ПРАВИЛА

Платежной системы «ХЕЛЛО»
(Редакция № 6)

Утверждены Решением единственного участника
Общества с ограниченной ответственностью «ХЕЛЛО»
(Решение № 03/03/23 от «03» марта 2023 г.)

Генеральный директор _____Фарбяж Р.А.

г. Москва

Введение.

Платежная система «ХЕЛЛО» (далее – «Платежная система», «ПС», «ПС ХЕЛЛО», «Система») представляет собой сообщество организаций (оператор платежной системы, операторы услуг платежной инфраструктуры, участники) объединенных единым информационным пространством и взаимодействующих в соответствии с настоящими Правилами Платежной системы «ХЕЛЛО» в целях осуществления переводов денежныхсредств, в том числе электронных денежных средств. Наименование на английском языке – Payment system HELLO.

Настоящие Правила Платежной системы «ХЕЛЛО» разработаны Обществом с ограниченной ответственностью «Хелло» - Оператором Платежной системы «ХЕЛЛО». Настоящие Правила Платежной системы «ХЕЛЛО» определяют условия участия в Платежной системе «ХЕЛЛО», осуществления перевода денежных средств, в том числе трансграничного перевода денежных средств, оказания услуг платежной инфраструктуры и иные условия, определяемые оператором платежной системы в соответствии с Федеральным законом от 27.06.2011 г. № 161-ФЗ «О национальной платежной системе» (далее – Закон о НПС) и иными нормативными актами БанкаРоссии.

Настоящие Правила не являются публичной офертой. Оператор платежной системы «ХЕЛЛО» вправе отказать в заключении договора участия без объяснения причин.

Правила системы разрабатывает и вводит в действие оператор платежной системы. Регулирование организационного и технологического взаимодействия между участниками платежной системы, установление стандартов безопасности и управление рисками является исключительной прерогативой оператора платежной системы. Требования в названных областях являются одинаковыми для всех субъектов платежной системы.

Сторонами Правил являются Оператор Платежной системы «ХЕЛЛО», Субъекты Платежной системы «ХЕЛЛО», операторы платежных систем, отвечающие требованиям Правил и Федеральным Закона о НПС, подписавшие соответствующий договор присоединения к Правилам, при условии, что данные лица принимают условия Правил в целом, в соответствии со ст. 428 Гражданского кодекса РФ. Субъекты Платежной системы «ХЕЛЛО», операторы Платежной системы «ХЕЛЛО» гарантируют, что обладают необходимой правоспособностью, а равно всеми правами и полномочиями, необходимыми идостаточными для присоединения к Правилам и исполнения обязательств в соответствии с их условиями.

Правила и тарифы, являющиеся частью Правил (Приложение№1), публикуются в открытом доступе на официальном сайте Оператора Платежной системы «ХЕЛЛО» в информационно-телекоммуникационной сети «Интернет» по адресу: www.hellopay.online

С О Д Е Р Ж А Н И Е

Введение

1. Термины и определения
2. Субъекты Платежной системы и требования к ним
2.1. Оператор Платежной системы «ХЕЛЛО». Права и обязанности
2.2. Участники Платежной системы «ХЕЛЛО». Права и обязанности
2.3. Операционный центр Платежной системы «ХЕЛЛО». Права и обязанности
2.4. Платежный клиринговый центр Платежной системы «ХЕЛЛО». Права и обязанности
2.5. Расчетный центр Платежной системы «ХЕЛЛО». Права и обязанности
3. Основные принципы договорных взаимоотношений
3.1. Основные положения договора участия между Оператором и Участником
3.2. Основные положения договора между Оператором и Расчетным центром
3.3. Основные положения договора между Участником и Расчетным центром
4. Порядок взаимодействия между Субъектами платежной системы
4.1. Общие положения
4.2. Взаимодействие Оператора с Участниками
4.3. Взаимодействие между Оператором и Расчетным центром
4.4. Взаимодействие между Расчетным центром и Участником
5. Порядок присоединения и участия в платежной системе Субъектов платежной системы
5.1. Порядок привлечения Операторов услуг платежной инфраструктуры, ведение перечня Операторов услуг платежной инфраструктуры
5.2. Категории Участников и Критерии участия (прямого и косвенного) в Платежной системе «ХЕЛЛО»
5.3. Порядок присоединения организации к Системе и наделение ее статусом Участника (прямого/косвенного)
5.4. Критерии приостановления и прекращение участия в Платежной системе «ХЕЛЛО»
5.5. Порядок присвоения идентификационного номера
5.6. Партнеры Платежной системы «ХЕЛЛО».
6. Порядок осуществления расчетов по операциям, совершаемым в соответствии с Правилами, и между Субъектами платежной системы
6.1. Применяемые формы безналичных расчетов
6.2. Порядок осуществления перевода денежных средств в рамках Платежной системы «ХЕЛЛО», включая моменты наступления его безотзывности, безусловности и окончательности. Отзыв Переводов. Возврат (аннулирование) Переводов
6.3. Осуществление денежных переводов через Банкомат, Платежный терминал
6.4. Предоставление информации об операциях, совершенных через пункты обслуживания клиентов, банкоматы и платежные терминалы
6.5. Порядок сопровождения перевода денежных средств сведениями о Плательщике
6.6. Порядок осуществления платежного клиринга и расчетов
6.7. Порядок обеспечения исполнения обязательств Участников по переводу денежных средств
6.8. Порядок оплаты услуг по переводу денежных средств
7. Система управления рисками в Платежной системе «ХЕЛЛО»
7.1. Модель управления рисками
7.2. Мероприятия по управлению рисками
7.3. Способы управления рисками
7.4. Методика анализа рисков

7.5. Организационная структура системы управления рисками
7.6. Доведение до органов управления рисками Оператора сведений о рисках
8. Порядок обеспечения бесперебойности функционирования Платежной системы «ХЕЛЛО»
8.1. Терминология раздела 8 Правил
8.2. Показатели бесперебойности Платежной системы «ХЕЛЛО»
8.3. Управление непрерывностью функционирования Платежной системы «ХЕЛЛО»
8.4. Требования к уровню бесперебойности оказания операционных услуг
8.5. Требования к уровню бесперебойности оказания расчетных услуг
8.6. Требования к уровню бесперебойности оказания услуг платежного клиринга
8.7. Уровень риска нарушения БФПС
8.8. Требования к содержанию деятельности по обеспечению БФПС, осуществляемой Оператором, Участниками, Операторами услуг платежной инфраструктуры
8.9. Порядок информационного взаимодействия Субъектов платежной системы и документационного обеспечения из деятельности по обеспечению БФПС
8.10. Контроль за соблюдением Операторами услуг платежной инфраструктуры и Участниками Платежной системы порядка обеспечения БФПС
8.11. Порядок изменения операционных и технологических средств и процедур
9. Порядок оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией
10. Временной регламент функционирования Платежной системы «ХЕЛЛО»
11. Порядок обмена информацией, необходимой для управления рисками
12. Обеспечение защиты информации в Платежной системе «ХЕЛЛО»
13. Защищаемая в Платежной системе «ХЕЛЛО» информация
14. Требования к обеспечению защиты информации
15. Использование средств криптографической защиты информации
16. Требования к обеспечению защиты информации от воздействия вредоносных кодов
17. Обеспечение защиты персональных данных в Платежной системе «ХЕЛЛО»
18. Информационное взаимодействие при выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств
19. Обеспечение банковской и коммерческой тайны в Платежной системе «ХЕЛЛО»
20. Порядок взаимодействия в рамках Платежной системы «ХЕЛЛО» в чрезвычайных и нестандартных ситуациях
21. Порядок взаимодействия в рамках Платежной системы «ХЕЛЛО» в спорных ситуациях, порядок досудебного разрешения споров между Субъектами платежной системы
22. Порядок разрешения споров между Субъектами платежной системы при участии комиссии
23. Порядок разрешения спорных ситуаций в судебном порядке
24. Перечень платежных систем, с которыми осуществляется взаимодействие, и порядок такого взаимодействия
25. Порядок осуществления контроля за соблюдением Правил Платежной системы «ХЕЛЛО»
26. Порядок предоставления Участниками и Операторами услуг платежной инфраструктуры информации о своей деятельности Оператору

27. Действия и меры принуждения, применяемые Оператором в отношении подконтрольных организаций в случае нарушения ими обязательств, принятых на себя в соответствии с настоящими Правилами
28. Ответственность за несоблюдение Правил
29. Порядок изменения Правил Платежной системы «ХЕЛЛО»

П Р И Л О Ж Е Н И Я

Приложение №1 «Тарифы Платежной системы «ХЕЛЛО»»

Приложение №2 «Регламент электронного документооборота»

Приложение №3 «Перечень документов, предоставляемый Участниками Оператору Платежной системы «ХЕЛЛО»»

Приложение №4 «Форма договора участия в Платежной системы «ХЕЛЛО»(для прямого Участника)»

Приложение №5 «Форма договора участия в Платежной системы «ХЕЛЛО»(для косвенного Участника)»

Приложение №6 «Протокол внесения изменений в Правила»

Приложение №7 «Положение по управлению рисками и бесперебойности функционирования ПС «ХЕЛЛО»

Приложение №8 Анкета «Выполнение требований по обеспечению защиты информации»

Приложение №9 «Сведения о выявленных Инцидентах, связанных с нарушением бесперебойности функционирования Платежной системы»

1. Термины и определения

Для целей настоящих Правил платежной системы используются следующие термины и определения:

Адресный перевод — Перевод, при отправлении которого указывается наименование Участника-исполнителя, с точностью до конкретного пункта выдачи Перевода.

Аннулирование перевода — отмена Перевода, не выплаченного Получателю, производимая по инициативе Отправителя или по инициативе Оператора.

Банкомат – электронный программно-технический комплекс Участника платежной системы, предназначенный для совершения без участия уполномоченного работника Участника денежного перевода физическими лицами, путем приема наличных денежных средств и/или банковских карт, составления документов, подтверждающих соответствующие операции, а также выдачи наличных денежных средств.

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

Бивалютный перевод – осуществляемый в рамках Платежной системы «ХЕЛЛО» перевод денежных средств, позволяющий осуществить автоматическую конвертацию по курсу Платежной системы «ХЕЛЛО» из одной валюты в другую. Используемые валюты: Российский рубль (RUB), Азербайджанский манат (AZN), Алжирский динар (DZD), Армянский драм (AMD), Бахрейнский динар (BHD), Белорусский рубль (DYN), Бразильский реал (BRL), Вьетнамский донг (VND), Гонконгский доллар (HKD), Грузинский лари (GEL), Дирхамы ОАЭ (AED), Доллар США (USD), ЕВРО (EUR), Египетский фунт (EGP), Индийская рупия (INR), Индонезийская рупия (IDR), Казахстанский тенге (KZT), Китайский юань (CNY), Киргизский сом (KGS), Молдавский лей (MDL), Оманский риал (OMR), Сингапурский доллар (SGD), Таджикский сомони (TJS), Турецкая лира (TRY), Узбекский сум (UZS), Южноафриканский рэнд (ZAR).

Валюта Перевода — валюта Российской Федерации или иностранная валюта из числа установленных Оператором для проведения Переводов.

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

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

Клиент – плательщик, получатель, представитель.

Комиссия за перевод — денежное вознаграждение субъектов Системы за осуществление Перевода, уплачиваемое Плательщиком через Участника-отправителя в момент отправления Перевода дополнительно к Сумме перевода.

Контрольный номер перевода (КНП) – уникальная последовательность символов, присваиваемая Оператором каждому переводу денежных средств при его отправлении, и являющаясяодним из реквизитов перевода.

Нестандартная ситуация – это ситуация, возникающая в результате отклонений от оптимального или текущего режима деятельности Субъектов Платежной системы. Нестандартная ситуация не влечет приостановление функционирования Платежной системы.

Обмен электронными сообщениями – получение операционным центром электронных сообщений, содержащих распоряжения участников платежной системы, передача указанных сообщений в платежный клиринговый центр, расчетный центр, а также передача извещений (подтверждений) о приеме и об исполнении распоряжений участников платежной системы.

Оператор платежной системы/Оператор – Общество с ограниченной ответственностью «ХЕЛЛО» (ОГРН 1167746654085), определяющее Правила платежной системы, а так же выполняющее иные обязанности, предусмотренные Законом о НПС и Правилами платежной системы.

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

Операционный центр – Общество с ограниченной ответственностью «ХЕЛЛО», обеспечивающее в рамках платежной 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, содержащих распоряжения Участников платежной системы (далее – операционные услуги).

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

Оператор электронных денежных средств/ОЭДС- оператор по переводу денежных средств, осуществляющий перевод электронных денежных средств без открытия банковского счета (перевод электронных денежных средств).

Перевод – осуществляемый в рамках Платежной системы «ХЕЛЛО» перевод денежных средствв соответствии с применяемыми формами безналичных расчетов, посредством зачисления денежных средств на банковский счет получателя средств, выдачи получателю средств наличных денежных средств либо учета денежных средств в пользу получателя средств без открытия банковского счета при переводе электронных денежных средств.

Перевод денежных средств – действия оператора по переводу денежных средств, в рамках применяемых форм безналичных расчетов по предоставлению Получателю средств денежных средств Плательщика.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (Отправителю, Получателю, Представителю), доступная Участнику, принявшему данную информацию в обработку.

Платежный клиринговый центр (ПКЦ) – Общество с ограниченной ответственностью «ХЕЛЛО», созданное в соответствии с законодательством Российской Федерации, обеспечивающее в рамках платежной системы прием к исполнению распоряжений Участников платежной системыоб осуществлении перевода денежных средств и выполнение иных действий, предусмотренных Законом о НПС (далее – услуги платежного клиринга).

Плательщик/Отправитель – физическое или юридическое лицо, дающее поручение Участнику на осуществление в рамках Платежной системы операции для целей перевода денежных средств.

Получатель – физическое или юридическое лицо, для перевода денежных средств которому, совершена операция по переводу денежных средств с использованием технологий, предусмотренных настоящими Правилами.

Представитель – представитель Получателя, обратившийся в Пункт обслуживания за получением Перевода на основании нотариально удостоверенной доверенности на получение Перевода, либо генеральной нотариально удостоверенной доверенности.

Платежный терминал – электронный программно-технический комплекс Участника платежной системы, предназначенный для осуществления без участия уполномоченного работника Участника денежного перевода, путем приема наличных денежных средств и/или банковских карт иных платежных систем, а также для составления документов, подтверждающих соответствующие операции.

Пункт обслуживания – подразделения Участников, осуществляющие операции по Переводам. Списки Пунктов обслуживания доступны для ознакомления на сайте www.hellopay.online

Партнеры Платежной системы «ХЕЛЛО» (Партнеры) – юридические лица, в т.ч. имеющие лицензию (разрешение) на осуществление переводов денежных средств, почтовых переводов в соответствии с законодательством страны своего местонахождения, не присоединившиеся к Правилам Системы в целом, осуществляющие перевод в качестве клиентов Участников, в соответствии с Правилами Системы и соответствующими соглашениями, заключенными с Участниками.

Платежные методы (способы) – методы (способы) оплаты, используемые при обеспечении осуществления Переводов и предоставляемые Участникам платежной системы Оператором платежной системы на основании отдельно заключенных с Партнерами Договоров и соглашений, включая: а) пополнение банковских карт, электронных средств платежа Плательщикаи лицевых счетов пользователя услуг связи, абонента; б) расчеты, переводы с использованием реквизитов банковских карт, банковских карт Visa, MasterCard/Maestro, МИР (эквайринг, интернет-эквайринг) и других платежных систем, с использованием электронных денежных средств на основании распоряжения пользователя услуг связи, абонента, с использованием предоплаченных карт, интернет-банкинга; в) иные электронные средства платежа, терминалы и иные устройства самообслуживания, системы денежных переводов.

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

Реестр платежей – документ или совокупность документов, содержащих информацию, необходимую Расчетному центру для осуществления расчетов в рамках платежной системы за определенный период времени, составляемый и предоставляемый Оператором платежной системы в электронной форме.

Спорная ситуация — это ситуация, которая требует анализа обстоятельств, на которые ссылаются все стороны, возникшего вопроса. Решение по спорной ситуации принимается в рабочем порядке и/или по итогам работы комиссии по разрешению спорной ситуации.

Субъекты платежной системы/Субъекты ПС – оператор платежной системы, операторы услуг платежной инфраструктуры и участники платежной системы.

Сумма Перевода — сумма денежных средств, подлежащая выплате/зачислению Получателю Участником-исполнителем.

Счет – банковский счет, предназначенный для проведения расчетов по операциям, совершенным в рамках платежной системы. Открывается Расчетным центром Участнику платежной системы на условиях договора, заключаемого между Участником платежной системы и Расчетным центром.

Согласованный канал связи – а) средства и способы, определенные Оператором и Участником для информационного обмена и расчетов: электронный способ информационного обмена и расчетов с применением Программного комплекса «ХЕЛЛО», указанного в Приложении № 2 к Правилам; б) средства и способы, согласованные в письменном виде Оператором и Субъектами ПС (за исключением Участников) для информационного обмена и расчетов. Субъекты ПС самостоятельно на ежедневной основе осуществляют проверку информации, переданной Оператором по согласованным каналам связи.

Тарифы – документ, устанавливающий размер платы за услуги по переводу денежных средств, в рамках Платежной системы (Приложение 1 к настоящим Правилам). Тарифы размещены на сайте Оператора в сети Интернет по адресу: www.hellopay.online

Тарифы для Клиентов Платежной системы «ХЕЛЛО» (Тарифы для Клиентов) – установленные Оператором размеры комиссии, взимаемой с Плательщика/Отправителя за оказание услуг по осуществлению Переводов денежных средств через Платежную систему «ХЕЛЛО». Тарифы для клиентов размещены на сайте Оператора в сети Интернет по адресу: www.hellopay.online

Тарифы для Участников Платежной системы «ХЕЛЛО» (Тарифы для Участников) – установленные Оператором размеры комиссий, уплачиваемых Участникам за обслуживание Клиентов при осуществлении Переводов денежных средств в рамках Платежной системы «ХЕЛЛО».

Транзитный перевод – перевод денежных средств, прием и выплата которого осуществляется за пределами Российской Федерации.

Трансграничный перевод – перевод денежных средств, при осуществлении которого Плательщик либо Получатель средств находится за пределами Российской Федерации.

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

Управление непрерывностью функционирования Платежной системы – выявление оказания услуг платежной инфраструктуры, не соответствующих требованиям к оказанию услуг, обеспечению функционирования Платежной системы «ХЕЛЛО» 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 ихоказания в течение периодов времени, установленных Оператором Платежной системы в настоящих Правилах Платежной системы «ХЕЛЛО».

Управление рисками в Платежной системе – организация системы управления рисками в Платежной системе, оценке и управлению рисками в Платежной системе.

Участники платежной системы/Участники – операторы по переводу денежных средств (в том числе операторы по переводу электронных денежных средств), иностранные центральные (национальные) банки, иностранные банки, имеющие право на осуществление денежных переводов, в соответствии с законодательством страны, на территории которой они зарегистрированы, присоединившиеся к Правилам Системы и открывшиесчета в РЦ / у прямого Участника, в целях оказания Услуг Платежной системы «ХЕЛЛО».

Участник-отправитель – сторона, принимающая от Отправителя поручение и денежные средства в целях осуществления Перевода.

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

Услуги Платежной системы «ХЕЛЛО» - Осуществление перевода денежных средств (электронных денежных средств), в том числе трансграничные переводы и переводы с использованием электронных средств платежа:

а) от физических лиц для выплаты наличными денежными средствами физическим лицам без открытия счета;

б) от физических лиц с целью увеличения/уменьшения остатка электронных денежных средств;

в) от физических лиц для зачисления на счета физических лиц в кредитных организациях;

г) от физических лиц юридическим лицам/индивидуальным предпринимателям в счет оплаты услуг;

д) от физических лиц юридическим лицам, при предоставлении полных реквизитов платежа;

е) от юридических лиц для выплаты физическим лицам, при предоставлении полных реквизитов платежа;

ж) от юридических лиц юридическим лицам, при предоставлении полных реквизитов платежа.

