного центра обработки данных для восстановления функционирования объектов информационной инфраструктуры Системы в случае наступления кризисной ситуации в основном центре обработки данных;
  - обеспечение наличия и своевременной актуализации процедур восстановления программного обеспечения и аппаратного комплекса, задействованного в рамках функционирования Системы и влияющего на БФПС;
  - обеспечение сохранения функциональных возможностей операционных и технологических средств, информационных систем при сбоях в их работе (отказоустойчивость), проведение их тестирования в целях выявления недостатков функционирования, а в случае выявления указанных недостатков - принятие мер по их устранению;
- анализ причин нарушения функционирования операционных и технологических средств, информационных систем, обеспечивающих осуществление переводов денежных средств и учет информации о переводах денежных средств и состоянии расчетов в рамках Системы;
- обеспечение наличия аппаратно-программных средств, используемых для выполнения требований по защите информации при осуществлении переводов денежных средств в рамках Системы;
- построение современной технологической и информационной платформ;
- заблаговременное осуществление инвестиций в новые системы безопасности и параллельные средства защиты и технологическую и информационную платформы;
- построение эффективной системы обеспечения информационной безопасности (применение организационных мер защиты информации и использование

средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации);
- разработка, проверка (тестирование) и пересмотр Плана ОНиВД;
- обеспечение собственной финансовой устойчивости;
- обеспечение сохранности имущества;
- обеспечение наличия квалифицированного персонала;
- построение системы оценки и управления рисками, присущими деятельности Субъекта Системы и способными оказать влияние на БФПС;
- надлежащее исполнение принятых на себя обязательств, в том числе:
  - поддержание РЦ ликвидности в объемах, необходимых для обеспечения обязательств по переводу денежных средств;
  - поддержание Участником остатка денежных средств на Счете Участника, достаточного для осуществления обязательств по переводу денежных средств.
- соблюдение регламента выполнения процедур, предусмотренного Правилами;
- соблюдение Операторами УПИ и РЦ уровней оказания УПИ;
- соблюдение Операторами УПИ продолжительности временных периодов, в течение которых должно быть восстановлено надлежащее функционирование Системы в случае его нарушения, в том числе в случае приостановления (прекращения) оказания УПИ;
- сбор, систематизация, накопление и направление документов и информации в рамках порядка предоставления Участниками и Операторами УПИ информации о своей деятельности Оператору и информационного взаимодействия при выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках Системы, установленных Правилами, в том числе информации о функционировании Системы, информации для расчета показателей БФПС, информации об инцидентах и уровнях оказания УПИ;
- информирование Оператора о случаях неоказания или нарушения требований к оказанию УПИ, и инцидентах, вызвавших операционные сбои, а также о событиях, вызвавших спорные, нестандартные и чрезвычайные ситуации, включая случаи системных сбоев, об их причинах и последствиях;
- прием и обработка обращений Участников, их Клиентов и Получателей по вопросам БФПС;
- осуществление взаимодействия с Оператором в целях управления непрерывностью функционирования Системы;
- иные меры, направленные на обеспечение непрерывности функционирования Системы.

10.2.3. Оператор, выполняющий функции ОЦ и ПКЦ, в целях управления непрерывностью функционирования Системы вправе:
- осуществлять координацию деятельности Субъектов Системы по обеспечению БФПС путем её регламентации в Правилах и путем осуществления контроля за выполнением Правил;
- проверять соблюдение Операторами УПИ и Участниками порядка обеспечения БФПС, в том числе контролировать соответствие документов привлеченных Операторов УПИ порядку обеспечения БФПС, и при выявлении несоответствия документов привлеченных Операторов УПИ порядку обеспечения БФПС направлять рекомендации привлеченным Операторам УПИ по устранению выявленных несоответствий;
- устанавливать требования к содержанию деятельности по обеспечению БФПС, осуществляемой Субъектами Системы;
- участвовать в проведении расследований событий, вызвавших операционные сбои, анализ их причин и последствий;

- применять к Субъектам Системы меры воздействия, включая применение штрафных санкций, предусмотренных Договором участия, вплоть до приостановления деятельности в Системе (временное или постоянное), в случае:
  - несоответствия установленному уровню обеспечения бесперебойности;
  - нарушения требований Правил до устранения допущенного нарушения;
  - неисполнения обязанности по обеспечению достаточности денежных средств для осуществления расчетов;
  - лишать кредитную организацию статуса Участника.
- проводить оценку и мониторинг финансовой устойчивости РЦ и Участников, которым установлен Предельный размер (лимит) обязательств Участника, а также факторов, несущих риски потери финансовой устойчивости РЦ и Участников, в том числе потенциальных, способных привести к потере финансовой устойчивости в будущем;
- проводить контроль соблюдения РЦ и Участниками условий выполнения перевода денежных путем выездных проверок или направлением запросов о предоставлении требуемой информации;
- изучать ситуацию, складывающуюся на финансовом рынке, в том числе на наличие признаков проблем в банковской сфере в целом, а также в отношении конкретных Субъектов Системы;
- определять ответственность привлеченных Операторов УПИ и Участников за неисполнение порядка обеспечения БФПС;
- организовывать проведение привлеченными Операторами УПИ проверки (тестирования) и пересмотра Планов ОНиВД.

10.2.4. РЦ в целях управления непрерывностью функционирования Системы вправе:

- контролировать правоспособность Участников, открывших Счет Участника в РЦ, наличие у них необходимых лицензий;
- проверять осуществление Участниками мероприятий по противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения.

10.3. Ответственность за неисполнение порядка обеспечения БФПС

10.3.1. Субъекты Системы несут ответственность за неисполнение порядка обеспечения БФПС.

10.3.2. Оператор, выполняющий в соответствии с Правилами функции ОЦ и ПКЦ, отвечает за:

- организацию системы управления рисками в Системе в соответствии с требованиями Закона о НПС и Правил;
- последствия реализации рисков в осуществляемой деятельности вследствие неоказания (ненадлежащего оказания) УПИ (за исключением услуг РЦ);
- управление рисками путем контроля за выполнением Участниками и РЦ своих функций, исходя из возложенной на них ответственности за оказание услуг по переводу денежных средств.

10.3.3. Ответственность Оператора за неоказание (ненадлежащее оказание) УПИ установлена пунктом 4.1.14. Правил.

10.3.4. РЦ и Участники несут ответственность за:

- несоблюдение требований законодательства Российской Федерации, нормативных актов Банка России, Правил и заключенных договоров в рамках Системы;
- необеспечение надлежащего функционирования операционных и технологических средств, информационных систем, телекоммуникационных

каналов, используемых для осуществления переводов денежных средств в рамках Системы;
- необеспечение надлежащей защиты информации при осуществлении переводов денежных средств в рамках Системы;
- несвоевременное обеспечение/необеспечение достаточности денежных средств на счетах, используемых для расчетов в рамках Системы;
- несоблюдение установленного Оператором регламента выполнения процедур;
- несоблюдение уровней оказания УПИ.

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

Нарушение	Размер штрафа
первое нарушение положений Правил, влияющее на БФПС	50 000 (Пятьдесят тысяч) рублей
второе нарушение положений Правил, влияющее на БФПС, в течение 12 (Двенадцати) месяцев со дня первого нарушения	100 000 (Сто тысяч) рублей
повторное нарушение одного и того же положения Правил, влияющее на БФПС, в течение 12 (Двенадцати) месяцев со дня первого нарушения	250 000 (Двести пятьдесят тысяч) руб.
третье нарушение положений Правил, влияющее на БФПС, в течение 12 (Двенадцати) месяцев со дня первого нарушения	500 000 (Пятьсот тысяч) рублей
четвертое и последующие нарушения того же самого положения Правил, влияющие на БФПС, и Стандартов Системы в течение 12 (Двенадцати) месяцев со дня первого нарушения	1 000 000 (Один миллион) рублей

10.4. Система параметров, на основании которых производится оценка функционирования Системы

10.4.1. Контроль за соблюдением регламента выполнения процедур осуществляется Оператором посредством анализа сведений о Системе и параметров (уровни оказания УПИ и показатели БФПС), на основании которых производится оценка функционирования Системы.

10.4.2. Уровни оказания УПИ:

а. Уровень оказания операционных услуг:
- показатель доступности услуг ОЦ – не менее 96,00 (Девяноста шести) % времени в течение календарного месяца;
- количество аварий, сбоев по вине ОЦ, влияющих на доступность услуг ОЦ – не более 2 (Двух) аварий, сбоев в месяц;
- количество отказов в приеме от РЦ сообщений об остатках денежных средств на Счетах Участников – не более 2 (Двух) раз в месяц;
- показатель количества обрабатываемых Операций – 100,00 (Сто) % операций;
- время на обработку запроса на совершение Операции не более 30 (Тридцати) секунд;

- время на прием и первичную обработку сообщений от РЦ об остатках денежных средств на Счете Участника – не более 1 (Одного) часа;
- показатель количества распоряжений Участников, по которым в течение календарного месяца были оказаны операционные услуги без нарушения регламента выполнения процедур – не менее 98,00 (Девяноста восьми) % распоряжений в течение календарного месяца;
- восстановление надлежащего оказания операционных услуг и/или возобновление осуществления операционных услуг в случае его приостановления в течение установленных временных периодов.

б. Уровень оказания услуг платежного клиринга:

- количество допущенных ошибок при определении Платежной клиринговой позиции Участника – 0 (Ноль);
- показатель количества распоряжений Участников, по которым в течение календарного месяца были оказаны услуги платежного клиринга без нарушения регламента выполнения процедур – не менее 98,00 (Девяноста восьми) % распоряжений Участников в течение календарного месяца;
- восстановление надлежащего оказания услуг платежного клиринга и/или возобновление осуществления услуг платежного клиринга в случае его приостановления в течение установленных временных периодов.

в. Уровень оказания расчетных услуг:

- показатель количества обрабатываемых распоряжений на перевод денежных средств – 100,00 (Сто) % распоряжений на перевод денежных средств, поступивших на исполнение в РЦ в составе Реестра распоряжений;
- количество допущенных ошибок при проведении операций по списанию/ зачислению денежных средств по Счетам Участников – 0 (Ноль);
- показатель количества распоряжений Участников, по которым в течение календарного месяца были оказаны расчетные услуги без нарушения регламента выполнения процедур – не менее 99,00 (Девяноста девяти) % распоряжений Участников в течение календарного месяца;
- восстановление надлежащего оказания расчетных услуг и/или возобновление осуществления расчетных услуг в случае его приостановления в течение установленных временных периодов.

10.4.3. Показатели БФПС:

10.4.3.1. Показатели 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.

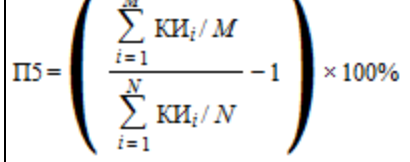
10.4.3.2. К показателям БФПС относятся:

- Продолжительность восстановления оказания УПИ (П1);
- Непрерывность оказания УПИ (П2);
- Соблюдение регламента выполнения процедур (П3);
- Доступность ОЦ (П4);
- Изменение частоты инцидентов (П5).

Наименование показателя БФПС	Единица измерения	Пороговые уровни показателей БФПС	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 осуществлении переводов денежных средств в рамках Системы, установленных нормативными актами Банка России. Определяется как период времени с момента приостановления оказания УПИ вследствие инцидента, произошедшего у Оператора УПИ, и до момента восстановления оказания УПИ.	в часах/ минутах/ секундах	П1 ≤ 6 (Шести) часов	Рассчитывается по каждому из Операторов УПИ и по каждому из инцидентов, повлекших приостановление оказания УПИ, как период времени с момента приостановления оказания УПИ вследствие инцидента, произошедшего у Оператора УПИ, и до момента восстановления оказания УПИ. При возникновении инцидентов, повлекших приостановление оказания УПИ одновременно двумя и более Операторами УПИ, 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 Операторами УПИ, у которых возникли инциденты.
Непрерывность оказания УПИ (П2):			
Период времени между двумя последовательно произошедшими в Системе инцидентами, которые привели к нарушению оказанию УПИ, соответствующего требованиям к оказанию услуг, в том числе вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных	в часах/ минутах/ секундах	П2 ≥ 24 (Двадцати четырех) часов Не рассматривается в качестве инцидентов приостановление (прекращение) участия в Системе в случаях, предусмотренных Правилами в соответствии	Рассчитывается по каждому из Операторов УПИ при возникновении каждого из инцидентов, повлекших приостановление оказания УПИ, как период времени между двумя последовательно произошедшими у оператора УПИ инцидентами, в результате которых приостанавливалось оказание УПИ, с момента устранения первого инцидента и до момента возникновения следующего. Если Оператор УПИ оказывает более одного вида УПИ одновременно, показатель П2 должен

средств, в результате которых приостанавливалось оказание УПИ.		с пунктом 4 части 1 статьи 20 Закона о НПС	рассчитываться одновременно по всем видам УПИ, оказываемым данным Оператором УПИ
Соблюдение регламента выполнения процедур (П3):			
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.	в % с точностью до двух знаков после запятой (с округлением по математическому методу).	П3 ≥ 98,00 % - для ОЦ и ПКЦ П3 ≥ 99,00 % - для РЦ	Рассчитывается ежемесячно по каждому Оператору УПИ. Для ОЦ показатель П3 должен рассчитываться как отношение количества распоряжений Участников (их Клиентов), по которым в течение календарного месяца были оказаны операционные услуги без нарушения регламента выполнения процедур, к общему количеству распоряжений Участников (их Клиентов), по которым были оказаны операционные услуги в течение календарного месяца, рассчитываемое по следующей формуле: $П3_{оц} = \left(N_{оц}/N_{оц}^{общ}\right) \times 100\%,$ где: $N_{оц}$ - количество распоряжений Участников (их Клиентов), по которым в течение календарного месяца были оказаны операционные услуги без нарушения регламента выполнения процедур, $N_{оц}^{общ}$- общее количество распоряжений Участников (их Клиентов), по которым были оказаны операционные услуги в течение календарного месяца. Для ПКЦ показатель П3 должен рассчитываться как отношение количества распоряжений Участников (их Клиентов), по которым в течение календарного месяца были оказаны услуги платежного клиринга без нарушения регламента выполнения процедур, к общему количеству

			распоряжений Участников (их Клиентов), по которым были оказаны услуги платежного клиринга в течение календарного месяца, рассчитываемое по следующей формуле: $П3_{пкц} = \left(N_{пкц}/N_{пкц}^{общ}\right) \times 100\%$, где: $N_{пкц}$ - количество распоряжений Участников (их Клиентов), по которым в течение календарного месяца были оказаны услуги платежного клиринга без нарушения регламента выполнения процедур, $N_{пкц}^{общ}$ - общее количество распоряжений Участников (их Клиентов), по которым были оказаны услуги платежного клиринга в течение календарного месяца. Для РЦ показатель П3 должен рассчитываться как отношение количества распоряжений Участников, по которым в течение календарного месяца были оказаны расчетные услуги без нарушения регламента выполнения процедур, к общему количеству распоряжений Участников, по которым были оказаны расчетные услуги в течение календарного месяца, рассчитываемое по следующей формуле: $П3_{рц} = \left(N_{рц}/N_{рц}^{общ}\right) \times 100\%$,где: $N_{рц}$ - количество распоряжений Участников, по которым в течение календарного месяца были оказаны расчетные услуги без нарушения регламента выполнения процедур, $N_{рц}^{общ}$ - общее количество распоряжений Участников, по которым были оказаны расчетные услуги в течение календарного месяца.

			Значение показателя П3 по Системе в целом принимается равным наименьшему из значений данного показателя, рассчитанных по всем Операторам УПИ 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.
Доступность операционного центра ПС (П4):			
П4 характеризует оказание операционных услуг ОЦ как среднее значение коэффициента доступности ОЦ за календарный месяц	в % с точностью до двух знаков после запятой (с округлением по математическому методу).	П4 ≥ 96,00 % в течение календарного месяца	Рассчитывается по следующей формуле: $П4 = \left(\sum_{i=1}^{M}\left(1-\frac{D_i}{T_i}\right)/M\right)\times 100\%$где: M - количество рабочих дней Системы в месяце, D_i - общая продолжительность всех приостановлений оказания операционных услуг ОЦ за i-ый рабочий день месяца в минутах, T_i - общая продолжительность времени оказания операционных услуг в течение i-го рабочего дня в минутах, установленная в соответствии с регламентом выполнения процедур.
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	в % с точностью до одного знака после запятой (с округлением по математическому методу).	пороговый уровень П5 зависит от количества инцидентов за предыдущие 12 месяцев, включая оцениваемый месяц (а): при а=0 допускается прирост не более 1210%;	Рассчитываться по Системе в целом и для каждого Оператора УПИ в отдельности в отношении всех видов услуг по следующей формуле:  ,

		при a=1 допускается прирост не более 1010 %; при a=2 допускается прирост не более 900 %; при a=3 допускается прирост не более 800 %; при a=4-5 допускается прирост не более 700 %; при a=6-8 допускается прирост не более 600 %; при a=9-11 допускается прирост не более 500 %; при a=12-15 допускается прирост не более 400 %; при a=16-20 допускается прирост не более 300 %	где: $КИ_i$ - количество инцидентов в течение i-го рабочего дня Системы оцениваемого календарного месяца, M - количество рабочих дней Системы в оцениваемом календарном месяце, N - количество рабочих дней Системы за 12 предыдущих календарных месяцев, включая оцениваемый месяц.

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

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

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

10.4.3.6. В случае, когда любой из показателей БФПС и показателей уровней оказания УПИ превышает установленный для него пороговый уровень, руководитель структурного подразделения (работник) Оператора, ответственный за управление рисками, присущими деятельности Системы, незамедлительно информирует об этом единоличный исполнительный орган Оператора и организует принятие мер по устранению выявленных нарушений.

10.4.4. Оператор осуществляет пересмотр системы параметров, на основании которых производится оценка функционирования Системы, по мере необходимости, но не реже1 (Одного) раза в год, с учетом следующего:

- изменений, внесенных в законодательство Российской Федерации и нормативные акты Банка России в области управления рисками в платежных системах;
- результатов оценки рисков в Системе;
- предложений, данных субъектами, входящими в организационную структуру системы управления рисками в Системе.

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

10.5. Сбор и обработка сведений, используемых для расчета показателей БФПС, а также сведений об Инцидентах

10.5.1. Оператор и привлеченные Операторы УПИ осуществляют сбор, документирование и статистическую обработку информации о функционировании Системы, в том числе по обеспечению БФПС.

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

- информация о времени приема к исполнению, времени исполнения распоряжений Участников об осуществлении переводов денежных средств;
- информация о количестве и суммах распоряжений Участников;
- информация о размерах платежных клиринговых позиций и остатках денежных средств на Счетах Участников;
- иная информация о функционировании Системы.

Хранение информации о функционировании Системы осуществляется в электронном виде. По запросу от Оператора привлеченные Операторы УПИ и Участники предоставляют информацию о функционировании Системы в электронном виде или в другом согласованном с Оператором формате.