Электронные денежные средства - денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица,предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа.

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

Чрезвычайная ситуация – это ситуация, возникающая внезапно, способная повлечь системные сбои и инциденты.

Настоящие термины имеют то же значение при использовании их во множественном числе и написании строчными буквами.

2. Субъекты Платежной системы и требования к ним. Оператор платежной системы. Права и обязанности.

Оператор платежной системы совмещает свою деятельность с деятельностью Оператора услуг платежной инфраструктуры (за исключением Расчетного центра) на основании части 3 статьи 15 Закона о НПС.

2.1. Оператор Платежной системы «ХЕЛЛО». Права и обязанности.

2.1.1. Обязанности Оператора:

а. Создать единую концептуальную основу взаимодействий в Платежной системе и обеспечивать организационную и технологическую целостность Платежной системы, а также равноправный доступ операторов услуг платежной инфраструктуры в Платежную систему.

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

в. Осуществлять привлечение Операторов услуг платежной инфраструктуры (за исключением случаев, когда Оператор платежной системы совмещает функции Оператора услуг платежной инфраструктуры), которые находятся на территории Российской Федерации и соответствуют требованиям, установленным законодательством Российской Федерации и Правилами, обеспечивать контроль за оказанием услуг платежной инфраструктуры, вести перечень операторов услуг платежной инфраструктуры.

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

д. Организовать систему управления рисками в платежной системе, осуществлять мониторинг, анализ, оценку и управление рисками в соответствии с требованиями законодательства Российской Федерации, нормативных актов Банка России и Правилами.

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

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

з. Обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, в соответствии с требованиями к защите указанной информации, установленными Правительством Российской Федерации, а также в соответствии с нормативными документами, указанными в п. 14.1. Правил.

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

к. Указывать свой регистрационный номер при предоставлении информации о платежной системе.

л. Привлекать в качестве Расчетных центров кредитные организации, которые не менее одного года осуществляют перевод денежных средств по открытым в этой кредитной организации банковским счетам.

м. Обеспечивать контроль за оказанием услуг платежной инфраструктуры Участникам платежной системы.

н. Письменно уведомлять Участников платежной системы о необходимости смены Расчетного центра не менее чем за 65 (Шестьдесят пять) календарных дней, за исключением по осуществлению банковских операций, влияющей на исполнение обязательств в качестве Расчетного центра, либо в иных случаях, вызванных требованиями контролирующих органов, о

чем Оператор уведомляет Участников незамедлительно по факту известности ему данного обстоятельства или получения уведомления от Расчетного центра.

о. Оператор платежной системы несет ответственность за реальный ущерб, причиненный Участникам платежной системы вследствие неоказания (ненадлежащего оказания) услуг платежной инфраструктуры в случае их осуществления (за исключением услуг Расчетного центра), при этом ответственность Оператора платежной системы за реальный ущерб ограничена размером неустойки, за исключением случаев умышленного неоказания (ненадлежащего оказания) услуг платежной инфраструктуры (за исключением услуг Расчетного центра). Размер неустойки определяется как размер реального ущерба, причиненного Участнику платежной системы. Факт причинения и размер реального ущерба доказывается Участником самостоятельно.

п. Оператор платежной системы устанавливает предельные размеры (лимиты) обязательств Участников платежной системы.

р. Оператор информирует Участников о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры в день такого приостановления (прекращения) любым из следующих способов:

- путем размещения на официальном сайте www.hellopay.online в информационно-телекоммуникационной сети «Интернет»;
- путем направления уведомления по электронной почте, представленной Участником.

2.1.2. Права Оператора:

а. В одностороннем порядке вносить изменения в Правила с соблюдением условий, установленных Законом о НПС, в порядке, определенными настоящими Правилами.

б. Не раскрывать информацию о требованиях к защите информации и информацию, доступ к которой ограничен в соответствии с федеральным законодательством и настоящими Правилами;

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

г. Определять Расчетный центр для Участника платежной системы;

д. Размещать в публичном доступе перечень Участников Платежной системы;

е. Приостанавливать и прекращать участие Участников платежной системы в платежной системе в порядке и по основаниям, установленным настоящими Правилами;

ж. Письменно уведомлять Участников платежной системы о необходимости смены Расчетного центра в более сокращенные сроки, чем установлены в настоящих Правилах, в случае наличия объективной информации о наличии риска невыполнения Расчетным центром своих обязательств по проведению расчетов;

з. Самостоятельно осуществлять приостановление операций по переводу денежных средств, осуществляемых Участниками платежной системы и Плательщиками, в отношении которых Оператором получена информации о принятии уполномоченными государственными или иными регулирующими органами решений о приостановлении операций по Счетам, о наложении ареста наденежные средства, размещенные на Счетах, отзыве лицензии на осуществление банковских операций, иных обстоятельствах, препятствующих Участнику платежной системы осуществлять перевод денежных средств.

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

к. Расширять перечень Услуг Платежной системы «ХЕЛЛО», устанавливать и изменять требования к качеству оказываемых Участниками Услуг Платежной системы «ХЕЛЛО», обязательные для всех Участников.

2.2. Участники Платежной системы «ХЕЛЛО». Права и обязанности.

Участниками Платежной системы «ХЕЛЛО» являются операторы по переводу денежных средств (в том числе операторы по переводу электронных денежных средств), иностранные центральные (национальные) банки, иностранные банки, имеющие право на осуществление денежных переводов, в соответствии с законодательством страны, на территории которой они зарегистрированы, присоединившиеся к Правилам Системы и открывшие счета в РЦ/у прямого Участника, в целях оказания Услуг Платежной системы «ХЕЛЛО».

В Платежной системе «ХЕЛЛО» предусматривается прямое и косвенное участие:

- Прямое (прямые Участники) - предполагает открытие Участниками корреспондентских счетов (ЛОРО – счетов) в Расчетном центре Системы.
- Косвенное (косвенные Участники) - предполагает открытие Участниками корреспондентских счетов (ЛОРО – счетов) у прямых Участников.

2.2.1. Право Участников:

а. Участвовать в других платежных системах. При условии наличия согласия Клиента, осуществлять денежный перевод, в том числе через иные платежные системы, участником которых он является, а также через операторов по переводу денежных средств, с которыми участник осуществляет сотрудничество на основании отдельно заключенных договоров. При этом, Участник гарантирует, что права Клиента не будут ущемлены.

б. Устанавливать размер оплаты услуг по переводу денежных средств (сверх комиссии за Перевод, устанавливаемой Оператором) с соблюдением законодательства Российской Федерации, нормативных актов Банка России и, при условии уведомления о данном факте Оператора.

в. Взимать с Отправителей комиссионное вознаграждение за оказываемые в рамках Системы услуги в соответствии с заключаемым между ними договором с соблюдением законодательства Российской Федерации и нормативных актов Банка России.

г. В случае несогласия Участника с фактом осуществления операции по переводу денежных средств в рамках Системы направить Оператору письменный запрос об обстоятельствах осуществления операции по переводу денежных средств.

д. Косвенный Участник Системы имеет право приобрести статус прямого Участника, для чего ему необходимо открыть счет в РЦ Системы и подать письменное заявление Оператору, в свободной форме о своем намерении стать прямым Участником.

е. Использовать наименование Системы при размещении информационных/рекламных материалов Участника Системы в СМИ и иных источниках информации, при условии предварительного согласования условий мероприятий, содержания рекламно-информационных материалов и форм их использования с Оператором Системы.

2.2.2. Обязанности Участников:

а. Обеспечивать взаимодействие с Операционным центром платежной системы для получения информации о финансовых сообщениях в соответствии с особенностями осуществления платежного клиринга, предусмотренного правилами платежной системы.

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

в. Открыть Счет в Расчетном центре, определенном Оператором платежной системы. Контролировать достаточность денежных средств на счете в Расчетном центре, согласно размеру

лимита, рассчитанного Оператором. Косвенные Участники обязаны открыть счет у прямого Участника.

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

д. Обеспечить получение согласия на обработку (включая автоматизированную обработку) персональных данных физических лиц (отправителей и получателей денежных переводов).

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

ж. В случае отзыва лицензии, разрешения на осуществление деятельности Участника, а также обстоятельствах, которые могут ухудшить финансовое состояние Участника и/или возникновения обстоятельств, влияющих на бесперебойность осуществления деятельности Участника, сообщить о данном факте незамедлительно в день известности его наступления, но не позднее окончания рабочего дня наступления факта (в случаях привлечении Оператором операционного центра), по согласованным каналам связи.

з. В случае внесения изменений в учредительные документы, а также при изменении других данных Участника, сообщить об изменениях с приложением подтверждающих документов не позднее 5 (пяти) рабочих дней с даты их государственной регистрации или наступления данных изменений.

и. Самостоятельно разрабатывать свою методику анализа рисков в Платежной системе и предоставлять ее Оператору по мере внесения изменений, но не реже одного раза в год.

к. Перевод электронных денежных средств Участники осуществляют с учетом ограничений, предусмотренных Законом о НПС, а именно:

- В случае проведения оператором электронных денежных средств идентификации клиента - физического лица в соответствии с Федеральным законом от 7 августа 2001 года N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" использование электронного средства платежа осуществляется клиентом - физическим лицом при условии, что остаток электронных денежных средств в любой момент не превышает 600 тысяч рублей либо сумму в иностранной валюте, эквивалентную 600 тысячам рублей по официальному курсу Банка России. Указанное электронное средство платежа является персонифицированным;

- В случае непроведения оператором электронных денежных средств идентификации клиента - физического лица в соответствии с Федеральным законом от 7 августа 2001 года N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" использование электронного средства платежа осуществляется клиентом - физическим лицом при условии, что остаток электронных денежных средств в любой момент не превышает 15 тысяч рублей, за исключением случая, проведения упрощенной идентификации. Указанное электронное средство платежа является неперсонифицированным;

- В случае проведения оператором электронных денежных средств упрощенной идентификации клиента - физического лица в соответствии с Федеральным законом от 7 августа 2001 года N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" использование неперсонифицированного электронного средства платежа может осуществляться клиентом - физическим лицом при условии, что остаток электронных денежных средств в любой момент не превышает 60 тысяч рублей, а общая сумма переводимых электронных денежных средств с использованием такого

неперсонифицированного электронного средства платежа не превышает 200 тысяч рублей в течение календарного месяца;

- Общая сумма переводимых электронных денежных средств с использованием одного неперсонифицированного электронного средства платежа не может превышать 40 тысяч рублей в течение календарного месяца, за исключением случая проведения упрощенной идентификации.

л. Поддерживать в необходимом размере остатки на своих счетах, открытых в РЦ Системы (для прямого Участника) или у прямого Участника (для косвенного Участника) в целях осуществления расчета с другими Участниками Системы.

м. Обеспечивать защиту информации при осуществлении переводов денежных средств, в т.ч. в соответствии с требованиями, установленными Банком России. Обеспечить реализацию механизмов, направленных на соблюдение требований к обеспечению защиты информации при осуществлении переводов денежных средств, и контроль их соблюдения

н. По письменному запросу Оператора (поступившему в том числе с электронного адреса Оператора Системы), направлять Оператору информацию, документы, отчетность по установленным Оператором формам, а также, при необходимости, оригиналы или должным образом заверенные копии документов, подтверждающих осуществление физическими лицами операций в Системе и/или согласие клиентов на обработку их персональных данных Участниками и Оператором Системы, а также связываться с Отправителем/Получателем Перевода для получения дополнительной информации и/или копии удостоверяющего личность Отправителя /Получателя документа;

2.3. Операционный центр Платежной системы «ХЕЛЛО». Права и обязанности.

Операционный центр обеспечивает в рамках платежной 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.

2.3.1. Обязанности Операционного центра:

а. Обеспечить маршрутизацию авторизационных сообщений, передаваемых в режиме реального времени между Участниками платежной системы.

б. Обеспечивать информационное и технологическое взаимодействие между субъектами Платежной системы.

в. Получать электронные сообщения, содержащие распоряжение Участников платежной системы на осуществление перевода денежных средств и передавать указанные сообщения в Платежный клиринговый центр, в Расчетный центр, а также передавать извещения (подтверждения) о приеме и об исполнении распоряжений Участников платежной системы.

г. Обеспечивать предоставление Участникам платежной системы информации о финансовых сообщениях.

д. Обеспечивать регистрацию (интеграцию) Участников в Платежной системе и доступ к услугам по переводу денежных средств.

е. Обеспечивать обмен информацией, не являющейся авторизационными и финансовыми сообщениями.

ж. Операционный центр обеспечивает получение, обработку, предоставление и поддержание в актуальном состоянии информации, необходимой для проведения операций с применением Банкоматов и Платежных терминалов, в пунктах обслуживания, в соответствии с требованиями, установленными Оператором платежной системы и предоставляемой Участниками платежной системы.

з. Обеспечивать защиту обрабатываемой в соответствии с выполняемыми функциями Операционного центра информации о переводах денежных средств.

и. Не раскрывать третьим лицам сведения об операциях и о Счетах Участников платежной системы и их клиентов, полученные при оказании операционных услуг, за исключением передачи

информации в рамках Платежной системы, а также случаев, предусмотренных федеральными законами.

к. Нести ответственность за реальный ущерб, причиненный вследствие неоказания (ненадлежащего оказания) операционных услуг Участникам платежной системы, Платежно-клиринговому центру и Расчетному центру.

л. Обеспечивать прием аутентифицированных сообщений от Участников посредством проверки Электронной подписи.

м. Обеспечивать взаимную (двустороннюю) аутентификацию участников обмена электронными сообщениями

н. Обеспечивать сверку выходных электронных сообщений с соответствующими входными и обработанными сообщениями при осуществлении расчетов в Платежной системе.

о. В случае приостановления деятельности Операционного центра, отзыва лицензии Операционного центра, являющийся кредитной организацией, влияющих на бесперебойность осуществления деятельности Операционного центра, а также обстоятельствах, которые могут ухудшить финансовое состояние Операционного центра, сообщить Оператору Платежной Системы о данном факте незамедлительно в день известности наступления по согласованным каналам связи (в случаях привлечения Оператором Операционного центра).

п. В случае внесения изменений в учредительные документы, а также при изменении других данных, сообщить об изменениях с приложением подтверждающих документов не позднее 5 (пяти) рабочих дней с даты их государственной регистрации или наступления данных изменений, по согласованным каналам связи (в случаях привлечения Оператором Операционного центра).

2.4. Платежный клиринговый центр Платежной системы «ХЕЛЛО». Права и обязанности.

2.4.1. Обязанности Платежного клирингового центра:

а. Обеспечивать в рамках платежной системы прием к исполнению распоряжений Участников платежной системы об осуществлении перевода денежных средств и осуществлять проверку соответствия распоряжений Участников платежной системы установленным требованиям.

б. Передавать Расчетному центру подлежащие исполнению распоряжения Участников платежной системы.

в. Осуществлять контроль лимита межбанковских расчетов.

г. Определять платежные клиринговые позиции (на нетто-основе по каждой из валют расчета).

д. Рассчитывать вознаграждения за услуги, оказываемые Участниками платежной системы и Операционным центром платежной системы.

е. Обеспечивать выполнения требований безопасности в платежной системе в соответствии с Правилами.

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

з. Нести ответственность за убытки, причиненные Участникам платежной системы и Расчетному центру вследствие неоказания (ненадлежащего оказания) услуг платежного клиринга**.**

и. Заключать договор об оказании услуг платежного клиринга с участниками платежной системы, в форме присоединения (в случае привлечения Оператором Платежной системы Оператора платежной инфраструктуры для выполнения им функций платежного клирингового центра);

к. В случае приостановлении деятельности Платежного клирингового центра, отзыва лицензии, разрешения на осуществление деятельности Платежного клирингового центра, а также обстоятельствах, которые могут ухудшить его финансовое состояние и/или возникновения обстоятельств, влияющих на бесперебойность осуществления его деятельности, сообщить о данном факте незамедлительно в день известности его наступления Оператору Платежной

Системы по согласованным каналам связи (в случаях привлечения Оператором Платежного клирингового центра).

л. В случае внесения изменений в учредительные документы, а также при изменении других данных, сообщить об изменениях с приложением подтверждающих документов не позднее 5 (пяти) рабочих дней с даты их государственной регистрации или наступления данных изменений, по согласованным каналам связи (в случаях привлечения Оператором Платежного клирингового центра).

м. Обеспечивать защиту обрабатываемой в соответствии с выполняемыми функциями Платежного клирингового центра информации о переводах денежных средств

2.5. Расчетный центр Платежной системы «ХЕЛЛО». Права и обязанности.

Правила являются неотъемлемой частью договора оказания услуг между Оператором платежной системы и Расчетным центром. Условия правоотношений, взаимодействия между Оператором и Расчетным центром регулируются настоящими Правилами и договором, заключенным между Оператором и Расчетным центром.

2.5.1. Требования к Расчетному центру:

а. Расчетным центром платежной системы может выступать кредитная организация, созданная в соответствии с законодательством РФ, в том числе небанковская кредитная организация, находящаяся на территории Российской Федерации, осуществляющая не менее одного года деятельность по переводу денежных средств по открытым в этой кредитной организации банковским счетам.

б. Расчетный центр должен соответствовать следующим требованиям:

- наличие лицензии Банка России и иных правоустанавливающих документов (учредительные документы, сертификаты и т.п.), необходимых для осуществления соответствующей деятельности кредитной организации согласно действующему законодательству Российской Федерации;
- кредитная организация не менее 1 (Одного) года осуществляет перевод денежных средств по открытым в этой кредитной организации банковским счетам;
- финансовая устойчивость (размер уставного капитала не ниже, установленного законодательством Российской Федерации);

- наличие возможности оказывать расчетные услуги в соответствии с законодательством Российской Федерации и Правилами Системы;
- возможность осуществления деятельности в рамках системы в соответствии с Правилами системы.

в. Расчетный центр выполняет обязательные требования Банка России, в том числе требования по обеспечению мер по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

г. Расчетный центр обеспечивает банковскую тайну, защиту информации при осуществлении переводов денежных средств и персональных данных Плательщиков (в случае их получения и обработки) в соответствии с законодательством РФ.

д. Расчетный центр принимает условия функционирования Платежной системы, изложенные в Правилах в полном объеме, в том числе соглашается нести ответственность в соответствии с Правилами за нарушение Правил.

е. Расчетный центр имеет технологическую возможность быть подключенным к Платежной системе.

ж. Расчетный центр осуществляет свою деятельность в соответствии с нормативными актами Банка России, Правилами платежной системы и на основании договора, заключаемого с Оператором платежной системы, а также договоров банковского счета.

2.5.2. Обязанности Расчетного центра:

а. Не изменять без согласования с Оператором платежной системы положения, определяющие порядок, условия и сроки предоставления услуг Расчетного центра.

б. Уведомлять Оператора платежной системы о намерении прекращения деятельности по осуществлению банковских операций, влияющей на исполнение обязательств в качестве Расчетного центра, в срок не менее чем за 65 (шестьдесят пять) календарных дней, а также о намерении изменения тарифов предоставления услуг Расчетного центра, по ведению банковского счета Участников не менее чем за 20 (Двадцать) календарных дней, а Участников о намерении изменения тарифов предоставления услуг по ведению банковского счета не менее чем за 30 (тридцать) календарных дней до даты вступления в силу таких изменений, если иное не согласовано между Расчетным центром и Оператором, Расчетным центром и Участником.

в. Обеспечивать в рамках Платежной системы исполнение распоряжений Участников платежной системы посредством списания и зачисления денежных средств по Счетам Участников платежной системы.

г. Обеспечивать направление подтверждений Оператору Платежной Системы, касающихся исполнения распоряжений Участников платежной системы.