10.5.3. Оператор организует сбор и обработку сведений, в том числе от привлеченных Операторов УПИ, используемых для расчета показателей БФПС, указанных в пункте 10.4.3. Правил, 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 УПИ (далее - бизнес-процесс), в ходе которых произошел инцидент;
- наименование бизнес-процесса, на который оказал влияние инцидент;
- наличие (отсутствие) факта приостановления (прекращения) оказания УПИ в результате инцидента;
- влияние инцидента на БФПС, определяемое с учетом требований, предусмотренных пунктами 10.5.9. и 10.5.10. Правил;
- степень влияния инцидента на функционирование Системы в зависимости от количества Операторов УПИ, и (или) количества и значимости Участников, на которых оказал непосредственное влияние инцидент, и (или) количества и суммы неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных распоряжений Участников, и иных факторов;
- время и дата восстановления оказания УПИ 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 УПИ, соответствующего 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 УПИ) и (или) взысканных с Оператора (Операторов УПИ);
  - количество и сумма неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных распоряжений Участников, на исполнение которых оказал влияние инцидент;
  - продолжительность приостановления оказания УПИ.

10.5.4. Субъекты Системы обязаны информировать и предоставлять Оператору информацию обо всех инцидентах, произошедших в их деятельности, которые привели к нарушению требований регламента выполнения процедур или оказали влияние на БФПС в порядке и сроки, определенные пунктом 6.12.1. Правил для взаимодействия в рамках Системы в чрезвычайных ситуациях, и руководствуясь пунктом 10.5.3. Правил.

10.5.5. Сбор, документирование и обработка информации могут осуществляться автоматизированным способом с использованием программного обеспечения, применяемого Субъектами Системы.

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

10.5.7. Сбор сведений, используемых для расчета показателей БФПС, сведений об инцидентах, а также иной информации о функционировании Системы осуществляется Оператором следующим образом:

- работниками структурного подразделения (работником) Оператора, ответственными (ым) за управление рисками, присущими деятельности Системы, в том числе с использованием программного комплекса «КП Ритейл» и посредством анализа жалоб и обращений Участников, их Клиентов и Получателей;
- посредством информационного взаимодействия с Субъектами Системы - предоставления Участниками и Операторами УПИ информации, в том числе информации об инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках Системы, порядок которого установлен Правилами.

10.5.8. РЦ ежемесячно, не позднее 3 (Третьего) рабочего дня месяца, следующего за отчетным, предоставляет Оператору по Согласованным каналам связи сведения, используемые для расчета показателей БФПС.

10.5.9. Оператор проводит оценку влияния на БФПС каждого произошедшего в Системе Инцидента в течение 24 (Двадцати четырех) часов с момента его возникновения (выявления), а также в течение 24 (Двадцати четырех) часов после устранения инцидента (восстановления оказания УПИ, соответствующего требованиям к оказанию услуг).

10.5.9.1. 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.

10.5.9.2. 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 УПИ, соответствующее требованиям к оказанию услуг.

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

10.5.10. Оператор проводит оценку влияния на БФПС всех инцидентов, произошедших в Системе в течение календарного месяца. Оценка влияния на БФПС данных инцидентов проводится в течение 5 (Пяти) рабочих дней после дня окончания календарного месяца, в котором возникли инциденты.

10.5.10.1. 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.

10.5.10.2. 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.

10.5.10.3. 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 5 (Пяти) рабочих дней после дня окончания календарного месяца, в котором выявлены инциденты или дополнительные обстоятельства.

10.5.11. Оператор обеспечивает хранение информации о функционировании Системы, в том числе информации об инцидентах не менее 3 (Трех) лет с даты получения указанных сведений.

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

10.6.1. В Системе установлены требования к деятельности по обеспечению БФПС, осуществляемой Субъектами Системы.

10.6.1.1. Оператор обязан:

- организовать и осуществлять деятельность по обеспечению БФПС в соответствии с принятыми на себя обязательствами и требованиями порядка обеспечения БФПС;
- обеспечить непрерывность деятельности и/или восстановления деятельности по оказанию УПИ при возникновении инцидентов, а также организовать в течение установленных периодов времени восстановление оказания УПИ в случае приостановления их оказания и восстановление оказания УПИ, соответствующего требованиям к оказанию услуг, в случае нарушения указанных требований;
- обеспечить реализацию мероприятий, предусмотренных пунктом 10.6.3. Правил;
- анализировать эффективность мероприятий по восстановлению оказания УПИ, соответствующего надлежащему функционированию Системы, и использовать полученные результаты при управлении рисками в Системе.

  Анализ эффективности мероприятий по восстановлению оказания УПИ, соответствующих требованиям к оказанию услуг, осуществляет структурное подразделение (работник) Оператора, ответственное (ый) за управление

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

10.6.1.2. Субъекты Системы обязаны:

- выполнять требования к Планам ОНиВД;
- реализовывать мероприятия, направленные на управление Оператором непрерывностью функционирования Системы в случае возникновения инцидентов, связанных с приостановлением оказания УПИ или нарушением установленных уровней оказания УПИ;
- соблюдать порядок оценки качества функционирования операционных и технологических средств, информационных систем;
- соблюдать порядок изменения операционных и технологических средств и процедур.

10.6.2. Требования к Планам ОНиВД

10.6.2.1. Субъекты Системы обязаны разработать, пересматривать, проводить проверку (тестирование) Плана ОНиВД по мере необходимости, но не реже 1 (Одного) раза в 2 (Два) года.

10.6.2.2. План ОНиВД должен определять порядок, способы и сроки осуществления комплекса мероприятий по предотвращению или своевременной ликвидации последствий возможного нарушения режима повседневного функционирования Субъекта Системы, вызванного непредвиденными обстоятельствами (возникновением чрезвычайной ситуации или иным событием, наступление которого возможно, но трудно предсказуемо и связано с угрозой существенных материальных потерь или иных последствий, препятствующих выполнению Субъектом Системы принятых на себя обязательств).

10.6.2.3. Субъекты Системы, являющиеся кредитными организациями, осуществляют разработку, тестирование (проверку) и пересмотр Плана ОНиВД в порядке, предусмотренном нормативными актами Банка России.

10.6.2.4. Оператор разрабатывает и включает в План ОНиВД мероприятия, направленные на управление непрерывностью функционирования Системы в случае возникновения инцидентов, связанных с приостановлением оказания УПИ или нарушением установленных уровней оказания УПИ, в том числе:

- при наличии в Системе 2 (Двух) и более РЦ - мероприятия по обеспечению взаимозаменяемости данных Операторов УПИ;
- при выполнении Оператором функций ОЦ, ПКЦ и при наличии в Системе одного РЦ - мероприятия по привлечению Операторов УПИ и по переходу Участников на обслуживание к вновь привлеченному Оператору УПИ в течение 20 (Двадцати) рабочих дней после привлечения в случаях:
  - превышения времени восстановления оказания УПИ при приостановлении их оказания более 2 (Двух) раз в течение 3 (Трех) месяцев подряд;
  - нарушения Правил, выразившего в отказе привлеченного Оператора УПИ в одностороннем порядке от оказания услуг Участнику (Участникам), не связанного с приостановлением (прекращением) участия в Системе в случаях, предусмотренных Правилами.

10.6.2.5. В случае, когда Оператор выполняет функции ОЦ и ПКЦ, а также при условии наличия в Системе одного РЦ, Оператор осуществляет мероприятия, указанные в пункте 10.6.2.4. Правил в соответствии с порядком, изложенным в пункте 10.6.3. Правил.

10.6.2.6. Оператор организует, при необходимости, разработку и контролирует наличие Планов ОНиВД у привлеченных Операторов УПИ, проведение ими тестирования и пересмотра Планов ОНиВД с периодичностью не реже 1 (Одного) раза в 2 (Два) года.

10.6.2.7. В целях контроля за выполнением указанной обязанности Оператор с периодичностью не реже 1 (Одного) раза в 2 (Два) года направляет в адрес РЦ запрос о предоставлении: копии Плана ОНиВД РЦ и информации о проведении РЦ проверки

(тестирования) и/или ее сроках/результатах, а также о периодичности пересмотра Плана ОНиВД.

10.6.3. Мероприятия, направленные на управление Оператором непрерывностью функционирования Системы в случае возникновения Инцидентов, связанных с приостановлением оказания УПИ или нарушением установленных уровней оказания УПИ

10.6.3.1.В случае нарушения обслуживающим Участников РЦ времени восстановления оказания УПИ при приостановлении их оказания более 2 (Двух) раз в течение 3 (Трех) месяцев подряд либо нарушения Правил, выразившегося в отказе в одностороннем порядке от оказания услуг Участнику (Участникам), не связанного с приостановлением (прекращением) участия в Системе в случаях, предусмотренных Правилами, Оператор в срок не более 1 (Одного) года с даты повторного превышения времени восстановления оказания УПИ осуществляет следующие мероприятия по привлечению другого РЦ:

- поиск кредитной организации, имеющей возможность осуществления услуг РЦ Системы;
- проведение переговоров и заключение договора с кредитной организацией, имеющей возможность осуществления услуг РЦ Системы;
- проведение правовой и технологической интеграции привлекаемого РЦ в Систему;
- обеспечение возможности для Участников осуществить переход на обслуживание во вновь привлеченный РЦ в течение не более 20 (Двадцати) рабочих дней.

10.6.3.2.В случае, если в течение 6 (Шести) месяцев с момента начала проведения Оператором мероприятий по привлечению нового РЦ отсутствовали факты нарушения РЦ требований к бесперебойности оказания услуг либо нарушения Правил, выразившегося в превышении времени восстановления оказания УПИ при приостановлении их оказания, Оператор вправе прекратить мероприятия по привлечению другого РЦ.

10.6.3.3.В случае нарушения обслуживающим Участников РЦ требований к бесперебойности оказания услуг, выразившегося в отказе в одностороннем порядке от оказания услуг Участнику (Участникам), не связанного с приостановлением (прекращением) участия в Системе в случаях, предусмотренных Правилами, Оператор в срок не более 3(Трех) месяцев с даты такого отказа осуществляет следующие мероприятия по привлечению другого РЦ:

- поиск кредитной организации, имеющей возможность осуществления услуг РЦ Системы;
- проведение переговоров и заключение договора с кредитной организацией, имеющей возможность осуществления услуг РЦ Системы;
- проведение правовой и технологической интеграции вновь привлекаемого РЦ в Систему;
- обеспечение возможности для Участников осуществить переход на обслуживание во вновь привлеченный РЦ в течение не более 20 (Двадцати) рабочих дней.

10.6.3.4.В случае превышения Оператором, выполняющим согласно Правилам функции ОЦ и ПКЦ, времени восстановления оказания УПИ при приостановлении их оказания более 2 (Двух) раз в течение 3 (Трех) месяцев подряд либо нарушения Правил, выразившегося в отказе в одностороннем порядке от оказания услуг Участнику (Участникам), не связанного с приостановлением (прекращением) участия в Системе в случаях, предусмотренных Правилами, Оператор в срок не более 4 (Четырех) месяцев с даты повторного превышения времени восстановления оказания УПИ либо даты отказа в одностороннем порядке от оказания услуг Участнику (Участникам), не связанного с приостановлением (прекращением) участия в Системе в случаях, предусмотренных Правилами, осуществляет следующие мероприятия по привлечению другого ОЦ и/или ПКЦ и по переходу Участников на обслуживание к вновь привлеченному Оператору УПИ:

- поиск специализированной организации, имеющей право и возможность осуществления услуг ОЦ и/или ПКЦ Системы;
- проведение переговоров и заключение договора со специализированной организацией, имеющей право и возможность осуществления услуг ОЦ и/или ПКЦ Системы;
- проведение правовой и технологической интеграции вновь привлеченного Оператора УПИ в Систему;
- перевод Участников на обслуживание к вновь привлеченному Оператору УПИ в течение не более 20 (Двадцати) рабочих дней.

10.6.3.5. В случае, если в течение трех месяцев с момента начала Оператором проведения мероприятий по привлечению нового Оператора УПИ факты превышения Оператором, выполняющим функции ОЦ и ПКЦ, времени восстановления оказания УПИ при приостановлении их оказания более 2 (Двух) раз в течение 3 (Трех) месяцев подряд либо нарушения Правил, выразившегося в отказе в одностороннем порядке от оказания услуг Участнику (Участникам), не связанного с приостановлением (прекращением) участия в Системе в случаях, предусмотренных Правилами, отсутствовали, - Оператор вправе прекратить мероприятия по привлечению другого ОЦ и/или ПКЦ.

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

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

10.6.4.2. Оценка качества функционирования операционных и технологических средств, информационных систем осуществляется Оператором самостоятельно (по мере необходимости) или с привлечением сторонней независимой организации (не реже 1 (Одного) раза в 5 (Пять) лет), выбираемой Оператором самостоятельно. Привлекаемая сторонняя независимая организация должна соответствовать требованиям, иметь лицензии (разрешения), необходимые для осуществления соответствующей деятельности (в случае, если такие требования, лицензии (разрешения) предусмотрены законодательством Российской Федерации). Оценка качества функционирования операционных и технологических средств, информационных систем осуществляется сторонней независимой организацией в соответствии со стандартами и правилами привлекаемой организации, стандартами и правилами, установленными законодательством Российской Федерации (при их наличии), в сроки, согласованные с Оператором и обеспечивающие качественное выполнение поставленной задачи. Периодичность проведения оценки качества функционирования операционных и технологических средств, информационных систем определяется Оператором с учетом изменения (модификации) угроз нарушения нормального функционирования средств и систем, а также в зависимости от изменения иных факторов, влияющих на функционирование операционных и технологических средств, информационных систем.

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

10.6.5. Порядок изменения операционных и технологических средств и процедур

10.6.5.1. 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.

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

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

- УПИ, соответствующие требованиям к оказанию услуг;
- УПИ, несоответствующие требованиям к оказанию услуг.

10.6.5.4. К УПИ, соответствующим требованиям к оказанию услуг, относятся УПИ, при которых одновременно соблюдаются:

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

10.6.5.5. К УПИ, несоответствующим требованиям к оказанию услуг, относятся УПИ, при которых не соблюдаются все или одно их указанных выше требований.

10.6.5.6. В случае если изменение операционных и технологических средств и процедур требует внесения изменений в Правила, Оператор вносит соответствующие изменения в порядке, предусмотренном Законом о НПС и Правилами.

10.6.5.7. В случае если изменение операционных и технологических средств и процедур не требует внесения изменений в Правила, Оператор либо РЦ направляет Участникам уведомление об изменении операционных и технологических средств и процедур с описанием таких изменений и/или размещает информацию о таких изменениях на Официальном сайте в сети интернет не позднее, чем за 10 (Десять) календарных дней до даты вступления в силу соответствующих изменений.

10.6.5.8. Изменение операционных и технологических средств и процедур в Системе осуществляется Оператором при наличии необходимости в случае изменения порядка совершения или видов операций, совершаемых в рамках Системы, в целях совершенствования системы управления рисками, по результатам проведения оценки качества функционирования операционных и технологических средств, информационных систем, проведенной самостоятельно или с привлечением независимой организации, а также в случаях, предусмотренных законодательством Российской Федерации, и по требованию Банка России.

10.6.5.9. РЦ и Участники вправе самостоятельно вносить изменения в операционные и технологические средства и процедуры по взаимодействию с Системой на стороне РЦ или Участника, если внесение таких изменений не противоречит нормативным актам соответствующих регуляторов, Правилам и условиям договоров, заключенных в рамках взаимодействия между Субъектами Системы, и не приводит к изменению порядка оказания Услуг Системы, предусмотренного Правилами, к объему и характеру их оказания Участникам, привлеченным Оператором УПИ, а также не повлияет негативно на обеспечение БФПС, управление рисками и обеспечение защиты информации в Системе.

10.7. Порядок взаимодействия Субъектов Системы по обеспечению БФПС

10.7.1. Субъекты Системы в целях управления непрерывностью функционирования Системы обязаны руководствоваться Правилами.

10.7.2. Порядок взаимодействия Субъектов Системы в целях управления рисками и непрерывностью функционирования Системы включает следующее:

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

10.7.3. С целью обеспечения БФПС привлеченные Операторы УПИ и Участники обязаны оперативно информировать Оператора о следующих событиях:

- 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;
- о возникновении в процессе работы в Системе нарушений и неисправностей либо об обстоятельствах, которые препятствуют исполнению переводов денежных средств, повлекших за собой значительное нарушение допустимого уровня риска (включая случаи системных сбоев);
- о наступлении спорных, чрезвычайных, нестандартных ситуаций;
- о случаях или попытках осуществления переводов денежных средств без согласия Клиента (Участника).

10.7.4. Направление информации осуществляется по Согласованным каналам связи в соответствии с требованиями пункта 6.12.1. Правил.

10.7.5. Оператор незамедлительно с момента получения от Субъекта Системы уведомления о наступлении событий/ситуаций совместно с соответствующими Субъектами Системы определяет план дальнейших действий индивидуально по каждому наступившему событию/ситуации в целях устранения возникших операционных сбоев, в том числе их последствий, и предотвращения наступления новых.

10.7.6. Оператор информирует Банк России, Участников и привлеченных Операторов УПИ о случаях и причинах приостановления (прекращения) оказания УПИ в следующем порядке:

- информирование Банка России (Департамента национальной платежной системы) осуществляется посредством направления сообщения на бумажном носителе или электронного сообщения, снабженного кодом аутентификации, в течение 2 (Двух) рабочих дней со дня приостановления (прекращения) оказания УПИ (при этом Оператор в день приостановления (прекращения) оказания УПИ незамедлительно направляет в Банк России (Департамент национальной платежной системы) уведомление о приостановлении (прекращении) оказания УПИ с использованием способа связи, информация о котором доведена до него Банком России (Департаментом национальной платежной системы));
- информирование Участников и привлеченных Операторов УПИ в день такого приостановления (прекращения) любым из указанных ниже способов:
  - размещение информации на Официальном сайте Оператора в сети интернет;
  - направление уведомления по Согласованным каналам связи, в том числе СЭДО, Кабинеты Участников, телефонная связь.

10.8. Порядок контроля за соблюдением привлеченными Операторами УПИ и Участниками порядка обеспечению БФПС

10.8.1. Деятельность по обеспечению БФПС осуществляется Субъектами Системы в соответствии с порядком обеспечения БФПС, установленным в Правилах.

10.8.2. Оператор осуществляет контроль за соблюдением привлеченными Операторами УПИ и Участниками порядка обеспечения БФПС в рамках осуществления контроля за соблюдением Правил, в указанных целях:

- запрашивает и получает документы и информацию о деятельности, связанной с выполнением требований по обеспечению БФПС, в соответствии с порядком предоставления Участниками и РЦ информации о своей деятельности Оператору, установленным пунктом 6.10. Правил, и в рамках информационного взаимодействия Субъектов Системы при выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках Системы, определенного пункте 11.6. Правил;
- проводит на основе полученной информации анализ и оценку рисков;
- проводит проверку соответствия результатов оценки риска, включая риск нарушения БФПС, фактической информации о риске.

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

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

10.8.4. Оператор контролирует соответствие Плана ОНиВД РЦ порядку обеспечения БФПС и при выявлении несоответствия порядку обеспечения БФПС направляет рекомендации РЦ по устранению выявленных несоответствий.

10.8.5. Оператор при выявлении нарушения порядка обеспечения БФПС привлеченными Операторами УПИ и Участниками:

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

11. Обеспечение защиты информации в Системе

11.1. Общие правила осуществления защиты информации

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

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

11.1.3. Защита информации при проведении операций по переводу денежных средств осуществляется Субъектами в соответствии с требованиями следующих документов, а также с учетом специфики деятельности Субъекта Системы:

- Постановления Правительства Российской Федерации № 584;
- Положения Банка России № 719-П;
- Правил.

Субъекты Системы, являющиеся кредитными организациями, осуществляют деятельность по защите информации в соответствии с требованиям и стандартам Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации.