д. Обеспечивать прием от Оператора платежной системы Реестра платежей и исполнять его до 14:30 МСК рабочего дня, в котором он был передан.

е. Направлять Оператору Платежной Системы отчет об исполнении Реестра платежей по итогам обработки Реестра платежейи проведения расчетов.

ж. Направлять Оператору Платежной Системы информацию о наличии денежных средств (указывается точная сумма), находящихся на Счетах Участников платежной системы.

з. Предоставлять Оператору по его запросу отчеты, любую информацию, связанную с осуществлением Расчетным центром, возложенных на него функций и соблюдением требований, изложенных в Правилах.

и. Уведомлять Оператора платежной системы о приостановлении деятельности Участников, открытии/закрытии Счетов Участников платежной системы, а также в случае получения документов от Участников о намерении закрытия Счетов, незамедлительно в день известности его наступления, но не позднее окончания рабочего дня наступления факта по согласованным каналам связи.

к. Передавать Оператору платежной системы сведения об остатках денежных средств на Счетах Участников платежной системы, в пределах которых Расчетный центр проводит расчеты поопераций, совершенным в рамках Платежной системы и проведенных по Счетам Участников платежной системы платежах, связанных с осуществлением расчетов по операциям, совершенным в рамках Платежной системы ежедневно, кроме выходных и праздничных дней.

л. Уведомлять Оператора платежной системы об отзыве лицензии Участника платежной системы, на осуществление банковских операций незамедлительно в день известности его наступления, но не позднее окончания рабочего дня наступления факта.

м. В случае внесения изменений в учредительные документы, а также при изменении других данных, сообщить Оператору Платежной Системы об изменениях с приложением подтверждающих документов не позднее 5 (пяти) рабочих дней с даты их государственной регистрации или наступления данных изменений, а в части изменениях сведений о наименовании, организационно-правовой формы, местонахождении, единоличном исполнительном органе, главном бухгалтере, адреса официального сайта, номеров контактных телефонов в срок не позднее 2 (двух) рабочих дней с даты регистрации изменений, наступления данных изменений при наличии подтверждающих документов.

н. Обеспечивать бесперебойность оказания расчетных услуг, предоставляемых им участникам платежной системы, а также организовывать управление рисками в части полномочий, делегированных ему Оператором Системы.

о. Самостоятельно разрабатывать свою методику анализа рисков в Платежной системе и предоставлять ее Оператору по мере внесения изменений, но не реже одного раза в год;

п. Обеспечивать защиту информации при осуществлении переводов денежных средств, в т.ч. в соответствии с требованиями, установленными Банком России. Обеспечить реализацию механизмов, направленных на соблюдение требований к обеспечению защиты информации при осуществлении переводов денежных средств, и контроль их соблюдения

р. В случае приостановления деятельности Расчетного центра, отзыва лицензии, разрешения на осуществление деятельности Расчетного центра, а также обстоятельствах, которые могут ухудшить его финансовое состояние и/или возникновения обстоятельств, влияющих на бесперебойность осуществления его деятельности, сообщить о данном факте незамедлительно в день известности его наступления Оператору Платежной Системы по согласованным каналам связи.

2.5.3. Права Расчетного центра:

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

б. Осуществлять кредитование Счетов Участников платежной системы путем заключения соглашения между Расчетным центром и Участником платежной системы.

в. Совмещать свою деятельность с деятельностью Участника платежной системы.

3. Основные принципы договорных взаимоотношений.

При присоединении к платежной системе взаимоотношения между Оператором платежной системы и Участником платежной системы определяются договором участия в платежной системе и Правилами. Каждый Участник платежной системы, при вступлении в Платежную систему, подписывает соответствующие его работе договоры и предоставляет указанные в Правилах документы.

3.1. Основные положения договора участия между Оператором и Участником.

Предметом договора участия в Платежной системе являются взаимоотношения между ООО «ХЕЛЛО» и Участником по порядку взаимодействия в платежной системе.

Договор определяет, что кредитная организация, являющаяся Участником платежной системы:

- приобретает статус Участника платежной системы;
- обязуется выполнять требования нормативных документов Системы;

- подтверждает, что она ознакомлена и согласна с положениями действующих Правил платежной системы и приложений к ним, в том числе с Тарифами для Участников платежной системы, и обязуется их выполнять;
- обязуется уплачивать вознаграждения и другие платежи в соответствии с Тарифами для Участников платежной системы, которые устанавливаются и изменяются в соответствии с Правилами платежной системы.

3.2. Основные положения договора между Оператором и Расчетным центром.

Предметом договора являются взаимоотношения между ООО «ХЕЛЛО» и Расчетным центром, определяющие порядок взаимодействия Оператора платежной системы и Расчетного центра при проведении расчетов в платежной системе.

Договор определяет:

- права и обязанности Оператора платежной системы;
- права и обязанности Расчетного центра;
- порядок и сроки проведения расчетов;
- порядок информационного обмена и документооборота при проведении расчетов;
- формат и структуру записей реестров представленных расчетных документов;
- условия обеспечения обязательств Расчетного центра по своевременному и полному проведению расчетов, порядок и форма его предоставления.

3.3. Основные положения договора между Участником и Расчетным центром.

Предметом договора являются межбанковские взаимоотношения между Участником и Расчетным центром, связанные с расчетами по итогам платежного клиринга распоряжений участников платежной системы о переводе денежных средств, направленных через Операционный центр платежной системы.

Договор определяет:

- условия открытия Счета Участнику платежной системы в Расчетном центре;
- порядок осуществления операций по Счету Участника платежной системы;
- условия обеспечения обязательств Участника платежной системы по своевременному и полному проведению операций по Счету;
- порядок информационного обмена и документооборота при проведении операций по Счету Участника платежной системы;
- условия предоставления со стороны Расчетного центра в пользу Оператора платежной системы сведений и информации в отношении Счета Участника платежной системы, в том числе составляющих банковскую тайну;
- условия установления режима Счета исключительно для расчетов в рамках платежной системы;
- условие о списании денежных средств со Счета Участника платежной системы без дополнительного распоряжения Участника платежной системы.

4. Порядок взаимодействия между Субъектами платежной системы.

4.1. Общие положения.

4.1.1. Участник платежной системы, вправе оказывать услуги по переводу денежных средств в рамках платежной системы, на условиях, предусмотренных Правилами и договором, заключаемым с Оператором платежной системы.

4.1.2. Операции по переводу денежных средств в Платежной системе совершаются Плательщиками через: пункты обслуживания клиентов, Банкоматы, Платежные терминалы.

4.1.3. Расчеты по платежам, совершенным в рамках Системы Отправителями, являющимися клиентами Участников, осуществляются через счета Участников, открытые в Расчетном центре (для прямых Участников) и через счета, открытые у прямых Участников (для косвенных Участников).

4.2. Взаимодействие Оператора с Участниками платежной системы.

4.2.1. Взаимодействие между Оператором платежной системы и Участником платежной системы осуществляется с момента выражения намерения юридического лица присоединиться к Правилам Платежной системы (выражением намерения является подписание договора участия в Платежной системе и открытие счета в Расчетном Центре) в качестве Участника платежной системы, и в дальнейшем в процессе осуществления им функций Участника платежной системы вплоть до момента прекращения указанной деятельности последнего.

4.2.2. Принимаемые Оператором платежной системы решения об участии, приостановлении и прекращении участия в Платежной системе направляются в адрес Участников платежной системы в виде письменных уведомлений.

4.2.3. Информация об участии в платежной системе новых операторов по переводу денежных средств, приостановлении и прекращении их участия в платежной системе, размещается Оператором платежной системы на официальном сайте в информационно-телекоммуникационной сети «Интернет» по адресу: www.hellopay.online

4.2.4. Взаимодействие между Оператором платежной системы и Участником платежной системы осуществляется, в том числе, в электронном виде. Порядок электронного документооборота между Оператором платежной системы и Участником платежной системы установлен в Приложении №2 «Регламент электронного документооборота» к Правилам.

4.3. Взаимодействие между Оператором и Расчетным центром.

4.3.1. Взаимодействие Расчетного центра с Оператором платежной системы, в том числе по вопросам защиты информации, обеспечения бесперебойности платежной системы, управления рисками, а также по иным вопросам осуществляется в соответствии с Правилами и на условиях договора, заключаемого между Расчетным центром и Оператором платежной системы.

4.3.2. Расчетный центр осуществляет функции в соответствии со статьей 2.5. Правил и на условиях договора, заключаемого между Расчетным центром и Оператором платежной системы,в том числе:

- уведомляет Оператора платежной системы об открытии/закрытии Счетов Участников платежной системы;
- передает Оператору платежной системы сведения о сумме денежных средств, в пределах которой Расчетный Центр проводит расчеты по операциям, совершенным в рамках платежной системы;
- передает Оператору платежной системы сведения о проведенных Расчетным центром операциях по Счетам Участников платежной системы, совершенных в рамках платежной системы;
- принимает и обрабатывает полученные от Оператора платежной системы Реестры платежей.

4.4. Взаимодействие между Расчетным центром и Участником.

4.4.1. Участнику платежной системы на условиях договора, заключаемого между Участником платежной системы и Расчетным центром, открывается Счет.

4.4.2. Договор счета между Расчетным центром и Участником платежной системы заключается после заключения договора присоединения Участником платежной системы к Правилам, по факту предоставления Участником платежной системы в адрес Расчетного центра копии договора участия в Платежной системе.

4.4.3. Открытие Счета и взаимодействие между Расчетным центром и Участником платежной системы по вопросам осуществления операций по Счету осуществляется в соответствии с требованиями законодательства Российской Федерации, нормативных актов Банка России, требованиями Расчетного центра, а также с учетом требований Правил (2.5. Правил).

4.4.4. Списание денежных средств со Счета Участника платежной системы по операциям, совершенным в рамках платежной системы, осуществляется Расчетным центром на основании распоряжения Оператора платежной системы, переданного Расчетному центру в виде Реестра платежей. При этом получение дополнительного распоряжения Участника платежной системы на списание денежных средств со Счета Участника платежной системы не требуется.

4.4.5. На основании Реестра платежей Расчетный центр формирует отдельные распоряжения на перевод денежных средств со Счета Участника-отправителя в адрес Участника-исполнителя, для последующей выдачи получателю. Расчетный центр не несет ответственности за правомерность и содержание включенных в состав Реестра платежей распоряжений о переводе денежных средств и указанных реквизитов.

4.4.6. Исполнение распоряжений по списанию денежных средств со Счета, полученных от Участника платежной системы и не связанных с операциями, совершенных в рамках платежной системы, осуществляется Расчетным центром по согласованию с Оператором платежной системы в пределах остатка денежных средств на Счете Участника платежной системы, образовавшегося после исполнения Расчетным центром Реестра платежей.

4.4.7. Исполнение распоряжений по зачислению денежных средств на Счет Участника осуществляется Расчетным центром на условиях договора счета с Участником.

5. Порядок присоединения и участия в платежной системе Субъектов платежной системы.

5.1. Порядок привлечения Операторов услуг платежной инфраструктуры, ведение перечня Операторов услуг платежной инфраструктуры.

5.1.1. Привлечение Оператором платежной системы Операторов услуг платежной инфраструктуры осуществляется на основаниях, предусмотренных Правилами, и на основании договора, заключаемого между Оператором платежной системы и Оператором услуг платежной инфраструктуры.

5.1.2. Привлечение Операторов услуг платежной инфраструктуры осуществляется на условиях обеспечения равноправного доступа Операторов услуг платежной инфраструктуры в Платежную систему и отсутствия условия об исключительном оказании услуг платежной инфраструктуры.

5.1.3. Ведение перечня Операторов услуг платежной инфраструктуры осуществляется Оператором платежной системы самостоятельно путем включения в него информации об Операторе услуг платежной инфраструктуры с указанием его типа. При привлечении Оператором Операционного центра и/или Платежного клирингового центра, к ним будут установлены требования в Правилах системы.

5.1.4. Оператор платежной системы поддерживает перечень Операторов услуг платежной инфраструктуры в актуальном состоянии:

- перечень операторов услуг публикуется на сайте Платежной системы www.hellopay.online;

▪ при любом изменении перечня операторов услуг Оператор в течение 5 (Пяти) рабочих дней с момента возникновения оснований для внесения изменений вносит изменения в перечень;

▪ Оператор представляет в Банк России новую редакцию перечня операторов услуг не позднее 10 (Десяти) календарных дней после внесенных изменений.

5.2. Категории Участников и Критерии участия (прямого и косвенного) в Платежной системе «ХЕЛЛО».

5.2.1. Все участники платежной системы подразделяются на две категории:

▪ Прямые Участники;

▪ Косвенные Участники.

5.2.2. Категория прямого участия в Системе подразумевает:

▪ наличие банковского счета (счетов) в РЦ Системы;

▪ наличие договора участия, заключенного с Оператором Системы;

▪ допустимость с точки зрения законодательства РФ и страны местонахождения (регистрации) Участника прямого участия в Системе;

5.2.3. Категория косвенного участия в Системе подразумевает:

▪ наличие банковского счета (счетов) у прямого Участника Системы;

▪ наличие договора участия, заключенного с Оператором Системы;

▪ допустимость с точки зрения законодательства РФ и страны местонахождения (регистрации) Участника косвенного участия в Системе.

5.2.4. Организация может присоединиться к Системе при удовлетворении такой организации следующим критериям:

Общие критерии для прямых и косвенных Участников:

▪ финансовая устойчивость юридического лица;

▪ иметь действующую лицензию на право осуществления перевода денежных средств;

▪ не находиться в стадии ликвидации, банкротства или наблюдения;

▪ иметь техническую возможность интеграции в Систему;

▪ иметь доступ к сети Интернет на скорости не менее 256 кбит/сек;

▪ использовать средства межсетевого экранирования при подключении к сетям общего пользования;

▪ соблюдение обязательных нормативов Банка России (в отношении кредитных организаций – резидентов Российской Федерации); соблюдение обязательных нормативов национального банка страны местонахождения (регистрации) Участников (в отношении кредитных организаций – нерезидентов Российской Федерации);

▪ соблюдение требований законодательства Российской Федерации по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в отношении кредитных организаций – резидентов Российской Федерации; в отношении кредитных организаций – нерезидентов Российской Федерации соблюдение аналогичных требований законодательства страны местонахождения (регистрации) Участника;

▪ обеспечение защиты информации в собственных информационных системах, а также при взаимодействии с Субъектами, в соответствии с требованиями, законодательства Российской Федерации, нормативных актов Правительства Российской Федерации и Банка России, Правил в отношении кредитных организаций – резидентов Российской Федерации; в отношении кредитных организаций – нерезидентов Российской Федерации соблюдение аналогичных требований Правил, законодательства страны местонахождения (регистрации) Участника.

5.2.5. Критерием, относящимся только к прямым Участникам, является открытие счета в РЦ Системы.

5.2.6. Критерием, относящимся только к косвенным Участникам, является открытие счета у Прямого Участника Системы.

5.3. Порядок присоединения организации к Системе и наделение ее статусом Участника (прямого/косвенного).

5.3.1. Для возможности рассмотрения в целях дальнейшего получения статуса Участника лицо, отвечающее критериям, установленным в разделе 2.2. настоящих Правил (далее - Заявитель), вправе направить Оператору заявление на участие в Системе в свободной форме или по форме Оператора, с указанием вида участия. Заявитель, намеревающийся стать косвенным Участником, указывает прямого Участника, у которого открыт его счет/у которого намеревается открыть счет и направляет аналогичное заявление прямому Участнику. Заявитель предоставляет Оператору Системы пакет документов в соответствии с перечнем, утвержденным Оператором Системы.

5.3.2. В случае принятия Оператором положительного решения о включении Заявителя в число Участников, Заявитель подписывает договор об участии, а также предоставляет иные сопутствующие документы, необходимость в которых возникает из характера устанавливаемых правоотношений.

При отрицательном решении Оператора, заявителю направляется только уведомление, содержащее информацию об отказе.

5.3.3. Оператор отказывает в возможности присвоении статуса Участника в случае несоответствия Заявителя требованиям Правил и действующего законодательства и/или непредоставления документов, предусмотренных Правилами.

5.3.4. Для изменения вида участия Участник вправе заявить о намерении путем направления Оператору заявления на участие в Системе в свободной форме или по форме Оператора с указанием вида участия, а также перечень прилагаемых документов (при необходимости). В случае принятия Оператором положительного решения об изменении вида участия, Участнику направляется новый договор об участии, а также иные сопутствующие документы, необходимость в заключении которых возникает из характера устанавливаемых правоотношений, при этом Участник обязан подписать и предоставить соглашение о расторжения договора участия с соответствующим статусом участия и копию соглашения о расторжении договора с прямым участником (в случае изменения статуса на «прямой Участник»), с Расчетным центром (в случае изменения статуса на «косвенный Участник»).

5.3.5. Датой начала участия в Системе, в целях уведомления об этом уполномоченного органа, является дата получения уведомления Оператором от Расчетного центра (или от прямого Участника, у которого косвенным Участником открыт счет) об открытии счета в Расчетном центре Системы (или у прямого Участника) при условии заключения договора участия в Платежной системе «ХЕЛЛО» или от Участника, по согласованным каналам связи, в зависимости от того какое событие наступит ранее.

5.4. Критерии приостановления и прекращения участия в Платежной системе «ХЕЛЛО».

5.4.1. В случае несоблюдения Участником платежной системы условий осуществления платежного клиринга и расчета, установленных Правилами, а также в иных случаях, установленных в Правилах, Оператор платежной системы вправе до даты устранения Участником платежной системы допущенного нарушения в одностороннем порядке приостановить его участие в Платежной системе, а именно: приостановить возможность совершения операций для целей перевода денежных средств клиентами Участника платежной системы, а также ограничить в иных правах и не оказывать иные услуги, предусмотренные Правилами и договором участия.

5.4.2. Оператор платежной системы вправе приостановить участие в Платежной системе Участника в случаях, предусмотренных в пунктах 6.6.10, 27.2. и 27.6. Правил, а также, если:

- имеющиеся в распоряжении Оператора платежной системы сведения позволяют сделать вывод о высокой вероятности возникновения рисков, ведущих к невозможности осуществления расчетов по операциям, совершенным клиентами Участника платежной системы для целей перевода денежных средств, в том числе неисполнения обязанности по обеспечению достаточности

денежных средств на Счете Участника платежной системы в сроки и порядке, установленные Правилами;

- любые компетентные органы власти приостанавливают или отменяют полномочия Участника или выпускают уведомление о своем намерении поступить таким образом;
- в случае приостановления государственным органом операций Участника или наложения ареста на денежные средства Участника, находящиеся на счете в Расчетном центре.

5.4.3. Оператор платежной системы не позднее 3 (трех) рабочих дней, следующих за днем приостановления участия, уведомляет Участника платежной системы в письменном виде о причинах приостановления участия и о необходимости устранения Участником платежной системы допущенных нарушений. После устранения Участником платежной системы допущенных нарушений и их последствий участие Участника в платежной системе возобновляется автоматически либо по письменному заявлению Участника платежной системы с приложением документов, подтверждающих устранение допущенных нарушений и их последствий (прилагаются при необходимости подтверждения).