11.1.4. 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.

11.1.5. К защищаемой в Системе информации относятся:

- информация об остатках денежных средств на Счетах Участников;
- информация о совершенных переводах денежных средств, в том числе содержащаяся в оформленных в рамках применяемой формы безналичных расчетов распоряжениях Клиентов Участников, Реестрах ПКЦ и Реестрах распоряжений, включая информацию о платежных клиринговых позициях;
- информации, хранящейся в ОЦ и ПКЦ, о совершенных переводах денежных средств с использованием ЭСП;
- информация, необходимая для удостоверения Клиентами права распоряжения денежными средствами, в том числе данных Пользователей ЭСП;
- информация о Конфигурации Участника, определяющей параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается Участниками, Операторами УПИ, и используемых для осуществления переводов денежных средств, а также информация о Конфигурации Участника, 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 и иная информация, подлежащая обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемая при осуществлении переводов денежных средств.

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

11.2. Требования к обеспечению защиты информации

11.2.1. Требования к обеспечению защиты информации включают в себя:

- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация и использование которых обеспечивается в рамках Системы (далее – объекты информационной инфраструктуры);
- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые в отношении прикладного программного обеспечения автоматизированных систем и приложений;
- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые в отношении технологии обработки

информации, подготавливаемой, обрабатываемой и хранимой на участках идентификации, аутентификации и авторизации Клиентов Участников;
- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые в отношении информирования Банка России об инцидентах (событиях), связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при использовании средств криптографической защиты информации;
- требования к доведению до Оператора информации об обеспечении в Системе защиты информации при осуществлении переводов денежных средств;
- требования к совершенствованию защиты информации при осуществлении переводов денежных средств.

Также Субъекты Системы обязаны выполнять следующие требования:

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

- требования к определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств;
- требования к оценке выполнения Оператором, Участником, Оператором УПИ требований к обеспечению защиты информации при осуществлении переводов денежных средств.

11.2.2. Субъекты Системы обязаны проводить в соответствии с требованиями нормативных актов Банка России оценки соответствия защиты информации и тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

Для проведения оценок соответствия защиты информации и анализа уязвимостей в прикладном программном обеспечении автоматизированных систем и приложений Субъектам Системы следует привлекать организацию, имеющую лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение соответствующих работ и услуг.

11.2.3. 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;
- изменения требований к защите информации, установленных Правилами;
- совершенствования защиты информации в Системе;
- выявления недостатков при осуществлении контроля защиты информации в Системе.

11.2.4. Субъекты Системы обязаны:

- обеспечивать реализацию установленных Положением Банка России № 719-П уровней защиты информации для объектов информационной инфраструктуры, используемых для обработки, передачи, хранения защищаемой информации, в целях осуществления переводов денежных средств;
- обеспечивать регистрацию результатов совершения действий, связанных с осуществлением доступа к защищаемой информации.

11.3. Порядок обеспечения защиты информации в Системе

11.3.1. В целях обеспечения защиты информации в Системе при хранении, обработке, обмене защищаемой информацией Субъекты Системы обеспечивают, включая, но, не ограничиваясь: применение организационных мер защиты информации, технических средств защиты информации, стандартов Банка России в области защиты информации, поддержки программ управления уязвимостями, а также обеспечивают создание и поддержание безопасной сетевой инфраструктуры, управление риском информационной безопасности, мониторинг сетевой инфраструктуры, внедрение и поддержание мер по управлению доступом к защищаемой информации.

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

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

11.3.4. В рамках реализации мер по поддержке программы управления уязвимостями Субъекты Системы обязаны выполнять установленные Правилами требования к обеспечению защиты информации от воздействия вредоносных кодов, обеспечить использование на всех объектах информационной инфраструктуры, задействованных в хранении, обработке и

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

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

- предоставление доступа к Системе только тем лицам, которым такой доступ необходим для выполнения возложенных на них функций, в том числе связанных с осуществлением переводов денежных средств в Системе;
- учет лиц, имеющих доступ к защищаемой информации;
- предоставление доступа каждому работнику с использованием уникального имени, учетной записи, пароля и/или ключа электронной подписи для доступа к защищаемой информации;
- многокомпонентность и многоразрядность (не менее 5 (Пяти) символов) используемых паролей, а также периодическую смену паролей;
- немедленный отзыв доступа при прекращении полномочий лица на доступ к защищаемой информации;
- ограничение доступа к техническим средствам автоматизированных систем, обеспечивающих взаимодействие в Системе;
- недопущение использования установленных производителем программного обеспечения паролей и иных параметров безопасности, устанавливаемых по умолчанию;
- ограничение доступа к материальным носителям, содержащим защищаемую информацию или её архивные и резервные копии, строгий контроль за хранением материальных носителей;
- включение в должностные обязанности работников, участвующих в обработке информации, обязанности по выполнению требований к защите информации;
- включение в должностные обязанности работников, участвующих в обработке информации, обязанности сообщения о подозрительных событиях в Системе, которые могут быть квалифицированы как инциденты защиты информации;
- приостановление обработки информации Субъектом в случае инцидента защиты информации, до устранения причин инцидента и/или предотвращения его возможных последствий.
- выявление инцидентов, связанных с нарушением требований к защите информации, немедленное информирование о них Оператора;
- контроль применения в автоматизированных системах Участников технических средств защиты информации (криптографические средства, средства защиты персональных компьютеров 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 (Одного) раза в 2 (Два) года.

11.3.6. В рамках реализации мер по мониторингу сетевой инфраструктуры Субъекты Системы должны контролировать доступ к сетевым ресурсам и защищаемой информации, для чего организуют мониторинг событий, касающихся доступа к сетевым ресурсам, регистрируют действия пользователей, необходимые для проведения расследования и анализа причин инцидентов защиты информации, обеспечивают хранение журналов событий не менее 1 (Одного) года, а в оперативном доступе не менее 3 (Трех) месяцев, обеспечивают плановую и внеплановую (при внесении изменений) проверку систем, процессов и программного обеспечения для поддержания их защищенности на должном уровне.

11.3.7. Субъекты Системы определяют структурное подразделение (работника), ответственное (ответственного) за организацию и контроль обеспечения защиты информации,

задачей которого, в том числе, является повышение осведомленности работников в области обеспечения защиты информации.

11.3.8. В части, не установленной в Правилах, Субъекты Системы, руководствуясь законодательством Российской Федерации, 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.

11.3.9. Управление риском информационной безопасности в Системе осуществляется Субъектами Системы как одним из видов операционного риска, присущих деятельности Системы, источниками реализации которого являются: недостатки процессов обеспечения защиты информации, в том числе недостатки применяемых технологических мер защиты информации, недостатки прикладного программного обеспечения автоматизированных систем и приложений, а также несоблюдение требований к указанным процессам деятельности Участниками и Операторами УПИ.

11.3.10. Субъекты Системы обязаны обеспечить реализацию мероприятий по управлению риском информационной безопасности с учетом требований, установленных в Положении Банка России № 719-П и Правилах, в том числе:

- выявлять и идентифицировать риск информационной безопасности в Системе в отношении объектов информационной инфраструктуры Субъекта Системы, входящих в состав и обеспечивающих реализацию технологических процессов, осуществляемых в рамках Системы (объекты информационной инфраструктуры), в том числе посредством следующего:
  - проведения аудита информационной безопасности в виде самооценки и/или привлечения организации, имеющей соответствующую лицензию;
  - проведения оценки соответствия уровням защиты информации, согласно Положению Банка России № 719-П;
  - проведения тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры Субъекта Системы;
  - составления и пересмотра моделей угроз и нарушителей информационной безопасности;
  - выявления новых информационных активов.

  В целях идентификации риска информационной безопасности Субъекты Системы разрабатывают и поддерживают в актуальном состоянии классификаторы рисков информационной безопасности: источники риска, типы риск-событий, виды потерь от реализации риска.
- выявлять риск информационной безопасности в Системе, в том числе посредством следующего:
  - ведения деятельности по выявлению следов активности нарушителя (включая регулярное изучение данных, полученных на основании анализа журналов регистрации информационных систем, систем защиты, и журналов действий и операций автоматизированных рабочих мест, серверного и сетевого оборудования, межсетевых экранов и автоматизированных систем);
  - обнаружения нетипичных событий, связанных с информационной безопасностью, и информирование о данных событиях структурного подразделения (работника), ответственного за организацию и контроль обеспечения защиты информации Субъекта Системы;

- проведения оценки уровня информационной безопасности;
- проведения анализа динамики показателей уровня риска информационной безопасности;
- проведения анализа внешних источников информации;
- осуществления контроля всех операций в бизнес-процессах, где осуществляется взаимодействие персонала со средствами и системами автоматизации;
- получения уведомлений/сообщений Банка России, иных органов, осуществляющих контроль или надзор за деятельностью Субъектов Системы;
- работы с претензиями и жалобами (заявлениями, обращениями) Клиентов Участников, Субъектов Системы;
- проведения процедур мониторинга информационной безопасности и анализа данных о действиях и операциях на объектах информационной инфраструктуры.

- проводить анализ и оценку риска информационной безопасности согласно разработанной Оператором и доведенной по Согласованным каналам связи до Субъектов Системы Методике анализа и оценки риска информационной безопасности в Платежной системе «КП Ритейл», в том числе:
  - инвентаризация объектов информационной инфраструктуры;
  - идентификация бизнес-требований и требований законодательства Российской Федерации в области информационной безопасности;
  - оценка ценности объектов информационной инфраструктуры;
  - анализ угроз и уязвимостей;
  - определение величины риска, оценивание и ранжирование.