5.4.4. Участие в Платежной системе Участника прекращается в следующих случаях и порядке:

- в случае отзыва у Участника необходимых для его деятельности в рамках Системы разрешений (лицензии) либо приостановления их действия, при этом датой прекращения участия является дата публикации на официальном сайте Банка России (в случае если Участник нерезидент
  - национального банка страны местонахождения Участника) или дата получения уведомления о данном факте от Участника/Расчетного центра, в зависимости от того какое событие наступит ранее;
- если Участник объявляет о своей ликвидации, либо в отношении него инициирована процедура банкротства, при этом датой прекращения участия является дата публикации в соответствующем средстве информации или дата получения уведомления о данном факте от Участника/Расчетного центра, в зависимости от того какое событие наступит ранее;
- в случае закрытия счета в Расчетном центре согласно предписанию национального (центрального) банка страны местонахождения (регистрации) Участника, при этом датой прекращения участия является дата получения уведомления о данном факте от Участника/Расчетного центра, в зависимости от того какое событие наступит ранее;
- по решению Оператора платежной системы в случаях, предусмотренных в Правилах (пункты 28.3 и 28.4. Правил). При этом участие Участника платежной системы приостанавливается, Оператор платежной системы уведомляет Участника платежной системы о приостановлении с указанием даты прекращения участия Участника платежной системы в Платежной системе, об объеме неисполненных обязательств Участника платежной системы, связанных с участием в Платежной системе, включая обязательства по осуществлению расчетов по операциям, совершенным клиентами Участника платежной системы для целей перевода денежных средств, и оплаты оказанных Участнику платежной системы услуг. Участник платежной системы обязан в срок, не позднее одного рабочего дня, с даты отправления уведомления по согласованным каналам связи Оператором платежной системы осуществить расчеты по всем своим обязательствам, по истечении указанного срока участие в Платежной системе прекращается.

5.4.5. Договор участия считается прекращенным с даты прекращения участия Участника платежной системы.

5.4.6. Участник может прекратить свое участие в Платежной системе, путем направления заявления о прекращении участия в Платежной системе, составленное в письменной форме на бумажном носителе, подписанного уполномоченным лицом Участника и скрепленного печатью Участника платежной системы, поданного Оператору платежной системы. Не позднее третьего рабочего дня, со дня получения заявления о прекращении участия Оператор приостанавливает участие Участника в Системе. Оператор платежной системы уведомляет Участника платежной системы об объеме неисполненных обязательств Участника платежной системы, связанных с

участием в платежной системе, включая обязательства по осуществлению расчетов по операциям, совершенным клиентами Участника платежной системы для целей перевода денежных средств, и оплаты, оказанных Участнику платежной системы услуг. Участник платежной системы обязан не позднее одного рабочего дня, с даты отправления уведомления от Оператора платежной системы, осуществить расчеты по всем своим обязательствам, по истечении указанного срока участие в Платежной системе прекращается.

5.5. Порядок присвоения идентификационного номера.

5.5.1. Участнику платежной системы присваивается идентификационный цифровой (четырехразрядный) порядковый номер, позволяющий однозначно установить Участника платежной системы.

Присвоение идентификационного номера Участнику осуществляется автоматически согласно шаблону XYYY, где:

- X равно 0 для прямых Участников Системы и 1 для косвенных Участников Системы;
- YYY – порядковый номер Участника Системы.

5.5.2. Идентификационный код присваивается Оператором платежной системы автоматически после конфигурации Участника платежной системы.

5.5.3. Идентификационный номер Участника позволяет установить наименование Участника, номер лицензии (или иного правоустанавливающего документа), страну инкорпорации.

5.5.4. Оператор может размещать реестр Участников с присвоенными им идентификационными номерами Участников системы на своем официальном сайте.

5.5.5. В случае если Участник выходит из состава Участников Платежной системы его номер не присваивается новому Участнику.

5.6. Партнеры Платежной системы «ХЕЛЛО».

5.6.1. Партнеры Платежной системы «ХЕЛЛО» - юридические лица, в т.ч. имеющие лицензию (разрешение) на осуществление переводов денежных средств, почтовых переводов в соответствии с законодательством страны своего местонахождения, не присоединившиеся к Правилам Системы в целом, осуществляющие перевод в качестве клиентов Участников, в соответствии с Правилами Системы и соответствующими соглашениями, заключенными с Участниками.

5.6.2. Заключаемые соглашения определяют порядок взаимодействия Участников, в т.ч. Оператора Системы, и Партнеров. Партнеры осуществляют переводы денежных средств в рамках единого информационного пространства Системы в соответствии с заключенными соглашениями. В случае если то или иное положение не оговорено такими соглашениями, Партнеры могут руководствоваться принципами Системы, используемыми Участниками в соответствующих случаях.

5.6.3. В соглашениях при необходимости (при невозможности руководствоваться принципами Системы) прописываются индивидуальные размер и порядок оплаты комиссионного вознаграждения, причитающегося Участнику, в т.ч. Оператору Системы, и Партнеру, условия осуществления расчетов и порядок электронного документооборота, особенности отправки/выплаты переводов в адрес/от клиентов Партнера, в том числе ограничения Партнера по суммам переводов при их наличии, валюта выплаты переводов Партнером и другие особенности взаимоотношений.

5.6.4. Наступление окончательности, порядок и условия внесения изменений или аннулирования Переводов, направленных для выплаты Получателю Партнером, имеют следующие особенности:

- Окончательность Перевода наступает в момент зачисления денежных средств на счет Участника, чьим клиентом является Партнер;

- Возможность или невозможность внесения изменений определяется Партнером Системы на основании запроса, полученного от Оператора Системы. При получении от Партнера информации о невозможности внесения изменений в Перевод Оператор Системы незамедлительно извещает Участника-Отправителя о данном факте доступными способами. Участник - Отправитель уведомляет Отправителя о результатах обработки запроса на внесение изменений. Дополнительная комиссия за внесение изменений не взимается, если иное не оговорено партнерским соглашением;
- Возможность или невозможность осуществления возврата Перевода определяется Партнером Системы на основании запроса, полученного от Оператора Системы. При получении от Партнера информации о невозможности возврата Перевода Оператор Системы незамедлительно извещает Участника-Отправителя о данном факте доступными способами.

5.6.5. Существующие особенности отправки/выплаты, внесения изменений или осуществления возврата Переводов в пользу клиентов Партнеров Системы, основанные, в том числе на положениях законодательства страны местонахождения Партнера, Оператор Системы доводит до сведения Участников Системы с помощью используемого программного обеспечения при оформлении Перевода и/или любым другим доступным способом.

5.6.6. Оператор оставляет за собой право доведения указанных особенностей до сведения заинтересованных лиц, путем размещения информации на официальном сайте Системы в сети интернет www.hellopay.online

6. Порядок осуществления расчетов по операциям, совершаемым в соответствии с Правилами, и между Субъектами платежной системы.

6.1. Применяемые формы безналичных расчетов.

6.1.1. Перевод денежных средств в Платежной системе осуществляется в форме безналичных расчетов - расчетов платежными поручениями.

6.1.2. Перевод денежных средств осуществляется со Счета Участника платежной системы на основании распоряжений, включенных в Реестр и поступающих в Расчетный центр от Оператора платежной системы по согласованным каналам связи.

6.1.3. На основании распоряжения, переданного в случаях и в порядке согласно п. 6.4 Правил, Оператором платежной системы Расчетному центру, Расчетный центр составляет распоряжения и осуществляет перевод денежных средств со Счета Участника-отправителя Участнику-исполнителю.

6.1.4. Бухгалтерское отражение операций по счетам Участников, осуществляется по итогам соответствующего операционного дня Оператора на общие суммы:

- по всем платежным распоряжениям, исходящим от Участника в качестве Участника–отправителя, принятым к исполнению Платежным клиринговым центром;
- по выплаченным/зачисляемым на счета денежным средствам Участником в качестве Участника-исполнителя;
- по отвергнутым Участниками-исполнителями распоряжениям;
- по списываемым и/или зачисляемым комиссиям.

6.2. Порядок осуществления перевода денежных средств в рамках Платежной системы «ХЕЛЛО», включая моменты наступления его безотзывности, безусловности и окончательности. Аннулирование Переводов.

6.2.1. Прием/списание денежных средств Участником-отправителем от Отправителя может осуществляться наличными (только для Отправителей – физических лиц) или безналичными денежными средствами (для Отправителей - физических или юридических лиц), со счета Отправителя. Прием/списание осуществляются сотрудником Участника - отправителя в пункте обслуживания Участника.

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

При отправке Перевода Оператором Системы присваивается уникальный номер (контрольный номер перевода).

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

Идентификация с участием уполномоченных работников:

- Прием от Отправителя – физического лица денежных средств производится при представлении Отправителем документа, удостоверяющего личность, содержащего сведения, достаточные для его идентификации и осуществления операции.
- Участник в соответствии с действующим законодательством страны своего местонахождения имеет право запросить у физического лица иные документы, необходимые для его идентификации.
- В случае обращения представителя Отправителя требуется представление документа, удостоверяющего личность представителя Отправителя, а также надлежащим образом оформленной доверенности.

Участник - отправитель обязан предоставить Отправителю документ, подтверждающий осуществление перевода, и сведения о переводе в электронном виде или на бумажном носителе.

6.2.2. Сроки осуществления Переводов денежных средств в Платежной системе «ХЕЛЛО».

1. По переводам в пользу физических лиц для выплаты наличными денежными средствами безусловность перевода наступает в момент обращения Получателя в точку выплаты.

По Переводам в пользу юридических лиц и для зачисления на счета физических лиц, при наличии у Участника или самого Получателя индивидуальных требований к информации, которая должна содержаться в Переводе в их пользу, проверка наступления безусловности может осуществляться:

- на этапе введения перевода в программное обеспечение Участника, при не прохождении проверки перевод не принимается в обработку;
- на этапе обработки перевода ПКЦ, в этом случае при не прохождении проверки Перевод возвращается Участнику - отправителю ПКЦ;
- самим Участником-исполнителем или Получателем - юридическим лицом при поступлении Перевода.

Перевод электронных денежных средств осуществляется незамедлительно после принятия оператором электронных денежных средств распоряжения клиента.

2. Окончательность Перевода с целью выплаты физическим лицам наличными денежными средствами наступает в момент зачисления перевода на счет Участника-исполнителя.

Окончательность Перевода, направленного для зачисления на счет физического лица или направленного в адрес юридического лица, наступает:

- в момент зачисления денежных средств на счет Получателя или

▪ в момент зачисления денежных средств на счет кредитной организации/иностранного банка, в которой открыт счет Получателя, или

▪ в момент зачисления денежных средств на счет организации-посредника, участвующей в доставке средств Получателю вышеуказанными способами, при совпадении каких-либо из вышеперечисленных условий окончательность перевода наступает в момент выполнения условия, наступившего раньше.

3. Безотзывность переводов, направленных для зачисления на счет Получателя, наступает в момент предоставления Отправителем наличных денежных средств или списания денежных средств со счета Отправителя в целях осуществления перевода, если иное не оговорено соответствующим соглашением Оператора Системы с Получателем или Участником - исполнителем.

4. Перевод электронных денежных средств становится безотзывным после принятия оператором электронных денежных средств (Участника – отправителя) распоряжения клиента на уменьшение остатка электронных денежных средств на сумму перевода электронных денежных средств. Перевод электронных денежных средств становится окончательным с момента увеличения оператором электронных денежных средств (Участника – исполнителя) остатка электронных денежных средств Получателя на сумму Перевода.

Порядок использования электронных средств платежа при осуществлении переводов электронных денежных средств регулируется условиями договоров Участников Платежной системы и их клиентов. Участники гарантируют осуществление перевода электронных денежных средств в соответствии со статьей 7 Закона о НПС и с учетом особенностей перевода электронных денежных средств с использованием электронных средств платежа, предусмотренных статьей 10 Закона о НПС.

Момент безотзывности Перевода, осуществленного посредством таких электронных средств платежа, как Банкомат и Платежный терминал, а также при использовании дистанционного банковского обслуживания (ДБО) определен в пп. 6.3.3., 6.3.6. Правил соответственно.

6.2.3. Отзыв, возврат (аннулирование) Переводов.

Отзыв, возврат (аннулирование) Переводов осуществляется:

1) по инициативе Отправителя;

2) по инициативе Оператора в одностороннем порядке в следующих случаях:

а) прекращение сотрудничества Оператора с Участником - исполнителем;

б) наступление иных обстоятельств, делающих невозможной выдачу Перевода Получателю Участником-исполнителем или иным Участником по причинам, независящим от Отправителя и Получателя.

Заявление об отзыве Перевода принимается Участником при условии предъявления Отправителем паспорта или иного документа, удостоверяющего личность и сообщения им КНП. Заявление об отзыве служит основанием для возврата (аннулирования) распоряжения, либо возврата суммы Перевода на основании нового распоряжения о переводе.

Заявление об отзыве адресного перевода подается через тот же пункт Участника-отправителя, что и заявление на осуществление перевода. Заявление об отзыве безадресного перевода Отправитель вправе подать через любого Участника Системы.

Отзыв, возврат (аннулирование) распоряжения о переводе денежных средств осуществляется до момента наступления безотзывности перевода денежных средств.

Возврат денежных средств на сумму Перевода может осуществляться при условии, что Перевод не выдан/зачислен Получателю (до момента наступления окончательности перевода).

При возврате Бивалютного перевода, Отправителю выдается сумма Перевода по курсу Оператора на день выдачи.

Возврат денежных средств на сумму Перевода по инициативе Оператора производится Оператором в одностороннем порядке после наступления обстоятельств, указанных в п. 6.2.3. Правил.

При возврате денежных средств на сумму Перевода вследствие прекращения сотрудничества Оператора с Участником - исполнителем или наступления иных обстоятельств, делающих невозможной выдачу Перевода Получателю Участником - исполнителем или иным Участником по любым причинам, независящим от Отправителя и Получателя, ранее уплаченная Отправителем Комиссия за Перевод подлежит возврату Отправителю. В тех случаях, когда Сумма Перевода по каким-либо причинам не может быть выплачена Отправителю Участником - отправителем, Сумма перевода может быть возвращена Отправителю Оператором. В этом случае Оператор обязан уведомить Участника - отправителя о состоявшейся выплате, а Участник-отправитель обязан возместить Оператору выплаченную последним Отправителю сумму в порядке, установленном для проведения взаиморасчетов Участников Системы.

Возврат сумм Переводов денежных средств, направленных для зачисления на счета физических лиц или в пользу юридических лиц, Оператором не осуществляется. Для возврата денежных средств Отправитель обращается к соответствующему юридическому лицу или к кредитной организации, в которой открыт счет Получателя, напрямую. В случае невозможности такого обращения Отправитель может подать через Участника-отправителя соответствующее заявление. Оператор Системы предпримет все возможные меры, но при этом Оператор не гарантирует возврат Суммы перевода, ввиду независящих от него обстоятельств.

Возврат суммы Перевода по инициативе Отправителя осуществляется:

Возврат Адресного перевода.

Отправитель обязан подать заявление об отзыве Перевода Участнику - отправителю данного Перевода. Срок возврата суммы Перевода зависит от особенностей технической интеграции,а также особенностей внутреннего порядка, законодательства того или иного Участника. Сроки возврата суммы Перевода подлежат уточнению Отправителем у Участника-отправителя непосредственно до подачи соответствующего Заявления.

Возврат Безадресного перевода.

Отправитель обязан подать заявление об отзыве Перевода любому Участнику на территории страны отправки.

Дополнительная комиссия за возврат суммы Перевода с Отправителя не взимается, при этом Комиссия за перевод возврату не подлежит.

6.3. Осуществление денежных переводов через Банкомат, Платежный терминал.

6.3.1. До осуществления Плательщиком денежных переводов через Банкомат, Платежный терминал Участник платежной системы обязан предоставить Плательщикам возможность ознакомления в доступной для них форме с условиями осуществления перевода денежных средств в рамках применяемой формы расчетов, в том числе:

- с размером вознаграждения и порядком его взимания;
- с порядком предъявления претензий, включая информацию для связи с Участником платежной системы;
- с иной информацией, обусловленной применяемой формой расчетов.

6.3.2. При проведении операций по переводу денежных средств с использованием Банкомата, Платежного терминала Операционным центром проверяются параметры, необходимые для принятия решения по авторизации операций.

6.3.3. Успешное проведение операции с использованием Банкомата, Платежного терминала завершается формированием Банкоматом, Платежным терминалом чека. С момента формирования Банкоматом, Платежным терминалом указанного документа, перевод денежных средств получает статус безотзывного, и операция не может быть отменена.

6.3.4. При успешном осуществлении денежного перевода с использованием Банкомата, Платежного терминала Лимит Участника платежной системы уменьшается Операционным центром на сумму операции и сумму денежных средств в оплату услуг Оператора платежной системы.

6.3.5. При проведении операций по уплате платежей с использованием Системы удаленного доступа Плательщик использует электронную подпись (ЭП), в целях распоряжения денежными средствами, доступными для проведения операции. ЭП должна принадлежать Плательщику в соответствии с действующим законодательством. В данном случае ответственность за распоряжение денежными средствами несет владелец Счета.

6.3.6. Подтверждением успешного завершения операции является формирование Системой ДБО соответствующего сообщения и электронного документа (чека). С момента формирования указанного документа перевод денежных средств получает статус безотзывного.

6.3.7. При успешном завершении операций Операционным центром уменьшается лимит Участника платежной системы на сумму операции и сумму денежных средств в оплату услуг Оператора.

6.4. Предоставление информации об операциях, совершенных через пункты обслуживания клиентов, банкоматы и платежные терминалы.

6.4.1. Предоставление Оператором платежной системы Участникам платежной системы информации об операциях, совершенных через пункты обслуживания клиентов, Банкоматов и Платежных терминалов осуществляется в соответствии с технической документацией, внутренним нормативным документом Оператора платежной системы, предоставляемыми Участникам Платежной системы.

6.5. Порядок сопровождения перевода денежных средств сведениями о Плательщике.

6.5.1. Сопровождение перевода денежных средств сведениями о Плательщике осуществляется Участником платежной системы в соответствии с требованиями Федерального закона от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон №115-ФЗ) в случае, если они не содержатся в распоряжении Участника платежной системы.

Участники платежной системы реализуют комплекс мероприятий, направленных на предотвращение легализации (отмывания) доходов, полученных преступным путем, и финансированию терроризма. Участники платежной системы при выявлении в платежной системе нарушений требований Федерального закона № 115-ФЗ при осуществлении переводов денежных средств, принимают меры по локализации выявленных нарушений и устранению негативных последствий, вызванных нарушением указанных требований.

В соответствии с п. 1.4. статьи 7 Федерального закона №115-ФЗ идентификация Плательщика при осуществлении переводов денежных средств на сумму, не превышающую 15 000рублей РФ, либо сумму в иностранной валюте, эквивалентную 15 000 рублей РФ:

-не проводится при осуществлении Переводов, в том числе в целях увеличения остатка электронных денежных средств, в пользу юридических лиц и индивидуальных предпринимателей;

- проводится полная идентификация при осуществлении переводов в пользу физических лиц, некоммерческих организаций (кроме религиозных и благотворительных организаций, зарегистрированных в установленном порядке, товариществ собственников недвижимости (жилья), жилищных, жилищно-строительных кооперативов или иных специализированных потребительских кооперативов, региональных операторов, созданных в организационно-правовой форме фонда в соответствии с Жилищным кодексом Российской Федерации), либо организаций, созданных за пределами территории Российской Федерации;

- проводится полная идентификация если у работников Участников возникают подозрения, что указанная операция осуществляется в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма.

Полная идентификация клиента - физического лица проводится независимо от суммы перевода при осуществлении Участниками перевода денежных средств без открытия банковского счета, в том числе электронных денежных средств, в целях оплаты товаров (работ, услуг), включенных в перечень товаров (работ, услуг), определенный Правительством Российской Федерации.

6.5.2. При осуществлении операций, в том числе с использованием Банкомата, Платежного терминала, Участники платежной системы вправе в целях выполнения требований, установленных статьей 7.2 Федерального закона №115-ФЗ, самостоятельно осуществлять заполнение расчетных документов Плательщиков с использованием информации, полученной от Плательщиков, в том числе при осуществлении процедуры идентификации.

6.5.3. Участники платежной системы, осуществляющие переводы денежных средств по поручению Плательщика, обязаны обеспечить неизменность информации, содержащейся в полученном расчетном документе, и ее хранение в соответствии с пунктом 4 статьи 7 Федерального закона №115-ФЗ.

6.5.4. Если у Субъектов платежной системы, участвующих в переводе денежных средств, возникают подозрения, что операция в целях перевода денежных средств осуществляется в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, Субъект платежной 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, и финансированию терроризма.

6.6. Порядок осуществления платежного клиринга и расчетов.

6.6.1. В целях обеспечения исполнения обязательств Участников системы, Оператором для каждого Участника устанавливаются предельные размеры обязательств (лимитов) для осуществления Расчетным центром для каждого Участника межбанковских расчетов. Размер установленных Оператором лимитов контролируется и изменяется Платежным клиринговым центром при формировании распоряжений Участников.

Расчеты по операциям, совершенным клиентом Участника-отправителя в целях перевода денежных средств и по обязательствам Участника-отправителя осуществляются со счета. При осуществлении расчета на нетто-основе должно обеспечиваться исполнение наибольшего по размеру обязательства Участника.

6.6.2. Платежный клиринг в Платежной системе осуществляется Платежным клиринговым центром, функции которого может выполнять Оператор Платежной Системы, посредством:

- выполнения процедур приема к исполнению распоряжений Участников платежной системы, включая проверку соответствия распоряжений Участников платежной системы установленным требованиям, определение достаточности денежных средств (лимита) для исполнения распоряжений Участников платежной системы и определение платежных клиринговых позиций;
- передачи Расчетному центру для исполнения принятых распоряжений Участников платежной системы;
- направления участникам платежной системы извещений (подтверждений), касающихся приема к исполнению распоряжений участников платежной системы, а также передачи извещений (подтверждений), касающихся исполнения распоряжений участников платежной системы;
- мониторинга исполнения распоряжений, содержащихся в Реестре на списание денежных средств со Счета в пользу получателей, на соответствие данных отчета об операциях, совершенных Плательщиками.

6.6.3. Завершение приема распоряжений к обработке текущим операционным днем (закрытие операционного дня) осуществляется в 23:59:59 МСК текущего операционного дня.

6.6.4. Составление Реестров и отчетов за операционный день и их передача Операционным центром в Платежный клиринговый центр с 00:00:00 МСК до 10:30 МСК рабочего дня,следующего за операционным (в случае привлечения Оператором Платежного клирингового центра).

6.6.5. При упоминании операций Участника будут подразумеваться операции прямых Участников с учетом операций косвенных Участников, открывших счета для расчетов в рамках Системы у соответствующих прямых Участников.

6.6.6. Расчеты с косвенными Участниками осуществляются Оператором Системы по счетам прямых Участников в операционные дни Оператора, при этом расчеты косвенного Участника с прямым Участником осуществляются самостоятельно в соответствии с заключенным между ними договором.

Прямой Участник самостоятельно рассчитывает нетто-позицию косвенного Участника. Оператор Системы, рассчитывая нетто-позицию для прямых Участников, открывших счета косвенным Участникам, учитывает сведения о распоряжениях, представленных косвенными Участниками.

В случае отсутствия/ недостаточности денежных средств на счетах косвенных Участников для осуществления своевременных расчетов прямой Участник обеспечивает:

- информирование косвенного Участника о необходимости пополнения счета;
- незамедлительное списание денежных средств при их поступлении на счет;
- соблюдение очередности исполнения распоряжений Оператора.

6.6.7. Прямой Участник, в случае открытия у него счетов косвенных Участников, обязан:

- включать в свои договоры с косвенными Участниками положения, обеспечивающие выполнение требований данного раздела Правил;
- уведомлять Оператора платежной системы об открытии/закрытии Счетов косвенных Участников платежной системы в течение 3 (трех) рабочих дней с момента открытия/закрытия Счета по согласованным каналам связи.
- поддерживать на своих счетах, открытых в Расчетном центре, остатки денежных средств, достаточные для осуществления своевременных и бесперебойных расчетов как по собственным операциям в Системе, так и по операциям косвенных Участников, рассчитывающихся через его счета;
- обеспечить завершение расчетов с косвенными Участниками Системы на основании предоставленных Оператором Системы реестров не позднее следующего за днем поступления реестра Операционного дня при условии достаточности средств на счетах косвенных Участников;

при невозможности обеспечить завершение расчетов с косвенными Участниками из-за недостаточности средств на счетах последних заблокировать средства в размере остатка по соответствующему счету такого косвенного Участника и незамедлительно известить об этом фактеОператора Системы по согласованным каналам связи;

- при поступлении средств на счет косвенного Участника в размере, достаточном для выполнения, оставшегося ранее без исполнения распоряжения Оператора Системы, незамедлительно отменить блокировку по счету данного косвенного Участника, списать необходимую для выполнения распоряжения Оператора Системы сумму и проинформировать об этом Оператора по электронной почте по согласованным адресам.

6.6.8. Прямой Участник, в случае открытия у него счетов косвенных Участников, имеет право:

- взимать с косвенных Участников, открывших у него счета, дополнительное комиссионное вознаграждение за расчетное и прочее обслуживание;
- предоставлять кредиты Участникам, открывшим у него счета, для осуществления расчетов в Системе;
- предъявлять требования к Участникам по открытию корреспондентских счетов, специально предназначенных для расчетов в рамках Системы**,** а также устанавливать валюту расчетов.

6.6.9. Косвенный Участник обязан при заключении договоров банковского счета с прямым Участником:

- предоставить ему право на списание денежных средств со счетов без дополнительного распоряжения владельца счета на условиях заранее данного акцепта при предъявлении требования о списании, полученного от Оператора Системы;
- поддерживать на счетах остатки денежных средств в размере, необходимом для выполнения ими своих обязательств в рамках Системы**.**

6.6.10. Оператор при наличии открытых отрицательных нетто – позиций косвенных Участников вправе заблокировать их возможность осуществлять операции по приему, оформлению и отправке новых переводов до окончательного урегулирования расчетов.

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

6.6.12. После определения платежной клиринговой позиции Оператор, выполняющий функции Платежного клирингового центра, формирует и направляет в Расчетный центр Реестр, содержащий распоряжения на списание и зачисление со/на Счета в пользу получателей. В случае приостановления участия в платежной системе Участника Оператор вправе, не дожидаясь окончания операционного дня, сформировать Реестр и направить его в Расчетный центр. В этом случае Реестр формируется на основании полученной с начала операционного дня и до момента приостановления участия информации, указанной в разделе 5 Правил, и услуг, оказанных Участнику Оператором за период с начала календарного месяца оказания услуг по дату приостановления участия в платежной системе. Оператор, действуя в качестве Платежного клирингового центра, осуществляет расчет платежной клиринговой позиции Участников не позднее 10:00 часов и направляет в Расчетный центр Реестр не позднее 12:00 часов по московскому времени рабочего дня, следующего за операционным днем.

6.6.13. Расчеты в платежной системе осуществляются Расчетным центром посредством списания и зачисления (без дополнительного распоряжения Участника платежной системы) денежных средств со/на Счета на основании поступившего от Оператора платежной системы, выполняющего функции Платежного клирингового центра, Реестра в размере сумм определенных платежных клиринговых позиций. Списание денежных средств со Счета на основании Реестра осуществляется Расчетным центром текущим рабочим днем (в период с момента поступления Реестра до 14.30 часов по московскому времени).

6.6.14. Направление Участникам платежной системы отчетов об операциях, совершенных Плательщиками в целях перевода денежных средств в течение операционного дня, расчеты по которым осуществляются за счет Участника платежной системы, осуществляется Оператором платежной системы, выполняющим функции Платежного клирингового центра.

6.6.15. Общая сумма совершенных Плательщиками операций по переводу денежных средств, списание по которым со Счета в пользу получателей еще не произведено, не должна превышать сумму лимита, установленного Оператором платежной системы Участнику платежной системы в порядке, определенном Правилами.

6.6.16. В случае несоблюдения Участником платежной системы условий, указанных в настоящей статье, Оператор платежной системы вправе до даты устранения Оператором по переводу денежных средств допущенного нарушения в одностороннем порядке приостановить возможность совершения операций в рамках платежной системы, а также не оказывать иные услуги, оказание которых предусмотрено Правилами и договором участия.

6.7. Порядок обеспечения исполнения обязательств Участников по переводу денежных средств.

6.7.1. Основополагающим механизмом обеспечения исполнения обязательств Участников Платежной системы является возможность осуществления переводов в пределах лимита Участника платежной системы.

6.7.2. Размер лимитов определяется Оператором Системы на основе анализа финансового состояния Участника и доводится до сведения Участников, которым установлены лимиты, по согласованным каналам связи.

6.7.3. Расчетный центр направляет информацию о размере остатка денежных средств Участника ПС «ХЕЛЛО». Расчетный центр осуществляет проведение операций в пределах остатка денежных средств на Счете Участника платежной системы на момент проведения расчетов. Расчетный центр, несет ответственность за своевременное оказание расчетных услуг в рамках платежной системы в рамках установленных лимитов.

6.8. Порядок оплаты услуг по переводу денежных средств.

6.8.1. Порядок оплаты услуг по переводу денежных средств и услуг платежной инфраструктуры и Оператора платежной системы в рамках Платежной системы являются едиными и единообразными для всех Участников платежной системы.

6.8.2. Услуги Оператора платежной системы, выполняющего функции Операционного центра и ПКЦ, предоставляемые в рамках Платежной системы, Участники платежной системы оплачивают в соответствии с Тарифами Оператора платежной системы (Приложение № 1 к Правилам).

6.8.3. Оператор платежной системы вправе вносить изменения в стоимость услуг и порядок их оплаты в порядке, предусмотренном для внесения изменений в Правила.

7. Система управления рисками в Платежной системе «ХЕЛЛО».

При обеспечении БФПС, которая достигается при условии оказания Участникам Платежной системы услуг платежной инфраструктуры согласно требованиям к оказанию услуг и (или) восстановления оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, в течение 24 часов и восстановления оказания УПИ в случае приостановления их оказания в течение 6 часов, к Оператору применяются следующие требования.

Оператор обеспечивает БФПС путем осуществления, скоординированной с Операторами услуг платежной инфраструктуры и Участниками Платежной системы «ХЕЛЛО» деятельности:

- по управлению рисками в Платежной системе «ХЕЛЛО»;
- по управлению непрерывностью функционирования Платежной системы «ХЕЛЛО».

Оператор определяет и соблюдает порядок обеспечения БФПС, который включает:

- управление рисками в Платежной системе;
- управление непрерывностью функционирования Платежной системы;
- организацию взаимодействия Субъектов Платежной системы по обеспечению БФПС;
- контроль за соблюдением Операторами услуг платежной инфраструктуры и Участниками Платежной системы порядка обеспечения БФПС.

Под системой управления рисками в Платежной системе понимается комплекс мероприятий и способов снижения вероятности возникновения неблагоприятных последствий в целях бесперебойности функционирования Платежной системы. Система управления рисками включает организационную модель управления рисками, перечень мероприятий, проводимых в рамках Платежной системы, и способов управления рисками.

7.1. Модель управления рисками.

7.1.1. Оператор организует систему управления рисками в Платежной системе с учетом организационной модели управления рисками в платежной системе, определенной в соответствии

с требованиями части 2 статьи 28 Закона о НПС. Система управления рисками в Платежной системе может быть интегрирована в систему управления рисками деятельности Оператора Платежной системы, не связанной с функционированием Платежной системы.

Оператор обеспечивает надежность Системы. Функции по оценке и управлению рисками в Системе распределяются между Субъектами Платежной системы.

Оператор проводит оценку рисков в Платежной системе не реже одного раза в год с использованием методик анализа рисков в Платежной системе, включая профили рисков по форме Приложения №7 к Правилам.

7.1.2. Настоящие Правила Платежной системы «ХЕЛЛО» содержат принципы управления рисками. Для организации деятельности по управлению рисками Оператор разрабатывает «Положение по управлению рисками и обеспечению бесперебойности функционирования Платежной системы «ХЕЛЛО»» (далее – Положение), которое является неотъемлемой частью настоящих Правил (Приложение № 7).

7.1.3. Положение разрабатывается Оператором в соответствии с требованиями Положения Банка России от 03.10.2017 г. № 607-П «О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включаяпрофили рисков», и определяет систему управления рисками в Платежной системе «ХЕЛЛО». Положение содержит, в том числе:

- организационную структуру управления рисками, обеспечивающую контроль за выполнением участниками платежной системы требований к управлению рисками, установленных Правилами платежной системы;
- функциональные обязанности лиц, ответственных за управление рисками, либо соответствующих структурных подразделений;
- обязанность доведения до органов управления оператора платежной системы соответствующей информации о рисках;
- показатели бесперебойности функционирования Платежной системы в соответствии с требованиями нормативных актов Банка России;
- порядок обеспечения бесперебойности функционирования платежной системы в соответствии с требованиями нормативных актов Банка России;
- методику анализа рисков в платежной системе, включая профили рисков, в соответствии с требованиями нормативных актов Банка России;
- порядок обмена информацией, необходимой для управления рисками;
- порядок взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев;
- порядок изменения операционных и технологических средств и процедур;
- порядок оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией;
- порядок обеспечения защиты информации в платежной системе.

7.1.4. Участники, операторы УПИ самостоятельно осуществляют деятельность:

- по управлению рисками, присущими их виду деятельности, в том числе риск информационной безопасности, и несут ответственность за последствия реализации указанных рисков;
- по обеспечению защиты информации при осуществлении своей деятельности в рамках Платежной Системы;
- по обеспечению надлежащего функционирования операционных и технологических средств, устройств, информационных систем, используемых ими в работе с Платежной Системой;
- по обеспечению и контролю соблюдения собственными структурными подразделениями Правил Платежной Системы, заключенных договоров с Оператором Платежной Системы, привлеченным Расчетным центром (для Участников), законодательных требований;

▪по контролю за соблюдением привлеченными Участниками БПА, БПС условий их привлечения в целях принятия от физических лиц и (или) выдачи физическим лицам наличных денежных средств в рамках предоставления услуг Платежной Системы, а также законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма и требований к обеспечению защиты информации при осуществлении переводов денежных средств.

7.2. Мероприятия по управлению рисками.

Система управления рисками включает следующие мероприятия:

7.2.1. определение организационной структуры управления рисками, обеспечивающей контроль за выполнением Участниками требований к управлению рисками, установленных Правилами Системы;

7.2.2. определение подразделения Оператора Платежной Системы, обеспечивающие информационную безопасность, осуществляющее управление риском информационной безопасности Оператора Платежной Системы в целом в т.ч. анализирующие и оценивающие обеспечение защиты информации в Платежной Системе;

7.2.3. определение подразделения, осуществляющее эксплуатацию информационных систем Оператора Платежной Системы в целом, в том числе в функции которого входит обеспечение бесперебойности функционирования Оператора Платежной Системы в целом;

7.2.4. определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений Оператора Системы;

7.2.5. доведение до органов управления Оператора Системы соответствующей информации о рисках;

7.2.6. определение показателей бесперебойности функционирования Системы;

7.2.7. определение порядка обеспечения бесперебойности функционирования Системы;

7.2.8. определение методик анализа рисков в Системе, включая профили рисков;

7.2.9. определение порядка обмена информацией, необходимой для управления рисками;

7.2.10. определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев;

7.2.11. определение порядка изменения операционных и технологических средств и процедур;

7.2.12. определение порядка оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией;

7.2.13. определение порядка обеспечения защиты информации в Системе;

7.2.14. определение системы управления риском информационной безопасности Оператора Системы в целом, включая выполняемые им функции оператора УПИ;

7.2.15. в рамках Положения № 719-П Оператор определяет требования к обеспечению защиты информации, управляет риском информационной безопасности в Системе, выявляя недостатки следующих процессов в своей инфраструктуре, а также в инфраструктурах Субъектов ПС:

- технологических мер защиты информации;
- прикладного программного обеспечения.

Участники ПС реализуют процессы выявления, идентификации и анализа рисков информационной безопасности в отношении своих объектов информационной инфраструктуры, включая процессы реагирования на инциденты связанные с защитой информации и восстановления их штатного функционирования.

Оператор также определяет следующие мероприятия по управлению риском информационной безопасности в отношении Субъектов Системы:

- определение порядка обеспечения защиты информации, системы управления риском ИБ Оператора Системы в целом, включая выполняемые им функции оператора УПИ, которые фиксируются во внутренних документах Оператора Системы, не являющихся публичными;
- управление риском ИБ в Системе;
- определение требований к защите информации;
- определение состава показателей уровня риска ИБ в Системе;
- реализация Участниками и операторами УПИ механизмов, направленных на

- соблюдение требований к обеспечению защиты информации при осуществлении переводов денежных средств, и контроль их соблюдения Участниками и операторами УПИ;
- обеспечение реализации Участниками и операторами УПИ процессов выявления и идентификации риска ИБ в Системе в отношении объектов информационной инфраструктуры Участников и операторов УПИ;
- выявление и анализ Участниками и операторами УПИ риска ИБ;
- установление порядка, формы и сроков информирования Оператора Системы, Участников Системы и операторов УПИ о выявленных в Системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации;
- определение порядка взаимодействия Субъектов Системы в случае выявления в Системе вышеуказанных инцидентов;
- обеспечение реализации Участниками и операторами УПИ процессов реагирования на инциденты защиты информации и восстановления штатного функционирования объектов информационной инфраструктуры в случае реализации инцидентов защиты информации;
- установление требований к реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента;
- ведение Оператором базы событий инцидентов, приведших к реализации риска ИБ;
- в рамках проведения анализа рисков осуществление Оператором оценки соблюдения в Системе установленных требований к защите информации;
- реализация Оператором процессов применения в отношении Участников и операторов УПИ ограничений по параметрам операций в случае выявления факта превышения значений показателей уровня риска, в том числе условий снятия таких ограничений.

7.2.16. В рамках системы управления рисками в Системе Оператор Системы дополнительно определяет мероприятия, которые обязаны выполнять Участники – операторы по переводу денежных средств и операторы УПИ:

- управление риском ИБ, в качестве субъекта Системы, как одним из видов операционного риска;
- установление состава показателей уровня риска ИБ в Системе (Оператор Системы рекомендует устанавливать минимум два показателя: количество инцидентов нарушения информационной безопасности и размер убытков от инцидентов риска информационной безопасности);
- реализация процессов выявления и идентификации риска ИБ в Системе в отношении объектов информационной инфраструктуры участников Системы, операторов УПИ, задействованных при функционировании в Системе, включающие в себя следующие способы, но не ограничиваясь (в случае применимости):
  - анализ базы событий операционного риска, включающей события риска ИБ (далее База событий);
  - проведение ежегодной самооценки уровня операционного риска, включающего риск ИБ, и форм (способов) контроля, направленных на снижение его уровня, на основе формализованных анкет;
  - анализ динамики количественных показателей, направленных на измерение и контроль уровня операционного риска, включающего риск ИБ, в определённый момент времени (ключевых индикаторов риска);
  - анализ информации работников организации, полученной в рамках инициативного информирования работниками организации Службы управления рисками и (или) Службы внутреннего аудита;
  - анализ других внешних и внутренних источников информации и способов выявления рисков.

Результаты процедуры идентификации риска ИБ используются для проведения процедур количественной и качественной оценки уровня риска ИБ и корректного учета связи идентифицированного риска ИБ с событиями риска в Базе событий. Порядок ведения Базы событий подлежит определению во внутренних документах организации.

7.2.16.1 В целях выявления и идентификации рисков ИБ процессы выявления и идентификации рисков ИБ должны быть направлены на идентификацию событий, действий, условий, которые могут оказать влияние на информационные системы и бизнес-процессы, реализующие платежные услуги, операционные услуги, услуги платежного клиринга и/или расчетные услуги в рамках Системы, а также определение возможных последствий, анализ причин и источников возникновения событий рисков ИБ.