- реагировать на инциденты защиты информации согласно разработанной Оператором и доведенной по Согласованным каналам связи до Субъектов Системы Методике реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе «КП Ритейл» и восстанавливать штатное функционирование объектов информационной инфраструктуры в случае реализации инцидентов защиты информации, руководствуясь пунктом 11.6.8. Правил;
- осуществлять обмен информацией об инцидентах защиты информации в порядке, установленном в пункте 11.6 Правил;
- противодействовать осуществлению переводов денежных средств без согласия Клиента или Участника согласно требованиям, установленным пунктом 11.9. Правил.

11.3.11. В целях управления риском информационной безопасности Оператор, выполняющий функции ОЦ и ПКЦ, устанавливает состав и допустимые значения показателей уровня риска информационной безопасности, на основании которых, в том числе применяет в отношении Субъектов Системы ограничения по параметрам операций по осуществлению переводов денежных средств, а также снятие таких ограничений:

Показатели уровня риска информационной безопасности в Системе

Показатели уровня риска информационной безопасности	**Пороговые значения низкого уровня риска информационной безопасности**	**Пороговые значения высокого уровня риска информационной безопасности**
Количество инцидентов	Не более 2 (Двух) в месяц	Более 2 (Двух) в месяц

Защиты информации в Системе, допущенных Субъектами Системы		
Доля переводов денежных средств без согласия Клиента Участника в общем количестве переводов денежных средств	Менее 0,005% в квартал	Более 0,005% в квартал
Событие риска информационной безопасности	Событие риска информационной безопасности, которое привело к временной деградации/недоступности сервисов. Сумма убытков Оператора составила менее 500 000 (Пятьсот тысяч) рублей/ раскрыта информация о менее 10% Банковских карт.	Событие риска информационной безопасности, вследствие которого информационная инфраструктура была атакована, затронуты критичные объекты информационной инфраструктуры, что привело/может привести к системной компрометации, утечке конфиденциальной информации, хищению денежных средств или нарушению критичных бизнес-процессов, приведшему к недоступности сервисов Системы и полному непредоставлению Услуг Системы. Сумма убытков Оператора составила 500 000 (Пятьсот тысяч) рублей и более/ раскрыта информация о 10% Банковских карт и более.
Итоговая оценка защиты информации согласно оценке полноты реализации процессов системы защиты информации, проведенной в соответствии с Национальным стандартом Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»	>=0,85	<0,85

В случае достижения пороговых значений показателей, характеризующих высокий уровень риска информационной безопасности, Оператор применяет в отношении Субъектов

Системы, на объектах информационной структуры которых произошло событие риска информационной безопасности, ограничения в виде:

- приостановления оказания услуг (в частности, в отношении Участника, вправе применить приостановление его участия в Системе в соответствии с пунктом 6.5. Правил);
- ограничения по параметрам операций по осуществлению переводов денежных средств – ограничение в отношении суммы единичной Операции, количества и/или суммы операций по переводу денежных средств за определяемый Оператором период времени.

О приостановлении оказания услуг Субъектом Системы Оператор направляет по Согласованным каналам связи уведомление на имя руководителя Субъекта Системы.

После устранения факторов, которые привели к превышению значений показателей уровня риска информационной безопасности, Субъект Системы направляет документальное подтверждение в адрес Оператора по Согласованным каналам связи.

Решение о снятии/продлении ограничений принимаются Оператором с учетом следующего:

- отсутствие инцидентов защиты информации в последующие 3 (Три) месяца;
- предоставление документов и информации об устранении причин возникновения инцидентов защиты информации, по результатам анализа которых Оператором реализованные Субъектом Системы корректирующие действия признаны эффективными;
- Субъектом Системы, в функциональной зоне которого был допущен инцидент защиты информации, возмещены Оператору убытки.

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

11.3.13. 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 договорных отношений с данным Субъектом Системы и прекращением его функций. В случае расторжения договорных отношений с привлеченным Оператором УПИ, Оператор реализует мероприятия, обеспечивающие возможность для Участников осуществить в течение срока, не превышающего 20 (Двадцати) рабочих дней переход на обслуживание к другому Оператору УПИ.

11.4. Использование средств криптографической защиты информации

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

11.4.2. Для защиты электронных сообщений, в целях обеспечения их целостности и аутентичности, в Системе применяются электронные подписи. При обмене электронными сообщениями между Субъектами Системы используются средства криптозащиты,

реализующие электронную подпись по ГОСТ 2012, сертифицированные ФСБ России, для обмена с абонентами - резидентами Российской Федерации;

11.4.3. Оператор, выполняющий функции ОЦ определяет требования к используемым при организации обмена сообщениями Системе средствам криптозащиты, входящим в состав операционных систем, которые доводятся до привлеченных Операторов УПИ и Участников по Согласованным каналам связи.

11.4.4. Сообщения, которыми обмениваются Субъекты Системы при использовании СЭДО, должны быть подписаны уполномоченными лицами соответствующих Субъектов Системы с использованием усиленной квалифицированной подписи, выданной удостоверяющим центром, имеющим аккредитацию Минкомсвязи России.

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

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

- самостоятельно организовать работу по защите информации от воздействия вредоносных кодов, включающую в том числе меры, осуществляемые для предотвращения воздействия вредоносного кода, меры, направленные на выявление проникновения вредоносного кода, меры реагирования на данный вид инцидентов защиты информации;
- использовать технические средства защиты информации, предназначенные для выявления вредоносного кода и для предотвращения воздействия вредоносного кода на объектах информационной инфраструктуры (далее – антивирусные средства);
- регулярно обновлять версий антивирусных средств и баз данных, используемых в работе антивирусных средств и содержащих описание вредоносных кодов и способы их обезвреживания, обеспечивая их актуальность;
- обеспечить функционирование антивирусных средств в автоматическом неотключаемом режиме;
- обеспечить антивирусный контроль при обмене данными с недоверенными сетями передачи данных;
- проводить регулярный анализ информации из общедоступных источников о новых видах вредоносных кодов для своевременной организации противодействия новым угрозам.

11.5.2. 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 Устройства приема платежей, выполняемой после установки или изменения программного обеспечения.

11.5.3. При обнаружении Субъектом Системы проникновения вредоносных кодов на объектах информационной инфраструктуры, задействованных в информационном обмене в рамках Системы, обнаруживший вредоносный код Субъект Системы, обязан:

- ограничить или приостановить информационный обмен с другими Субъектами Системы;

- ограничить или приостановить работу объекта информационной инфраструктуры, который является источником заражения;
- проинформировать стороны информационного обмена в электронном виде по Согласованным каналам связи о возникновении инцидента защиты информации;
- принять меры реагирования при возникновении данного вида инцидента защиты информации, в том числе:
  - провести резервирование критичной информации;
  - провести антивирусным программным обеспечением «лечебные» мероприятия;
  - при обнаружении файлов, не подлежащих «лечению», или возникновению подозрений на некорректное «лечение» файлов – обратиться к разработчику антивирусного программного обеспечения для срочного оказания технической поддержки и помощи в устранении заражения;
  - проверить целостность и корректность рабочих файлов.
- по согласованию с Оператором перейти на штатное функционирование объектов информационной инфраструктуры;
- проинформировать стороны информационного обмена в электронном виде по Согласованным каналам связи о возобновлении указанного вида информационного обмена после восстановления нормального функционирования объектов информационной инфраструктуры, используемых в электронном обмене.

11.6. Порядок действий и информационное взаимодействие при выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и восстановление штатного функционирования объектов информационной инфраструктуры

11.6.1. При выявлении инцидентов защиты информации, в результате которых был нарушен регламент выполнения процедур и которые повлияли на БФПС (критичность инцидента согласно Методике реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе «КП Ритейл», оценена, как «Высокая» и «Средняя»):

- Субъект Системы, выявивший указанные обстоятельства, незамедлительно принимает меры по снижению негативных последствий, вызванных нарушением требований;
- немедленно информирует Оператора и Субъекта Системы, в функциональной зоне ответственности которого находится область возникновения инцидента;
- Субъект Системы, допустивший инцидент, принимает меры реагирования, направленные на устранение причин, вызвавших инцидент, и на недопущение его повторного возникновения, и последствий инцидента.

11.6.2. При выявлении инцидентов защиты информации, в результате которых не был нарушен регламент выполнения процедур и, которые не повлияли на БФПС (критичность инцидента согласно Методике реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе «КП Ритейл» оценена, как «Низкая»):

- Субъект Системы, выявивший указанные обстоятельства:
  - незамедлительно принимает меры по снижению негативных последствий, вызванных нарушением требований;
  - немедленно информирует Субъекта Системы, в функциональной зоне ответственности которого находится область возникновения инцидента;
  - информирует Оператора не позднее 3 (Третьего) рабочего дня месяца, следующего за месяцем, в котором имели место данные инциденты.

– Субъект Системы, допустивший инцидент, принимает меры реагирования, направленные на устранение причин, вызвавших инцидент, и на недопущение его повторного возникновения, и последствий инцидента.

11.6.3. Участники обеспечивают регистрацию ставших им известными инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, выявленных Клиентами Участников.

Участники и привлеченные Операторы УПИ обеспечивают регистрацию самостоятельно выявленных инцидентов защиты информации.

Оператор обеспечивает регистрацию в собственной информационной системе всех выявленных Субъектами Системы инцидентов защиты информации.

11.6.4. Участники и привлеченные Операторы УПИ информируют Оператора об обстоятельствах, указанных в пунктах 11.6.1. и 11.6.2. Правил, по СЭДО, в процессе обмена электронными документами по которой для обеспечения конфиденциальности электронных документов, определения уполномоченного лица, подписавшего электронный документ, а также для подтверждения того, что электронный документ исходит от одной из сторон и не претерпел изменений, применяются средства криптографической защиты информации (сообщение об инциденте подписывается квалифицированной электронной подписью уполномоченного лица стороны обмена). Резервными способами передачи информации Оператору являются:

– электронная почта (адрес электронной почты Оператора: cpretail@cpretail.ru;
– телефонный звонок на номер 8 (800) 101 88 80.