Выявление и анализ риска ИБ в Системе должен включать в себя:

- определение источников риска и событий (определение угроз информационной безопасности), реализация которых может привести к возникновению инцидента (риск-события), и определение для каждого из выявленных риск-событий величины риска, характеризуемого вероятностью наступления риск-событий и величиной возможных последствий их реализации;
- тестирования на проникновение в информационную инфраструктуру Участников, при тестировании каждой области оценивается возможности по компрометации безопасности ИТ систем Участников;
- использование специализированного программного обеспечения для выявления уязвимостей программного обеспечения;
- непрерывный мониторинг событий ИБ.

7.2.16.2 В целях минимизации последствий от реализации угроз информационной безопасности должны быть разработаны процессы реагирования на инциденты, в т.ч. планы восстановления штатного функционирования объектов информационной инфраструктуры. Процесс реагирования на инциденты защиты информации состоит из следующих последовательных этапов:

- локализация инцидента;
- выявление последствий инцидента;
- ликвидация последствий инцидента,
- проверке работоспособности элементов, подвергшихся воздействию инцидента.

Основными целями процесса реагирования на инциденты являются:

- не допустить или минимизировать последствия инцидента, сохраняя непрерывность деятельности в рамках Системы;
- обеспечить эффективное и своевременное восстановление работоспособности (штатного функционирования) информационных ресурсов;
- повысить уровень обеспечения информационной безопасности в организации и эффективность ведения деятельности по управлению инцидентами;
- реализация взаимодействия при обмене информацией об инцидентах защиты информации;
- анализ возникших нештатных ситуаций и их последствий;
- принятие мер по недопущению их повторного возникновения инцидента.

7.2.16.3 Оператор Системы в целях управления рисками осуществляет следующие мероприятия:

- определение организационной структуры управления рисками, обеспечивающей контроль за выполнением Участниками требований к управлению рисками, установленных Правилами Системы;
- определение подразделения Оператора Платежной Системы, обеспечивающие информационную безопасность, осуществляющее управление риском информационной безопасности Оператора Платежной Системы в целом в т.ч. анализирующие и оценивающие обеспечение защиты информации в Платежной Системе;
- определение подразделения, осуществляющее эксплуатацию информационных систем Оператора Платежной Системы в целом, в том числе в функции которого входит обеспечение бесперебойности функционирования Оператора Платежной Системы в целом;

- определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений Оператора Системы;
- доведение до органов управления Оператора Системы соответствующей информации о рисках;
- определение показателей бесперебойности функционирования Системы;
- определение порядка обеспечения бесперебойности функционирования Системы;
- определение методик анализа рисков в Системе, включая профили рисков;
- определение порядка обмена информацией, необходимой для управления рисками;
- определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев;
- определение порядка изменения операционных и технологических средств и процедур;
- определение порядка оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией;
- определение порядка обеспечения защиты информации в Системе;
- определение системы управления риском информационной безопасности Оператора Системы в целом, включая выполняемые им функции оператора УПИ.

7.2.16.4 Участники ПС реализуют процессы выявления, идентификации и анализа рисков информационной безопасности в отношении своих объектов информационной инфраструктуры, включая процессы реагирования на инциденты связанные с защитой информации и восстановления их штатного функционирования.

7.2.17. Участники и привлеченные Операторы УПИ обязаны выявлять Инциденты при оказании УПИ, связанные с приостановлением их оказания и восстановлением оказания УПИ, соответствующего требованиям к оказанию услуг, в случае нарушения указанных требований и предоставлять сведения о выявленных Инцидентах Оператору ПС в течение 12 (Двенадцати) часов с момента возникновения (выявления) Инцидента путем направления сообщения по Согласованным каналам связи. Форма предоставления сведений по выявленным Инцидентам приведена в Приложении 9 к настоящим Правилам.

7.2.18. Оператор ПС при выявлении нарушения порядка обеспечения БФПС Участниками или привлеченными Операторами УПИ:

- информирует Участников и привлеченных Операторов УПИ о выявленных в их деятельности нарушениях путем направления по Согласованным каналам связи официального письма и устанавливает сроки устранения нарушений;
- при необходимости совместно с Участником или привлеченным Оператором УПИ согласовывает мероприятия по устранению нарушений;
- осуществляет проверку результатов устранения нарушений и информирует о результатах проведенной проверки Участников и привлеченных Операторов УПИ, в деятельности которых выявлены нарушения, путем направления по Согласованным каналам связи официального письма.

7.2.19. При выявлении фактов неисполнения порядка обеспечения БФПС или неисполнения мероприятий по устранению выявленных нарушений привлеченными Операторами УПИ/Участниками Оператор ПС вправе приостановить участие такого Участника в Платежной системе или расторгнуть договор с привлеченным Оператором УПИ.

7.2.20. В случаях временного приостановления (прекращения) оказания ОУПИ Оператор ПС:

- в день приостановления (прекращения) оказания УПИ информирует:
  - Банк России (Департамент национальной платежной системы) — путем направления уведомления о приостановлении (прекращении) оказания услуг платежной инфраструктуры
  - по адресу электронной почты: SVC_DNPS_UONN@cbr.ru с подтверждением отправки по телефонам: 8 (495) 676-86-64, 8 (495) 771-49-25;
  - Участников и привлеченных Операторов УПИ (в случае их привлечения) — путем направления уведомлений по Согласованным каналам связи и (или) посредством размещения уведомления на Сайте Платежной системы в информационно-

телекоммуникационной сети Интернет в течение 2 (Двух) рабочих дней со дня приостановления (прекращения) оказания

- ОУПИ направляет в Банк России (Департамент национальной платежной системы) уведомление на бумажном носителе или в виде электронного сообщения, снабженного Кодом аутентификации.

7.2.21. Определение порядка взаимодействия Субъектов ПС в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев. При возникновении спорных и чрезвычайных ситуаций Участники и привлеченные Операторы УПИ (в случае их привлечения) незамедлительно информируют Оператора ПС о данных ситуациях, о причинах их возникновения и последствиях любым доступным Участнику способом, в т.ч, путем направления сообщения в свободном формате по Согласованным каналам связи. Допускается информирование Участником и привлеченным Оператором УПИ Оператора ПС о причинах возникновения спорной/чрезвычайной ситуации, если их выявление потребует проведение отдельного расследования, по завершении такого расследования по Согласованным каналам связи, но не позднее 5 (Пяти) рабочих дней с момента возникновения спорной/чрезвычайной ситуации.

7.2.22. Оператор ПС после получения информации в соответствии с п. 7.2.17 настоящих Правил определяет действия Участника(ов) и привлеченных Операторов УПИ с целью урегулирования ситуации. Конкретные действия определяются индивидуально по каждому обращению по договоренности Сторон.

7.2.23. В случае принятия решения о модернизации или замене используемых операционных и технологических средств и процедур Оператор ПС:

- разрабатывает технические требования на создание и внедрение новых операционных и технологических средств и процедур;
- по завершении разработки производит тестирование новых операционных и технологических средств и процедур;
- осуществляет внедрение новых операционных и технологических средств и процедур.

Информирование Участников о предполагаемых изменениях операционных и технологических средств и процедур Платежной системы осуществляется Оператором ПС путем публикации информации на Сайте Платежной системы с описанием планируемых изменений и сроков их внедрения. Срок, отведенный для ознакомления и направления замечаний и предложений по планируемым изменениям, устанавливается Оператором ПС, но не может быть менее 1 (Одного) месяца.

7.3. Способы управления рисками.

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

7.3.2. Система управления рисками предусматривает следующие способы управления рисками:

- осуществление расчета в пределах предоставленных Участниками денежных средств (в отношении прямых Участников, открывших банковские счета в Расчетном центре - Операторе Системы);
- автоматизированное управление очередностью исполнения распоряжений Участников - по времени поступления распоряжений (распоряжения исполняются в момент поступления при достаточности предоставленных денежных средств, в том числе за счет кредита, предоставленного прямым Участником, Расчетным центром);
- осуществление расчета в Системе до конца рабочего дня (в отношении прямых Участников, открывших банковские счета в Расчетном центре - Операторе Системы);
- установление предельных размеров (лимитов) обязательств в отношении Участников, открывших счета в привлеченном Расчетном центре, с учетом уровня риска.

Оператор Системы оставляет за собой право применять иные способы управления рисками, в том числе: анализ и изучение финансовой отчетности, других сведений и документов Участников, операторов услуг платежной инфраструктуры (при их наличии), а также анализ и изучение информации в СМИ, отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов.

7.4. Методика анализа рисков.

7.4.1. Выявление и анализ рисков в Платежной системе проводится Оператором с применением следующих элементов методик, основанных на статистическом и сценарном анализе функционирования системы и соответствующих **ГОСТ Р** 58771-2019 "Менеджмент риска. Технологии оценки риска":

- анализ, отслеживание и фиксирование параметров работы Участников в Платежной системе, в т. ч. соблюдение порядка расчетов согласно пункту 6.6. настоящих Правил;
- накопление и статистический анализ информации о нестандартных, спорных и чрезвычайных ситуациях, а также иных событий реализации рисков системы;
- оценка и ретроспективный анализ данных мониторинга показателей БФПС с целью выявления закономерностей и выработки мер по улучшению функционирования Платежной системы;
- стресс-тестирование рисков Платежной системы путем разработки стресс-сценариев, описывающих вероятные ситуации, угрожающие БФПС, на основе анализа информации об угрозах функционирования системы, описанных СМИ и другими источниками;
- анализ и оценка факторов риска, влияющих на бесперебойность предоставления услуг Платежной системы.

7.4.2. Методики анализа рисков в Платежной системе обеспечивают:

- выявление и анализ рисков в Платежной системе, включая выявление событий, реализация которых может привести к возникновению инцидента (далее - риск-события), и определение для каждого из выявленных риск-событий величины риска, характеризуемого вероятностью наступления риск-событий и величиной возможных последствий их реализации (далее - уровень риска);

- определение для каждого из выявленных рисков в Платежной системе уровня риска, имеющегося до применения способов управления рисками в Платежной системе (далее - уровень присущего риска), а также максимального уровня риска, при котором восстановление оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, включая восстановление оказания услуг платежной инфраструктуры в случае приостановления их оказания, осуществляется в течение периодов времени, установленных Оператором, и предполагаемый ущерб от которого Оператор готов принять без применения способов управления рисками в Платежной системе (далее - уровень допустимого риска);

- определение рисков в Платежной системе, для которых уровень присущего риска выше уровня допустимого риска (далее - значимые для платежной системы риски);

- определение уровня каждого из значимых для Платежной системы рисков после применения способов управления рисками в Платежной системе (далее - уровень остаточного риска).

7.4.3. Методики анализа рисков в Платежной системе предусматривают выполнение следующих мероприятий:

- формирование и поддержание в актуальном состоянии перечней бизнес-процессов (Приложение № 7 к Правилам);

- разработку и поддержание в актуальном состоянии классификаторов (структурированных перечней) рисков в Платежной системе, риск-событий, причин риск-событий;

- проведение анализа бизнес-процессов в платежной системе, включая анализ и оценку технологического обеспечения Операторов услуг платежной инфраструктуры и других факторов, влияющих на БФПС;

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

- определение уровня присущего риска для каждого из выявленных рисков в Платежной системе и установление уровня допустимого риска;

- сопоставление определенного уровня присущего риска и установленного уровня допустимого риска по каждому из выявленных рисков в Платежной системе для выделения значимых для Платежной системы рисков;

применение способов управления рисками в Платежной системе для каждого из значимых для Платежной системы рисков и последующее определение уровня остаточного риска для каждого из значимых для Платежной системы рисков;

- сопоставление уровней остаточного риска и допустимого риска для каждого из значимых для Платежной системы рисков и принятие решения о необходимости применения других способов управления рисками в Платежной системе в дополнение к ранее примененным способам;

- мониторинг рисков в Платежной системе, в том числе уровней остаточных рисков в Платежной системе, их соответствия уровню допустимого риска;

- составление и пересмотр (актуализацию) по результатам оценки рисков в Платежной системе и анализа эффективности мероприятий по восстановлению оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, профиля каждого из выявленных рисков в Платежной системе, включая профиль риска нарушения БФПС (далее - профили рисков) по форме Приложения № 7 к Правилам.

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

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

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

7.4.7. Оператор Системы в рамках системы управления рисками разрабатывает методику анализа рисков в платежной системе в соответствии с вышеуказанными требованиями. Операторы услуг платежной инфраструктуры, и Участники самостоятельно разрабатывают свою методику анализа рисков.

Оценка эффективности методики анализа рисков осуществляется на основании данных, представляемых Операторами услуг платежной инфраструктуры и Участниками по запросу Оператора, но не реже одного раза в год, а также на основании заключений аудиторских компаний, приглашаемых Оператором по мере необходимости.

7.4.8. Идентификация рисков осуществляется ОПДС и ОУПИ путем определения их видов и источников возникновения. Идентификация каждого события риска включает в себя определение:

- типа (вида) события риска;
- причины (источника) события риска;
- объекта события риска (вид деятельности / бизнес-процесс / документ);
- места возникновения события риска;
- типов возможных убытков по выявленным событиям риска.

7.4.9. Анализ рисков, предусматривает определение метода их измерения, определение вероятности наступления таких рисков и степени их воздействия на работоспособность ОИИ. В ходе анализа рисков делаются выводы об объектах риска, в которых реализованы/могут быть реализованы наибольшие риски (по частоте возникновения событий риска и по их тяжести (величине и существенности убытков), формулируются выводы о причинах/возможных причинах возникновения событий риска, а также выделяются факторы, приводящие к реализации риска. Анализ рисков осуществляется по каждому из видов риска, а также по совокупности рисков, реализация которых может быть взаимозависима. Методика оценки событий рисков разрабатывается на основе как количественных, так и качественных методов. Методы качественной оценки используются в случаях, когда невозможно получить достаточно надежные данные, требуемые для количественной оценки, либо получение и анализ таких данных оказываются слишком дорогостоящими. В отношении каждого из видов рисков определяется методология оценки риска, включая набор и источники данных, используемых для оценки. На основе статистки реализации событий риска и его влияния на деятельность Платежной системы осуществляется определение вероятности возникновения событий риска и количественная оценка их возможных последствий (степени воздействия). Вероятностные методы оценки используются по мере накопления необходимой статистики событий соответствующего риска.

7.4.10. Способами выявления рисков в отношении объектов информационной инфраструктуры (ОИИ) ОПДС и ОУПИ могут быть:

- проведение тестирования на проникновение и анализ уязвимостей на объектах информационной инфраструктуры, задействованных для работы в Системе не реже одного раза в год;
- проведение внешнего аудита на соответствие применяемых мер по защите информации требованиям, определенным для ОПДС и ОУПИ в соответствие с 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;

7.4.11. Информирование Оператора о выявленных в Системе рисков, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств осуществляется по по согласованным каналам связи.

7.5. Организационная структура системы управления рисками.

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

В соответствии со стратегическими планами развития Платежной системы «ХЕЛЛО» для реализации эффективной политики управления рисками в Платежной системе создается Комитет по управлению рисками. Комитет по управлению рисками Платежной системы «ХЕЛЛО» является постоянно действующим коллегиальным органом, в состав которого входят представители Оператора, РЦ и Участников.

Комитет по управлению рисками проводит оценку системы управления рисками в Платежной системе «ХЕЛЛО», в том числе используемых методов оценки рисков в Платежной системе, результатов применения способов управления рисками в Платежной системе, не реже одного раза в два года и документально оформляет результаты указанной оценки.

Оператор вносит изменения в систему управления рисками в Платежной системе «ХЕЛЛО» в случае, если действующая система управления рисками в Платежной системе не позволила предотвратить нарушение оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, а также восстановить оказание услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг в течение 24 часов, и (или) восстановить оказание услуг платежной инфраструктуры в случае приостановления их оказания в течение 6 часов. В полномочия Комитета входит принятие решений рекомендательного характера по вопросам управления рисками в отношении менеджмента Оператора, Участников и третьих лиц.

7.5.2. Оператор, Субъекты Платежной системы внутренними документами определяют должностное лицо или структурное подразделение, к обязанностям которых относится обеспечение мониторинга и проведение мероприятий, связанных с управлением рисками в Системе.

Указанные лица (структурные подразделения) подчиняются непосредственно исполнительному органу и/или единоличному исполнительному органу работодателя.

7.5.3. В состав органов управления рисками Оператора Платежной системы включаются:

- Генеральный директор;
- Руководитель отдела управлениями рисками;
- Руководитель отдела информационных технологий.

7.5.4. В функциональные обязанности и компетенцию органов управления рисками Оператора Системы входят, в частности:

- разработка и утверждение внутренних документов, регулирующих систему управления рисками, в том числе методики анализа рисков в Платежной системе;
- установление критериев оценки системы управления рисками, включая системный риск, проведения указанной оценки и формирование предложений и рекомендаций по итогам проведения оценки;
- установление предельных размеров (лимитов) обязательств Участников Платежной системы с учетом уровня рисков;
- установление допустимого уровня рисков нарушения бесперебойности функционирования Платежной системы;
- принятие мер по обеспечению бесперебойности функционирования Платежной системы и минимизации уровня рисков;
- осуществление контроля за уровнем рисков;
- проведение оценки эффективности системы управления рисками Платежной системы и ее совершенствование в порядке, установленном внутренними документами оператора Системы.

7.6. Доведение до органов управления рисками сведений о рисках.

7.6.1. Информация о выявленных рисках незамедлительно предоставляется должностным лицом (структурным подразделением), ответственным за управление рисками, исполнительному органу и/или единоличному исполнительному органу Оператора или Субъекта Платежной системы в виде письменных отчетов по итогам проверок деятельности Оператора или Субъекта Системы, содержащих подробное описание характера риска, вероятных причин его возникновения и возможных последствий.

7.6.2. Информация об общем уровне рисков Платежной системы доводится до сведения общего собрания участников ООО «ХЕЛЛО» не реже одного раза в год.

8. Порядок обеспечения бесперебойности функционирования Платежной системы «ХЕЛЛО».

8.1. Терминология главы 8 Правил.

Для целей настоящей главы используются следующие понятия:

8.1.1. *Риск нарушения БФПС* – возможность приостановления (прекращения) осуществления или ненадлежащего осуществления переводов денежных средств либо нарушений законных интересов Участников платежной системы, Плательщиков вследствие неблагоприятного стечения обстоятельств (наступления событий), связанных с внутренними и внешними факторами функционирования Платежной системы (факторами риска нарушения БФПС).

8.1.2. *Обеспечение БФПС* – скоординированная деятельность Субъектов платежной системы, направленная на достижение, подтверждение и поддержание допустимого уровня риска нарушения БФПС, под которым понимается вероятность возникновения на заданном отрезке времени неблагоприятных последствий для БФПС с учетом размера причиняемого ущерба. Обеспечение БФПС осуществляется посредством управления рисками Платежной системы.

8.1.3. *Функционирование Платежной системы* – взаимодействие Оператора платежной системы, Участников платежной системы, Операторов услуг платежной инфраструктуры, привлеченных Оператором платежной системы на договорной основе (в случае привлечения), в целях осуществления переводов денежных средств.

8.1.4. *Надлежащее функционирование Платежной системы* – функционирование Платежной системы в соответствии с требованиями законодательства Российской Федерации, Правил, договоров, соглашений с Субъектами платежной системы, определяющих условия и порядок ее функционирования.

8.1.5. *Бесперебойность функционирования Платежной системы (БФПС)* – комплексное свойство Платежной системы, обозначающее ее способность предупреждать нарушения надлежащего функционирования (в том числе не допускать приостановления (прекращения) осуществления или ненадлежащего осуществления переводов денежных средств), а также восстанавливать надлежащее функционирование в случае его нарушения.

8.2. Показатели бесперебойности Платежной системы «ХЕЛЛО».

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 платежной системы, ответственного за их реализацию.

8.2.1. Оператор, в соответствии с нормативными документами, определяет следующие показатели БФПС:

8.2.1.1. **Показатель 1 (П1)** - показатель продолжительности восстановления оказания услуг платежной инфраструктуры, характеризующий период времени восстановления оказания услуг Операторами услуг платежной инфраструктуры в случае приостановления оказания услуг платежной инфраструктуры, в том числе вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России от 04.06.2020 года № 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». Рассчитывается по каждому из Операторов услуг платежной инфраструктуры и по каждому из инцидентов, повлекших приостановление оказания услуг платежной инфраструктуры, как период времени с момента приостановления оказания услуг платежной инфраструктуры вследствие инцидента, произошедшего у Оператора услуг платежной инфраструктуры, и до момента восстановления оказания услуг платежной инфраструктуры;

8.2.1.2. **Показатель 2 (П2) -** показатель непрерывности оказания услуг платежной инфраструктуры, характеризующий период времени между двумя последовательно произошедшими в Платежной системе инцидентами, в результате которых приостанавливалось оказание услуг платежной инфраструктуры. Приостановление (прекращение) участия в Платежной системе в случаях, предусмотренных настоящими Правилами в соответствии с пунктом 4 части 1 статьи 20 Закона о НПС не рассматривается в качестве инцидентов. Рассчитывается по каждому из Операторов услуг платежной инфраструктуры при возникновении каждого из инцидентов, повлекших приостановление оказания услуг платежной инфраструктуры, как период времени между двумя последовательно произошедшими у Оператора услуг платежной инфраструктуры инцидентами, в результате которых приостанавливалось оказание услуг платежной инфраструктуры, с момента устранения первого инцидента и до момента возникновения следующего;

8.2.1.3. **Показатель 3 (П3) -** показатель соблюдения регламента, характеризующий соблюдение Операторами услуг платежной инфраструктуры времени начала, времени окончания, продолжительности и последовательности процедур, выполняемых Операторами услуг платежной инфраструктуры при оказании операционных услуг, услуг платежного клиринга и расчетных услуг, предусмотренных частями 3 и 4 статьи 17, частью 4 статьи 19 и частями 1 и 8 статьи 25 Закона о НПС и настоящими Правилами. Рассчитывается ежемесячно по каждому Оператору услуг платежной инфраструктуры и по Платежной системе «ХЕЛЛО» в целом;

8.2.1.4. **Показатель 4 (П4) -** показатель доступности Операционного центра Платежной системы «ХЕЛЛО», характеризующий оказание операционных услуг Операционным центром Платежной системы «ХЕЛЛО». Рассчитывается ежемесячно по Операционному центру и по Платежной системе «ХЕЛЛО» в целом;

8.2.1.5. **Показатель 5 (П5) -** показатель изменения частоты инцидентов, характеризующий темп прироста частоты инцидентов. Рассчитывается ежемесячно для каждого Оператора услуг платежной инфраструктуры и по Платежной системе «ХЕЛЛО» в целом.

Порядок определения (расчета) показателей БФПС указан в Приложении № 7 к Правилам.

8.2.2. Оператор устанавливает и пересматривает с использованием результатов оценки рисков в Платежной системе «ХЕЛЛО» пороговые уровни показателей БФПС, указанные в Приложении № 7 к Правилам.

Оператор рассчитывает и анализирует значения показателей БФПС, в том числе путем их сравнения с пороговыми уровнями показателей БФПС, и использует результаты указанного анализа при оценке системы управления рисками в Платежной системе «ХЕЛЛО» и при оценке влияния инцидентов на БФПС.

Для оценки показателя БФПС в Платежной системе применяется показатель доступности (услуги, Субъекта Платежной системы в целом) в среднем в течение заданного временного интервала.

Факторы, влияющие на БФПС:

- финансовое состояние Участников платежной системы;
- предусмотренные в Платежной системе способы управления ликвидностью и обеспечения исполнения обязательств Участников платежной системы (в сочетании с требованиями, предъявляемыми к финансовому состоянию Участников платежной системы);
- финансовое состояние Операторов услуг платежной инфраструктуры;
- надежность технической инфраструктуры;
- технологическое обеспечение Операторов услуг платежной инфраструктуры, Участников платежной системы;
- возможность выявления неурегулированных вопросов правового характера, касающихся

взаимоотношений Субъектов платежной системы;

- возможность возникновения конфликта интересов Субъекта платежной системы при осуществлении им деятельности, направленной на достижение собственных целей и целей, установленных в рамках Платежной системы (в том числе по обеспечению БФПС);
- зависимость от внешних поставщиков услуг;
- рыночные и инфраструктурные факторы;
- иные внешние и внутренние факторы, в соответствии с особенностями функционирования Платежной системы.

8.3. **Управление непрерывностью функционирования Платежной системы «ХЕЛЛО».**

Оператор управляет непрерывностью функционирования Платежной системы с учетом следующихтребований.

Оператор организует деятельность по управлению непрерывностью функционирования Платежной системы «ХЕЛЛО», в том числе путем установления прав и обязанностей Субъектов Платежной системы по управлению непрерывностью функционирования Платежной системы в зависимости от организационной модели управления рисками в платежной системе, определенной в соответствии с требованиями части 2 статьи 28 Закона о НПС и указанной в п.7.1.1 настоящих Правил.

Оператор Системы устанавливает следующие права и обязанности Субъектов Системы по управлению непрерывностью функционирования Системы с учетом модели управления рисками в Системе:

Оператор, Участники Системы и операторы УПИ самостоятельно управляют непрерывностью своей деятельности, влияющей на функционирование Платежной Системы «ХЕЛЛО», в т.ч. в части обслуживания клиентов – физических и юридических лиц, банков – корреспондентов;

Для обеспечения БФПС Участники Платежной Системы обязаны осуществлять:

- меры, направленные на недопущение нарушений функционирования операционных и технологических средств, устройств, информационных систем, обеспечивающих взаимодействие с Платежной Системой, учет информации о переводах денежных средств по Платежной Системе, в которых данный Участник выступает Участником-Отправителем или Участником-Получателем, о состоянии расчетов с Оператором Системы и Клиентами, а в случае возникновения указанных нарушений осуществляет меры по их устранению;
- анализ причин нарушений функционирования операционных и технологических средств, устройств, информационных систем, выработку и реализацию мер по их устранению;
- обеспечение сохранения функциональных возможностей операционных и технологических средств, устройств, информационных систем при сбоях в их работе (отказоустойчивость), проведение их тестирования в целях выявления недостатков функционирования, а в случае выявления указанных недостатков - принятие мер по их устранению;
- выявление и идентификацию, анализ рисков нарушения своего надлежащего функционирования в рамках Системы, в т.ч. риска ИБ, в отношении объектов информационной инфраструктуры участников платежной системы и операторов УПИ, оценку эффективности методик анализа и минимизации выявленных рисков, а также выявление новых рисков в рамках внутренних систем управления рисками в своей деятельности в части выполнения функций Участника;
- меры, направленные на поддержание остатка денежных средств на своих банковских счетах, используемых для осуществления расчетов по операциям в Платежной Системе, достаточного для осуществления бесперебойных расчетов, а также меры по обеспечению достаточных наличных денежных средств в своих кассовых подразделениях для своевременной выплаты переводов.

Для обеспечения БФПС операторы УПИ обязаны осуществлять:

- меры, направленные на недопущение нарушений функционирования операционных и технологических средств, устройств, информационных систем, обеспечивающих

взаимодействие с Платежной Системой, а также осуществление расчетов по счетам Участников, учет информации о состоянии расчетов, а в случае возникновения указанных нарушений осуществляет меры по их устранению;

- анализ причин нарушений функционирования операционных и технологических средств, устройств, информационных систем, выработку и реализацию мер по их устранению;
- обеспечение сохранения функциональных возможностей операционных и технологических средств, устройств, информационных систем при сбоях в их работе (отказоустойчивость), проведение их тестирования в целях выявления недостатков функционирования, а в случае выявления указанных недостатков – принятие мер по их устранению;
- выявление и анализ рисков нарушения надлежащего функционирования в рамках Системы, в т.ч. риска ИБ, в отношении объектов информационной инфраструктуры участников платежной системы и операторов УПИ, оценку эффективности методик анализа и минимизации выявленных рисков, а также выявление новых рисков в рамках внутренних систем управления рисками своей деятельности в части выполнения функций оператора УПИ.

Для обеспечения БФПС Расчетный Центр обязан осуществлять:

- меры, направленные на недопущение нарушений функционирования операционных и технологических средств, устройств, информационных систем, обеспечивающих взаимодействие с Платежной Системой, учет информации о переводах денежных средств по Платежной Системе, в которых данный Участник выступает Участником-Отправителем или Участником-Получателем, о состоянии расчетов с Оператором Системы и Клиентами, а в случае возникновения указанных нарушений осуществляет меры по их устранению;
- анализ причин нарушений функционирования операционных и технологических средств, устройств, информационных систем, выработку и реализацию мер по их устранению;
- обеспечение сохранения функциональных возможностей операционных и технологических средств, устройств, информационных систем при сбоях в их работе (отказоустойчивость), проведение их тестирования в целях выявления недостатков функционирования, а в случае выявления указанных недостатков - принятие мер по их устранению;
- анализ рисков нарушения своего надлежащего функционирования в рамках Платежной Системы, оценку эффективности методик анализа и минимизации выявленных рисков, а также выявление новых рисков в рамках внутренних систем управления рисками своей деятельности в части выполнения функций Расчетного центра Системы;
- обеспечение собственной финансовой устойчивости, а именно – поддержание ликвидности, соблюдения экономических нормативов, поддержания финансовых показателей в соответствии с требованиями Банка России.

Субъекты Системы в целях обеспечения БФПС имеют право осуществлять дополнительные меры по своему усмотрению.

Для обеспечения БФПС Оператор Системы, выполняя в т.ч. функции ОЦ, ПКЦ обязан осуществлять:

- меры, направленные на недопущение нарушений функционирования операционных и технологических средств, устройств, информационных систем, обеспечивающих взаимодействие с Участниками, операторами УПИ, доступность Платежной Системы, учет информации о переводах, платежных позициях Участников и состоянии расчетов (организация бесперебойности электропитания, дублирование каналов связи и вычислительных мощностей, резервное копирование баз данных Платежной Системы «ХЕЛЛО», защита информационных систем от воздействия вредоносного программного обеспечения и т.д.), а в случае возникновения указанных нарушений осуществляет меры по их устранению;
- анализ причин нарушений функционирования операционных и технологических средств, устройств, информационных систем, выработку и реализацию мер по их устранению;
- обеспечение сохранения функциональных возможностей операционных и технологических средств, устройств, информационных систем при сбоях в их работе (отказоустойчивость), проведение их тестирования в целях выявления недостатков функционирования, а в случае выявления указанных недостатков - принятие мер по их устранению;

- выявление оказания УПИ, не соответствующего требованиям к оказанию услуг;
- обеспечение функционирования Системы в случае нарушения оказания УПИ, соответствующего требованиям к оказанию услуг;
- обеспечение собственной финансовой устойчивости (при выполнении функций ЦПКК), а именно – поддержание ликвидности, соблюдения экономических нормативов, поддержания финансовых показателей в соответствии с требованиями Банка России, обеспечение достаточности денежных средств на счетах ЦПКК в привлеченном Расчетном центре.

Оператор Системы, операторы УПИ обязаны иметь планы обеспечения непрерывности деятельности и восстановления деятельности (далее – ПОНиВД), а также обеспечить их тестирование и пересмотр не реже одного раза в два года.

Оператор организует сбор и обработку сведений, в том числе от привлеченных Операторов услуг платежной инфраструктуры, используемых для расчета показателей БФПС, указанных в п. 8.2.1 настоящих Правил (далее - сведения по Платежной системе), а также следующих сведений об инцидентах:

- время и дата возникновения инцидента (в случае невозможности установить время возникновения инцидента указывается время его выявления);

- краткое описание инцидента (характеристика произошедшего события и его последствия);

- наименование взаимосвязанных последовательных технологических процедур, выполняемых при оказании услуг платежной инфраструктуры (далее - бизнес-процесс), в ходе которых произошел инцидент;

- наименование бизнес-процесса, на который оказал влияние инцидент;

- наличие (отсутствие) факта приостановления (прекращения) оказания услуг платежной инфраструктуры в результате инцидента;

- влияние инцидента на БФПС, определяемое с учетом требований, предусмотренных настоящим пунктом Правил;

- степень влияния инцидента на функционирование Платежной системы в зависимости от количества Операторов услуг платежной инфраструктуры, и (или) количества и значимости Участников Платежной системы, на которых оказал непосредственное влияние инцидент, и (или) количества и суммы неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных распоряжений Участников Платежной системы, и иных факторов;

- время и дата восстановления оказания услуг платежной инфраструктуры в случае приостановления их оказания;

- мероприятия по устранению инцидента и его неблагоприятных последствий с указанием планируемой и фактической продолжительности проведения данных мероприятий;

- дата восстановления оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг;

- неблагоприятные последствия инцидента по Субъектам Платежной системы, в том числе:

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

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

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

продолжительность приостановления оказания услуг платежной инфраструктуры.

Оператор обеспечивает хранение сведений по Платежной системе и сведений об инцидентах не менее трех лет с даты получения указанных сведений.

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

Оператор, Участники и Операторы услуг платежной инфраструктуры организуют деятельность по реализации порядка обеспечения БФПС в рамках внутренних систем управления рисками своей деятельности. В целях управления рисками нарушения БФПС в Системе Оператор запрашивает и получает от Участников и Операторов услуг платежной инфраструктуры информацию, необходимую для управления рисками нарушения БФПС. Оператор систематизирует, обрабатывает, накапливает и хранит данную информацию.

Оператор Системы осуществляет контроль за соблюдением Участниками и Операторами услуг платежной инфраструктуры порядка обеспечения БФПС как в рамках осуществления контроля за соблюдением Правил Системы в целом, так и с помощью направления запросов о предоставлении информации, необходимой Оператору Системы для осуществления вышеуказанного контроля.

Оператор определяет ответственность Операторов услуг платежной инфраструктуры и Участников за неисполнение порядка обеспечения БФПС. Каждый Субъект Платежной системы несет индивидуальную ответственность за невыполнение / несоблюдение мер по обеспечению БФПС, закрепленных в настоящем пункте Правил соответственно выполняемому функционалу, меру ответственности устанавливает Оператор в соответствии с п.28 настоящих Правил. Оператор рассматривает неисполнение порядка обеспечения БФПС, определенного в настоящих Правилах, в том числе, как несоблюдение Правил.

Оператор несет ответственность за реальный ущерб, причиненный Участникам платежной системы вследствие неоказания (ненадлежащего оказания) услуг платежной инфраструктуры в случае их осуществления (за исключением услуг Расчетного центра), при этом ответственность Оператора за реальный ущерб ограничена размером неустойки, за исключением случаев умышленного неоказания (ненадлежащего оказания) услуг платежной инфраструктуры (за исключением услуг Расчетного центра). Размер неустойки определяется как размер реального ущерба, причиненного Участнику платежной системы. Факт причинения и размер реального ущерба доказывается Участником самостоятельно

Оператор проводит оценку влияния на БФПС каждого произошедшего в Платежной системе «ХЕЛЛО» инцидента в течение 24 часов с момента его возникновения (выявления), а также в течение 24 часов после устранения инцидента (восстановления оказания УПИ, соответствующего требованиям к оказанию услуг).

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

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

- нарушен регламент выполнения процедур при одновременном нарушении порогового уровня показателя П2;

- нарушен пороговый уровень показателя П1;

- превышена продолжительность установленного Оператором времени, в течение которого должно быть восстановлено оказание услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг.

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

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

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

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

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

8.3.1. Способы обеспечения БФПС Оператором Платежной системы «ХЕЛЛО».

Обеспечение БФПС Оператором платежной системы осуществляется путем:

- осуществления координации деятельности Субъектов платежной системы по обеспечению БФПС, проведение которой определяется настоящими Правилами. Оператор непосредственно осуществляет координацию деятельности субъектов платежной системы по обеспечению БФПС в следующем порядке: Правила устанавливают основные требования к деятельности субъектов по обеспечению БФПС и реализации ими мероприятий системы управления рисками. Субъекты обязаны выполнять реализовать установленные мероприятия в рамках собственной системы управления рисками руководствуясь требованиями настоящих Правил;
- установления Отделом управлениями рисками не реже одного раза в квартал допустимого уровня риска нарушения БФПС;
- выявления факторов риска нарушения БФПС, определения степени и характера влияния указанных факторов на БФПС, проведения оценки соответствия уровня риска нарушения БФПС предельно допустимому уровню;
- проведения мониторинга изменений характера и степени влияния факторов риска;
- проведения расследований событий, вызвавших операционные сбои, анализ их причин и последствий;
- проведения оценки рисков, присущих видам деятельности Оператора платежной системы для обеспечения непрерывности деятельности Платежной системы;
- принятия мер по устранению или минимизации рисков нарушения БФПС. К Участникам платежной системы применяются штрафные санкции, предусмотренные договором, использование обеспечительных мер, приостановление деятельности в Платежной системе (временное или постоянное), в случае несоответствия установленному уровню обеспечения бесперебойности;
- проведения оценки и мониторинга финансовой устойчивости Участников платежной системы, факторов, несущих риски потери финансовой устойчивости Участников платежной системы, в том числе потенциальных, способных привести к потере финансовой устойчивости Участников платежной системы в будущем;

- осуществления контроля соблюдения требований Правил, договорных обязательств, соблюдения порядка обеспечения БФПС операторами услуг платежной инфраструктуры и Участниками платежной системы;
- проведения регулярных проверок Участников платежной системы на предмет соблюдения условий осуществления переводов денежных средств, требований настоящих Правил; контроль за соблюдением условий может осуществляться как путем выездных проверок, так и направлением запросов Платежной системы о предоставлении требуемой информации;
- осуществления контроля использования наименования и товарных знаков Платежной системы исключительно в рамках заключенных договоров, соглашений и настоящих Правил;
- обеспечения сохранения функциональных возможностей операционных и технических средств, информационных систем при сбоях, проведение тестирования для выявления недостатков, принятие мер по устранению выявленных недостатков;
- доведения информации о возникающих рисках нарушения БФПС до органов управления Оператора платежной системы.
- выявления Оператором организаций, предоставляющих участникам, их клиентам услуги платежной инфраструктуры, в том числе в случаях, если услуги платежной инфраструктуры оказываются единственному участнику или ограниченному числу участников и (или) их клиентов
- обеспечения возможности для Участников осуществить переход в течение не более 10 рабочих дней, на обслуживание к другому РЦ, в случае нарушения обслуживающим их РЦ требований к бесперебойности оказания услуг платежной инфраструктуры, в том числе приостановления (прекращения) оказания услуг.

8.3.2. Способы обеспечения БФПС Операторами услуг платежной инфраструктуры.

Обеспечение БФПС Операторами услуг платежной инфраструктуры осуществляется путем:

- выполнения функций по управлению риском нарушения БФПС, возложенных на них установленным порядком обеспечения БФПС, в соответствии с организационной моделью управления рисками в Платежной системе;
- сбора и обработки доступной Операторам услуг платежной инфраструктуры информации и времени поступления в Платежную систему распоряжений Участников платежной системы по переводам денежных средств, ходе исполнения указанных распоряжений, характеристиках осуществляемых переводов денежных средств, количестве, сумме и времени наступления окончательности переводов, размере клиринговых позиций и остатках денежных средств на Счетах Участников платежной системы;
- письменного информирования (в соответствии с Порядком электронного документооборота, Приложении 2 к Правилам) Оператора платежной системы о событиях, вызвавших операционные сбои, об их причинах и последствиях, а также в случае возникновения или реализации угрозы неисполнения или ненадлежащего исполнения Участниками платежной системы принятых на себя обязательств;
- организации и осуществления деятельности по обеспечению бесперебойности оказания услуг Участникам платежной системы в соответствии с принятыми на себя обязательствами и требованиями порядка обеспечения БФПС;
- обеспечения непрерывности деятельности и/или восстановления деятельности по оказанию услуг платежной инфраструктуры, нарушенной в результате непредвиденных обстоятельств, в сроки и в соответствии с требованиями, установленными порядком обеспечения БФПС;
- регулярной оценки качества и надежности функционирования применяемых информационных систем, работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается Оператором платежной системы, Участниками платежной системы, их совершенствования.