Ответственными должностными лицами для взаимодействия по вопросам выявления инцидентов защиты информации со стороны Оператора являются работники подразделения информационной безопасности.

Резервные способы передачи сообщения об инциденте защиты информации Оператору используются только в случаях отсутствия телекоммуникационной доступности СЭДО и/или отсутствия технической возможности передачи информации.

11.6.5. Оператор информирует Участников и Операторов УПИ об обстоятельствах, указанных в пунктах 11.6.1. и 11.6.2. Правил, незамедлительно, в день выявления или получения информации об инциденте защиты информации от Участника или привлеченных Операторов УПИ по любому из доступных каналов связи:

– Официальный сайт Оператора в сети интернет;
– СЭДО;
– электронная почта должностного лица Субъекта Системы - ответственными должностными лицами для взаимодействия с Оператором по вопросам выявления инцидентов защиты информации, являются уполномоченные должностные лица Субъекта Системы (стороны обмена по системе электронного документооборота).

11.6.6. Сообщение об инциденте защиты информации должно включать, в том числе, даты возникновения и устранения инцидента, описание инцидента, информацию о событиях, по мнению отправителя, вызвавших инцидент, о его причинах и последствиях, меры, принятые для его устранения и предупреждения его возникновения в дальнейшем.

11.6.7. Восстановление штатного функционирования объектов информационной инфраструктуры после реализации инцидентов защиты информации осуществляется в соответствии с Планами ОНиВД Субъектов Системы, а также после проведения следующих мероприятий:

– Субъект Системы, в функциональной зоне ответственности которого находится область возникновения инцидента:
  - реализует комплекс мер, направленных на нейтрализацию угроз, устранение источников инцидента и последствий;
  - восстанавливает работоспособность объектов информационной инфраструктуры, в том числе проводит оценку объема необходимых работ по ремонту/замене оборудования, восстанавливает работоспособность

поврежденных критичных аппаратных средств и другого оборудования, при необходимости производит замену отказавших узлов и блоков резервными либо посредством покупки новых;

- восстанавливает поврежденное критичное программное обеспечение, используя эталонные копии;
- восстанавливает необходимые данные, используя резервные копии, или осуществляет перенос данных с резервного вычислительного центра, в случае, когда ведение технологических процедур бизнес-процессов осуществлялось на территории резервного вычислительного центра;
- проверяет работоспособность восстановленных подсистем, а также удостоверяется в том, что последствия нештатной ситуации не оказывают воздействия на дальнейшую работу объектов информационной инфраструктуры.

– направляет Оператору подтверждение о реализации указанного выше комплекса мер, а также о функционировании системы обеспечения защиты информации в штатном режиме, характеризующемся исправной работой всех средств защиты информации, а также восстановлением свойств информационной безопасности, отсутствием серьезных уязвимостей и наличием адекватных контрмер.

Время восстановления штатного функционирования объектов информационной инфраструктуры после реализации инцидентов защиты информации, не повлекших фатальных сбоев, не должно превышать временных периодов, установленных пунктом 10.1.5. Правил.

– Оператор:

- согласует переход Субъекта Системы на штатное функционирование объекта информационной инфраструктуры;
- проводит контроль восстановления штатного функционирования объектов информационной инфраструктуры Системы, основным критерием которого является соблюдение пороговых значений показателей уровней оказания УПИ, установленных пунктом 10.4.2. Правил.

11.6.8. Участники и привлеченные Операторы УПИ в составе информации о своей деятельности, представляемой в порядке и сроки, определенные пунктом 6.10. Правил, представляют данные для целей анализа обеспечения в Системе защиты информации при осуществлении переводов денежных средств. При этом состав указанных данных должен соответствовать требованиям нормативных актов Банка России, регламентирующих требования к обеспечению защиты информации в Системе при осуществлении переводов денежных средств.

11.7. Обеспечение защиты персональных данных в Системе

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

11.7.2. Субъекты Системы гарантируют Оператору, что осуществляют на законных основаниях обработку, включая сбор и передачу Оператору и иным лицам персональных данных субъектов персональных данных в целях реализации Правил.

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

11.8. Обеспечение банковской и коммерческой тайны в Системе

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

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

11.9. Порядок реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия Клиента Участника (Участника)

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

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

- обеспечивают защиту информации согласно требованиям, установленным Правилами;
- реализуют определенные нормативными актами Банка России и Правилами мероприятия по противодействию осуществлению Перевод без согласия Клиента Участника;
- в рамках информационного взаимодействия направляют информацию, полученную в ходе реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия Клиента Участника (Участника), в порядке, установленном в пункте 11.9.6. Правил.

11.9.3. Оператор, выполняющий функции ОЦ и ПКЦ, при реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия Клиента должен:

- выявлять компьютерные атаки, направленные на объекты информационной инфраструктуры Оператора и (или) Клиентов Участников, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия Клиента Участника;
- рассматривать случаи и (или) попытки осуществления переводов денежных средств без согласия Клиента Участника, вызванные компьютерными атаками, направленными на объекты информационной инфраструктуры Субъектов Системы и (или) Клиентов Участника;
- реализовывать меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры Оператора и (или) Клиентов Участников, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия Клиента Участника;
- использовать информацию о Переводах без согласия Клиента Участника для выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента;
- осуществлять анализ Операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, в рамках Системы.

11.9.3.1. Порядок выявления компьютерных атак, направленных на объекты информационной инфраструктуры Оператора и (или) Клиентов Участников, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия Клиента Участника, и реагирования:

- выявление компьютерных атак осуществляется техническими средствами защиты информации, применяемыми Оператором, входящими в систему

защиты информации, техническими средствами защиты информации на уровне провайдеров, оказывающих Оператору услуги связи, а также в рамках информационного взаимодействия с Субъектами Системы в порядке, установленном Правилами;

- контроль наличия и работоспособности технических средств защиты информации, применяемых Оператором;
- источниками информации о компьютерных атаках являются:
  - сообщение о компьютерной атаке, выявленной посредством технических средств защиты информации, применяемых Оператором;
  - информирование Оператора о компьютерной атаке провайдером услуг связи по согласованным каналам связи в соответствии с заключенными договорными отношениями;
  - информирование структурным подразделением Оператора, непосредственно взаимодействующим с Субъектами Системы.
- при получении информации о компьютерной атаке Оператор организует проведение мер по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры Оператора, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия Клиента Участника в соответствии с пунктами 11.9.3.2. и 11.9.3.3. Правил.

11.9.3.2. Порядок рассмотрения случаев и (или) попыток осуществления переводов денежных средств без согласия Клиента Участника, вызванных компьютерными атаками, направленными на объекты информационной инфраструктуры Субъектов Системы и (или) Клиентов Участника:

Оператор, выполняющий функции ОЦ и ПКЦ, в целях рассмотрения случаев и (или) попыток осуществления переводов денежных средств без согласия Клиента Участника, вызванных компьютерными атаками, направленными на объекты информационной инфраструктуры:

- осуществляет сбор, аккумулирование и изучение:
  - информации о компьютерных атаках, направленных на объекты информационной инфраструктуры Оператора, выявленные техническими средствами защиты информации, применяемыми Оператором или провайдерами услуг связи;
  - информации о компьютерных атаках, направленных на объекты информационной инфраструктуры РЦ, Участников и (или) Клиентов Участников, направляемой Субъектами Системы в рамках информационного взаимодействия;
  - информации об операциях/попытках осуществления операций по Переводу, совершенных в результате несанкционированного доступа к инфраструктуре Устройств приема платежей;
  - сведений об обращении Плательщика в правоохранительные органы при их наличии;
  - сведений о предпринятых и (или) предпринимаемых мерах для противодействия выявленным компьютерным атакам, направленным на объекты информационно инфраструктуры РЦ, Участников и (или) Клиентов Участников, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия Клиента, полученных Оператором в рамках информационного обмена от Субъектов Системы.
- рассматривает все случаи и (или) попытки осуществления переводов денежных средств без согласия Клиента, вызванные компьютерными атаками, направленными на объекты информационной инфраструктуры Субъектов

Системы и (или) Клиентов Участников, выявленные Оператором самостоятельно или полученные Оператором от провайдеров услуг, РЦ и Участников;

- использует полученную о компьютерных атаках информацию применительно к информационной инфраструктуре Оператора в целях противодействия осуществлению переводов денежных средств без согласия Клиента;
- в случае необходимости, запрашивает у Субъектов Системы дополнительную информацию, а также вправе создать рабочую группу для разработки и реализации мер, направленных на предотвращение и устранение воздействия компьютерной атаки, направленной на объекты информационной инфраструктуры РЦ, Участников и (или) Клиентов Участников.

11.9.3.3. Порядок реализации мер по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры Оператора и (или) Клиентов Участников, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия Клиента Участника.

Оператор реализует меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры Оператора и (или) Клиентов Участников, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия Клиента Участника в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 08.08.2017 3 822-ст «Об утверждении национального стандарта».

11.9.3.4. Порядок использования информации о переводах денежных средств без согласия клиента для выявления Операций, соответствующих признакам осуществления переводов денежных средств без согласия Клиента:

- выявление переводов денежных средств без согласия Клиента Участника, соответствующих признакам осуществления переводов денежных средств без согласия клиента, осуществляется Оператором с использованием информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, формируемой Банком России (далее – База данных);
- в целях получения Базы данных, Оператором обеспечивается подключение к автоматизированной системе обработки инцидентов Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России – Личный кабинет участника АСОИ ФинЦЕРТ;
- База данных подлежит загрузке в систему фрод-мониторинга;
- выявление Операций, в том числе Межсистемных Операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, содержащимся в Базе данных, производится в автоматическом режиме при обработке Оператором, выполняющим функции ОЦ, запроса на разрешение проведения Операции;
- в случае выявления при обработке запроса на разрешение проведения Операции совпадений с информацией, содержащейся в Базе данных, в автоматическом режиме производится отказ в совершении Операции.

11.9.3.5. Порядок осуществления анализа Операций, соответствующих признакам осуществления переводов денежных средств без согласия Клиента Участника, в рамках Системы:

- Оператор с учетом архитектуры Системы и специфики и характера Операций, проводимых в рамках Системы, устанавливаются следующие признаки осуществления переводов денежных средств без согласия Клиента Участника,

указывающие на несоответствие характера, и (или) параметров, и (или) объема проводимой Операции, Операциям, обычно проводимым Клиентом Участника:

- запросы разрешения проведения Операции по переводу денежных средств, содержащие повторяющиеся или похожие реквизиты в течение коротких временных промежутков;
- запросы разрешения проведения Операции по переводу денежных средств, содержащие нехарактерные суммы Операции для данного Клиента Участника;
- запросы разрешения проведения Операции по переводу денежных средств, совершающиеся в нехарактерное время или в нехарактерном месте для данного Клиента Участника.

– выявление Операций по переводу денежных средств без согласия Клиента Участника, соответствующих признакам осуществления переводов денежных средств без согласия клиента, осуществляется Оператором в автоматическом режиме посредством системы фрод-мониторинга;
– в случае выявления при проверке правил, определенных в системе фрод-мониторинга, Операции по переводу денежных средств без согласия Клиента Участника производятся следующие действия:

- системой в автоматическом режиме формируется отрицательный результат проверки и направляется Плательщику отказ в авторизации;
- системой в автоматическом режиме формируется сообщение, содержащее код ошибки, и незамедлительно направляется руководителю подразделения информационной безопасности посредством электронной почты;
- по факту получения сообщения, содержащего код ошибки, проводится расследование в целях подтверждения попытки совершения Операции без согласия Клиента либо подтверждения попытки совершения операции вследствие ошибочных действий Клиента Участника.

11.9.4. РЦ при реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия Клиента Участника должен:

11.9.4.1. Реализовывать меры по противодействию осуществлению переводов денежных средств без согласия Клиента (Участника) посредством построения системы защиты информации, направленной на защиту информации при осуществлении переводов денежных средств от неправомерного доступа, уничтожения, модифицирования, в том числе применения организационных мер защиты информации и технических средств защиты информации, включая средства защиты от воздействия вредоносного кода, в соответствии с требованиями, установленными Правилами.

11.9.4.2. Выявлять компьютерные атаки, направленные на объекты информационной инфраструктуры Субъектов Системы и (или) Клиентов Участников, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия Клиента Участника. В целях выявления компьютерных атак необходимо:

– обеспечить применение технических средств защиты информации, позволяющих осуществлять мониторинг и контроль содержимого сетевого трафика, а также регистрацию событий, связанных с результатами мониторинга и контроля содержимого сетевого трафика;
– при выборе провайдеров услуг связи предъявлять к ним требования об обязательном применении технических средств защиты информации на уровне провайдера;
– осуществлять взаимодействие при обмене информацией об инцидентах защиты информации с Субъектами Системы в порядке, установленном Правилами.

11.9.4.3. Рассматривать случаи и (или) попытки осуществления переводов денежных средств без согласия Клиента Участника, вызванные компьютерными атаками,

направленными на объекты информационной инфраструктуры Субъектов Системы и (или) Клиентов Участников:

- осуществлять сбор, аккумулирование и изучение:
  - информации о компьютерных атаках, направленных на объекты информационной инфраструктуры РЦ, выявленные техническими средствами защиты информации, применяемыми РЦ или провайдером услуг связи;
  - информации о компьютерных атаках, направленных на объекты информационной инфраструктуры Субъектов Системы и (или) Клиентов Участников, направляемой Субъектами Системы в рамках информационного взаимодействия;
  - сведений об обращении Плательщиков (Клиентов Участников) или Участников в правоохранительные органы при их наличии;
  - сведений о предпринятых и (или) предпринимаемых мерах для противодействия выявленным компьютерным атакам, направленным на объекты информационной инфраструктуры Субъектов Системы и (или) Клиентов Участников, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия Клиента, полученных в рамках информационного обмена от Субъектов Системы.
- использовать полученную о компьютерных атаках информацию применительно к информационной инфраструктуре РЦ в целях противодействия осуществлению переводов денежных средств без согласия Клиента.

11.9.4.4. Реализовывать меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры РЦ, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия Клиента Участника в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 08.08.2017 3 822-ст «Об утверждении национального стандарта».

11.9.4.5. Использовать информацию о переводах денежных средств без согласия клиента для выявления Операций, соответствующих признакам осуществления переводов денежных средств без согласия Клиента (Участника), содержащуюся в Базе данных, формируемой Банком России (в целях получения указанной базы данных требуется обеспечить подключение к автоматизированной системе обработки инцидентов Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России – Личный кабинет участника АСОИ ФинЦЕРТ).

11.9.4.6. Осуществлять анализ операций, соответствующих признакам осуществления переводов денежных средств без согласия Клиента (Участника), в рамках Системы посредством проведения проверки Реестра распоряжений, получаемого от Оператора, выполняющего функции ПКЦ, на основании которого производится списание денежных средств со Счетов Участников, а также иных переводов денежных средств с указанных счетов на предмет совпадения содержащейся в них информации о получателе денежных средств с Базой данных, формируемой Банком России.

11.9.5. Участники при реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия Клиента должны:

11.9.5.1. Выявлять Операции по переводу, соответствующие признакам осуществления перевода денежных средств без согласия клиента, в том числе, совершенные в результате несанкционированного доступа к объектам информационной инфраструктуры Участника посредством следующего:

- получения информации о таких переводах от Клиентов;

– проведения проверки переводов денежных средств, осуществляемых со счетов Клиентов, на предмет совпадения содержащейся в них информации о получателе денежных средств с Базой данных, формируемой Банком России (в целях получения указанной базы данных требуется обеспечить подключение к автоматизированной системе обработки инцидентов Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России – Личный кабинет участника АСОИ ФинЦЕРТ).

11.9.5.2. Выявлять компьютерные атаки, направленные на объекты информационной инфраструктуры Субъектов Системы и (или) Клиентов Участников, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия Клиента. В целях выявления компьютерных атак необходимо:

– обеспечить применение технических средств защиты информации, позволяющих осуществлять мониторинг и контроль содержимого сетевого трафика, а также регистрацию событий, связанных с результатами мониторинга и контроля содержимого сетевого трафика;
– при выборе провайдеров услуг связи предъявлять к ним требования об обязательном применении технических средств защиты информации на уровне провайдера;
– осуществлять взаимодействие при обмене информацией об инцидентах защиты информации с Субъектами Системы в порядке, установленном Правилами.

11.9.5.3. Осуществлять сбор технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры Субъектов Системы и (или) Клиентов Участников, при их наличии, посредством аккумулирования и изучения:

– информации о компьютерных атаках, направленных на объекты информационной инфраструктуры, выявленные техническими средствами защиты информации, применяемыми Участником или провайдером услуг связи;
– информации о компьютерных атаках, направленных на объекты информационной инфраструктуры Субъектов Системы и (или) Клиентов Участников, направляемой Субъектами Системы в рамках информационного взаимодействия.

11.9.5.4. Осуществлять сбор сведений об обращении Клиентов в правоохранительные органы при их наличии.

11.9.5.5. Рассматривать случаи и (или) попытки осуществления переводов денежных средств без согласия Клиента, вызванные компьютерными атаками, направленными на объекты информационной инфраструктуры Субъектов Системы и (или) Клиентов Участников, выявленные самостоятельно или полученные от провайдеров услуг, Субъектов Системы, Клиентов.

11.9.5.6. Реализовывать меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры Субъектов Системы и (или) Клиентов Участника, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия Клиента в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 08.08.2017 3 822-ст «Об утверждении национального стандарта».

11.9.5.7. Определять во внутренних документах Участника, регламентирующих процедуры управления рисками, процедуры выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, на основе анализа характера совершаемых Клиентами Участника операций (осуществляемой клиентами деятельности) в соответствии с частью 5.1. статьи 8 Закона о НПС, в частности определить порядок проведения проверки получаемых от Оператора Реестров ПКЦ за операционный день на предмет содержания в них информации исключительно об Операциях по переводу

денежных средств, совершенных с использованием ЭСП, на основании которых производится списание денежных средств со счетов Плательщиков.

11.9.5.8. Использовать выявленную Участником информацию о технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры Участника и (или) его Клиентов, применительно к своей инфраструктуре в целях противодействия осуществлению переводов денежных средств без согласия Клиента.

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

- Банк России в порядке и в сроки, установленные Указанием Банка России № 4926-У 08.10.2018 «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента» (далее – Указание Банка России № 4926-У);
- Оператора во всех случаях в соответствии с порядком взаимодействия в рамках Системы в чрезвычайных ситуациях.

11.9.7. Оператор направляет информацию в Банк России в виде электронных сообщений посредством Личного кабинета участника АСОИ ФинЦЕРТ (в случае недоступности технической инфраструктуры (автоматизированной системы) Банка России – с использование резервного способа взаимодействия: электронная почта fincert@cbr.ru; телефонный номер 8 (495) 772-70-90) по форме первичного, промежуточного и окончательного уведомления согласно Указанию Банка России № 4926-У.

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

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

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

Приложение № 1 к Правилам

Т А Р И Ф Ы

Платежной системы «КП Ритейл»

№ п/п	Наименование услуги	Стоимость
1	Конфигурация Участника	100 000 рублей + НДС
2	Обработка платежных операций по переводу денежных средств	0,07% от суммы платежей за расчетный месяц НДС не облагается
3	Подготовка и предоставление отчетов по операциям с Банковскими картами по запросу Участника	100 рублей/отчет НДС не облагается
4	Проведение по запросу Участника мероприятий, связанных с опротестованием Операций	120 рублей/ мероприятие НДС не облагается