8.3.3. Способы обеспечения БФПС Участниками.

Обеспечение БФПС Участниками платежной системы осуществляется путем:

- проведения оценки рисков, присущих его виду деятельности, для обеспечения непрерывности деятельности;
- принятия мер по обеспечению соответствия требованиям Платежной системы и надлежащего исполнения принятых на себя обязательств;
- предоставления Оператору платежной системы в электронном виде финансовых отчетов (баланс, расчет обязательных экономических нормативов, расчет собственных средств и отчет о прибылях и убытках) на каждую отчетную дату[1], по запросу Оператора платежной системы (в случае отсутствия на официальном сайте Банка России, национального банка).
- информирования Оператора платежной системы о случаях неоказания или ненадлежащего оказания услуг, предоставляемых в рамках Платежной системы, и событиях, вызвавших операционные сбои, а также о событиях, вызвавших спорные, нестандартные и чрезвычайные ситуации, включая случаи системных сбоев, об их причинах и последствиях;
- осуществления контроля соблюдения требований законодательства, настоящих Правил, договоров и условий осуществления переводов денежных средств;
- осуществления контроля использования наименования и товарных знаков Платежной системы исключительно в рамках заключенных договоров и настоящих Правил.

Оператор обеспечивает оказание услуг платежной инфраструктуры при возникновении инцидентов, а также организует в течение 6 часов восстановление оказания услуг Операторами услуг платежной инфраструктуры в случае приостановления их оказания и в течение 24 часов восстановление оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, в случае нарушения указанных требований.

8.4. Требования к уровню бесперебойности оказания операционных услуг.

Уровень доступности оказания операционных услуг:

- показатель информационно-технологической готовности Банкоматов, Платежных терминалов, Системы удаленного доступа - 97 % времени в течение операционного дня;
- количество аварий, сбоев по вине Операционного центра, влияющих на информационно-технологическую готовность Банкоматов, Платежных терминалов, Системы удаленного доступа - не более пяти аварий, сбоев в квартал;
- количество отказов в приеме от Расчетного центра сообщений об остатках денежных средств на Счетах Участников платежной системы – не более 1 (одного) раза в месяц;
- количество отказов в приеме от Участника платежной системы сообщений о лимите расходования средств Счета – не более 2 (Двух) раз в месяц.

Уровень непрерывности оказания операционных услуг:

- показатель количества обрабатываемых операций – 100% операций;
- время на обработку запроса на совершение операции не более 25 (двадцати пяти) секунд;
- время на прием и первичную обработку сообщений от Расчетного центра об остатках денежных средств на Счетах участника платежной системы– не более 1 (Одного) часа;
- показатель временных потерь по фиксируемым случаям сбоев информационно-технологических систем – не более 4 (четырех) часов в месяц.

В случае нарушения надлежащего функционирования Операционного центра продолжительность периода времени, в течение которого должно быть восстановлено надлежащее функционирование не должно превышать 24 часа.

---

[1]Для российских кредитных организаций периодичность предоставления информации – ежемесячно,
для иностранных кредитных организаций периодичность предоставления информации – в соответствии стребованиями национального банка.

8.5. Требования к уровню бесперебойности оказания расчетных услуг.

Уровень доступности оказания расчетных услуг:

- показатель временных потерь по фиксируемым случаям сбоев информационно-технологических систем, влияющих на принятие расчетным центром Реестра, – не более 4 (четырех) часов в месяц.

Уровень непрерывности оказания расчетных услуг:

- показатель достаточности денежных средств для осуществления расчетов – отношение остатка денежных средств на момент осуществления расчетов на счете Расчетного центра, открытом в обслуживающем подразделении расчетной сети Банка России, к сумме совершенных операций по переводу денежных средств, по которым осуществляется расчет – коэффициент ≥ 1;
- показатель количества обрабатываемых в соответствии с Правилами распоряжений на перевод денежных средств – 100%;
- количество допущенных ошибок при проведении операций по списанию/зачислению денежных средств по Счетам Участников платежной системы – 0;
- соблюдение Расчетным центром обязательных нормативов, установленных Банком России.

В случае нарушения надлежащего функционирования Расчетного центра. продолжительность периода времени, в течение которого должно быть восстановлено надлежащее функционирование не должно превышать 24 часа.

8.6. **Требования к уровню бесперебойности оказания услуг платежного клиринга.**

Услуги платежного клиринга в платежной системе оказываются ежедневно по рабочим дням.

Уровень бесперебойности и доступности оказания услуг Платежного клиринга:

- нарушение сроков предоставления Реестра Расчетному центру для осуществления расчетов – не более 9 (девяти) раз в год;
- нарушение сроков предоставления Участникам платежной системы отчетов об операциях, совершенных Плательщиками в целях перевода денежных средств в течение операционного дня, расчеты по которым осуществляются за счет Участника платежной системы, – не более 9 (девяти) раз в год.

Уровень непрерывности оказания услуг Платежного клиринга:

- нарушение сроков определения платежной клиринговой позиции Участника платежной системы не более 9 (девяти) раз в год;
- количество допущенных ошибок при определении платежной клиринговой позиции Участника платежной системы– 0.

В случае нарушения надлежащего функционирования Платежного клирингового центра. продолжительность периода времени, в течение которого должно быть восстановлено надлежащее функционирование не должно превышать 24 часа.

8.7. Уровень риска нарушения БФПС.

Уровень риска нарушения БФПС определяется Оператором в Положение по управлению рисками и бесперебойности функционирования ПС «ХЕЛЛО (Приложении №7 к настоящим Правилам)

8.8. Требования к содержанию деятельности по обеспечению БФПС, осуществляемой Оператором, Участниками, Операторами услуг платежной инфраструктуры.

8.8.1. В рамках деятельности по управлению рисками нарушения БФПС Оператор Системы осуществляет:

-определение допустимого уровня рисков нарушения БФПС на регулярной основе в разрезе категорий субъектов платежной системы;

-анализ рисков нарушения БФПС;

-порядок выбора и реализацию мероприятий и способов, направленных на достижение или поддержание приемлемого уровня рисков нарушения БФПС;

-мониторинг рисков нарушения БФПС на регулярной основе;

-организацию информационного взаимодействия субъектов Системы в целях управления рисками нарушения БФПС.

Оператор разрабатывает, тестирует и пересматривает план действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности (далее - план ОНиВД) Оператора Платежной системы «ХЕЛЛО», с периодичностью не реже одного раза в два года. Оператор разрабатывает и включает в план ОНиВД мероприятия, направленные на управление непрерывностью функционирования Платежной системы в случае возникновения инцидентов, связанных с приостановлением оказания услуг платежной инфраструктуры или нарушением установленных уровней оказания услуг платежной инфраструктуры, в том числе:

- при наличии в Платежной системе двух и более Расчетных центров - мероприятия по обеспечению взаимозаменяемости данных Операторов услуг платежной инфраструктуры;

- при наличии в Платежной системе одного Операционного, и (или) Платежного клирингового центров - мероприятия по привлечению другого Оператора услуг платежной инфраструктуры и по переходу Участников Платежной системы на обслуживание к вновь привлеченному Оператору услуг платежной инфраструктуры в течение 10 рабочих дней в случаях:

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

нарушения Правил Платежной системы «ХЕЛЛО», выразившегося в отказе Оператора услуг платежной инфраструктуры в одностороннем порядке от оказания услуг Участнику (Участникам) Платежной системы, не связанного с приостановлением (прекращением) участия в Платежной системе в случаях, предусмотренных настоящими Правилами.

Оператор обеспечивает реализацию указанных выше мероприятий.

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

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

Оператор передает часть функций по реализации мероприятий по управлению рисками и непрерывностью функционирования Платежной системы «ХЕЛЛО» Операторам услуг платежной инфраструктуры и Участникам Платежной системы.

8.8.2. Операторы услуг платежной инфраструктуры для обеспечения бесперебойного оказания услуг платежной инфраструктуры, предоставляемых Участникам и их клиентам, осуществляют следующее:

- разрабатывают планы восстановления деятельности после сбоев функционирования операционной и клиринговой системы;

- определяют допустимые технологические перерывы в оказании операционных и клиринговых услуг на основании оценки допустимого уровня рисков;

- осуществляют сбор и обработку информации об инцидентах, вызвавших операционные сбои в Системе;

- обеспечивают наличие резервирования компонентов сетевой, вычислительной инфраструктуры и систем электроснабжения и охлаждения;

- обеспечивают регулярное резервное копирование данных Системы;

- обеспечивают наличие территориально удаленного резервного центра обработки данных для восстановления функционирования Системы в случае наступления кризисной ситуации в основном центре обработки данных;

- обеспечивает проведение оценки качества и функционирования информационных систем, операционных и технологических средств, применяемых Оператором Системы (раздел 9).

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

8.9.1. Оператор организует взаимодействие Субъектов Платежной системы «ХЕЛЛО» по обеспечению БФПС с учетом следующих требований.

Оператор определяет порядок взаимодействия Субъектов Платежной системы при реализации мероприятий по управлению рисками и непрерывностью функционирования Платежной системы «ХЕЛЛО» с учетом организационной модели управления рисками в Платежнойсистеме, определенной в соответствии с требованиями части 2 статьи 28 Закона о НПС и п.7.1.1 настоящих Правил.

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

Операторы услуг платежной инфраструктуры незамедлительно и оперативно информируют Оператора о нарушении оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, при котором превышено время восстановления оказания услуг платежной инфраструктуры, в случае их приостановления и (или) время восстановления оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг посредством электронной почты, а также по согласованным каналам связи.

Информация о нарушении оказания услуг платежной инфраструктуры незамедлительно предоставляется исполнительным органом или должностным лицом (структурным подразделением), ответственным за управление рисками, Оператора услуг платежной инфраструктуры исполнительному органу и/или должностному лицу (структурному подразделению), ответственному за управление рисками, Оператора.

С целью обеспечения БФПС Оператор Системы, Операторы услуг платежной инфраструктуры, и Участники осуществляют информационное взаимодействие. Обмен информацией осуществляется посредством электронной почты, а также по согласованным каналам связи.

8.9.2. С целью организации работы по обеспечению БФПС Оператор соблюдает порядок обеспечения бесперебойности функционирования Платежной системы в соответствии с разработанными документами Оператора. С целью организации работы по обеспечению БФПС Субъекты ПС обязаны соблюдать порядок обеспечения бесперебойности функционирования Платежной системы в соответствии с Правилами.

8.9.3. Субъектам Системы рекомендуется разработать следующие регламентирующие документы:

- план действий сотрудников в ходе нештатных ситуаций;
- политика информационной безопасности;
- политика защиты от вредоносного кода;
- политика использования сети Интернет;
- политика резервного копирования.

8.9.4. Оператор и Субъекты Системы осуществляют сбор, документирование и статистическую обработку первичной информации о функционировании Системы.

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

В состав первичной информации о функционировании Системы должно входить следующее:

- информация о времени приема к исполнению, исполнения распоряжений Участников Системы об осуществлении Переводов;
- информация о количестве и суммах указанных распоряжений;
- информация о размерах клиринговых позиций и остатках денежных средств на банковских счетах Участников Системы, открытых в расчетном центре;
- иная информация о функционировании Системы, предусмотренная настоящими Правилами.

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

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

8.10. Контроль за соблюдением Операторами услуг платежной инфраструктуры и Участниками Платежной системы порядка обеспечения БФПС.

8.10.1. Оператор в рамках осуществления контроля за соблюдением настоящих Правил проверяет соблюдение Операторами услуг платежной инфраструктуры и Участниками Платежной системы порядка обеспечения БФПС с учетом следующих требований.

Оператор определяет следующий порядок проведения контроля за соблюдением Операторами услуг платежной инфраструктуры и Участниками Платежной системы порядка обеспечения БФПС.

Оператор контролирует соответствие документов Операторов услуг платежной инфраструктуры порядку обеспечения БФПС и при выявлении несоответствия документов Операторов услуг платежной инфраструктуры порядку обеспечения БФПС направляет рекомендации Операторам услуг платежной инфраструктуры по устранению выявленных несоответствий.

Оператор при выявлении нарушения порядка обеспечения БФПС Операторами услуг платежной инфраструктуры и Участниками Платежной системы:

- информирует Операторов услуг платежной инфраструктуры и Участников Платежной системы о выявленных в их деятельности нарушениях и устанавливает сроки устранения нарушений;
- осуществляет проверку результатов устранения нарушений и информирует Операторов услуг платежной инфраструктуры и Участников Платежной системы, в деятельности которых выявлены нарушения, о результатах проведенной проверки.

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

8.11. Порядок изменения операционных и технологических средств и процедур.

8.11.1. Оператор платежной системы 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.

8.11.2. В случае если изменение операционных и технологических средств и процедур Оператором платежной системы требует внесения изменений в настоящие Правила, Оператор платежной системы вносит соответствующие изменения в порядке, предусмотренном настоящими Правилами. В случае если изменение операционных и технологических средств и процедур Оператором платежной системы не требует внесения изменений в настоящие Правила, Оператор платежной системы направляет Участникам платежной системы уведомление об изменении операционных и технологических средств и процедур с описанием таких изменений не позднее, чем за 30 (тридцать) календарных дней до даты вступления в силу соответствующих изменений.

8.11.3. Участник платежной системы, Оператор платежной инфраструктуры вправе самостоятельно вносить изменения в операционные и технологические средства и процедуры по взаимодействию с Платежной системой на стороне Участника платежной системы, Оператора платежной инфраструктуры, в случае, если внесение таких изменений не противоречит настоящим Правилам, законодательству Российской Федерации и не приводит к изменению порядка оказания услуг по переводам денежных средств, предусмотренного настоящими Правилами, а также к объему и характеру их оказания Участником платежной системы, Оператором платежной инфраструктуры.

8.12. Мероприятия по восстановлению штатного функционирования ОИИ

8.12.1. ОПДС, должен руководствоваться следующим планом действий по восстановлению штатного функционирования ОИИ, в случае реализации инцидентов защиты информации.

№	Инцидент	Действия	Сроки исполнения
1	Проблемы с предоставлением услуг связи ISP	Необходимо иметь резервный канал связи. При наступлении инцидента необходимо перейти на резервный канал.	1-2 часа
2	Выход из строя сетевого оборудования	Необходимо обеспечить наличие резервного сетевого оборудования, задействованного на участке ПС. Поддерживать в актуальном виде копию конфигурации сетевого оборудования. При наступлении инцидента необходимо заменить вышедшее из строя оборудование и загрузить актуальную версию конфигурации на оборудование.	1-2 часа
3	Выход из строя автоматизированного рабочего места	Необходимо обеспечить наличие резервного автоматизированного рабочего места, задействованного на участке ПС. Поддерживать в актуальном виде копию конфигурации оборудования. При наступлении инцидента необходимо заменить вышедшее из строя оборудование и произвести повторное подключение к ПС	1-2 часа
3	Выход из строя СКЗИ	Необходимо осуществить полное удаление СКЗИ с АРМ, перезагрузить АРМ и произвести повторную установку СКЗИ.	1-2 часа

9. Порядок оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией.

9.1. Оператор платежной системы проводит оценку качества функционирования операционных и технологических средств и информационных систем Платежной системы путем привлечения независимой организации.

9.2. Оператор платежной системы самостоятельно осуществляет выбор привлекаемой независимой организации.

9.3. В результате проведения оценки качества функционирования операционных и технологических средств и информационных систем Платежной системы независимой организацией Оператор платежной системы вправе принимать решение об изменении операционных и технологических средств и процедур Платежной системы в порядке, предусмотренном настоящими Правилами.

9.4. Участники платежной системы и Операторы услуг платежной инфраструктуры вправе по своему усмотрению и за свой счет проводить оценку качества функционирования операционных и технологических средств и информационных систем на стороне Участников платежной системы и Операторов услуг платежной инфраструктуры с привлечением независимых организаций. При этом привлекающая сторона обязуется подписать соглашение о неразглашении конфиденциальной информации с привлекаемой независимой организацией.

10. Временной регламент функционирования Платежной системы «ХЕЛЛО».

10.1. Операционный день.

10.1.1. В Платежной системе устанавливается операционный день с 00:00:00 МСК до 23:59:59 МСК календарного дня.

10.1.2. В Платежной системе, учитывая временной регламент функционирования Платежной системы, допускается отклонение в пределах тридцати минут от времени окончания операционного дня, время начала следующего операционного дня сдвигается на величину отклонения времени закрытия предыдущего операционного дня в соответствующую сторону. Отклонение времени начала (окончания) операционного дня в пределах установленного значения является нормальным, не требует специального уведомления Участников платежной системы.

10.2. Временной регламент функционирования Платежной системы «ХЕЛЛО».

10.2.1. В качестве единой шкалы времени при расчетах в Платежной системе признается московскоевремя. Контрольным является время системных часов аппаратных средств Оператора платежной системы. Время проведения расчетов представлено в Таблице №1, регламенты обработки распоряжений и проведения расчетов представлены в Таблице №2.

Таблица 1. Время приема к исполнению распоряжений Плательщиков и Участников платежной системы.

Событие	Время по Московскому времени
Прием распоряжений Плательщиков	Круглосуточно
Прием распоряжений Участников	Круглосуточно

Таблица 2. Регламент обработки распоряжений и проведения расчетов Плательщиков и Участников платежной системы.

Событие	Исполняющий ОУПИ	Получающий ОУПИ	Время по Московскому времени
Завершение приема распоряжений к обработке текущимотчетным периодом (закрытие отчетного периода)	Операционный центр		23:59:59
Составление Реестров переводов (платежей) и отчетов за закрытый отчетный период и передача их Операционным центром в Платежный клиринговый центр	Операционный центр	Платежный клиринговый центр	С 00:00 до 10:30
Расчет платежных клиринговых позиций Платежным клиринговым центром и направление, посредством Операционного центра, подтверждений Участникам приема к исполнению (отказа в приеме) распоряжений	Платежный клиринговый центр	Расчетный центр/Участники	С момента получения Реестров переводов (платежей) до 12:00
Осуществление расчетов по счетам Участников Расчетным центром	Расчетный центр		С момента получения распоряжений до 14:30 дня получения распоряжений
Подтверждение исполнения распоряжений	Расчетный центр	Платежный клиринговый центр	С момента окончания расчетов до 15:00
			С 15:00 до 15:30
	Платежный клиринговый центр	Участники	С 15:30 до 16:30

Расчеты проводятся ежедневно, по рабочим дням.

Днем расчетов считается следующий рабочий день за днем:

- выдачи перевода при отправке для выплаты наличными денежными средствами Получателю;
- отправки перевода для зачисления на счет Получателя/оплаты услуг.

Правила определения дня расчетов в зависимости от дня выплаты наличными денежными средствами/отправки на счет Получателю перевода представлены в Таблице №3.

Таблица 3. Определение дня расчетов.

День выплаты наличными денежными средствами Получателю/отправки на счет Получателя	День передачи распоряжения в Платежный клиринговый центр и его обработки Платежным клиринговым центром	День исполнения распоряжения Расчетным центром
Понедельник	Вторник	Вторник
Вторник	Среда	Среда

Среда	Четверг	Четверг
Четверг	Пятница	Пятница
Пятница	Понедельник	Понедельник
Суббота	Понедельник	Понедельник
Воскресенье	Понедельник	Понедельник

10.2.2. В случае разового изменения времени смены операционного дня Оператор платежной системы доводит данную информацию до Участников платежной системы.

10.2.3. О проведении плановых технических, профилактических и ремонтных работ Оператор платежной системы уведомляет Участников платежной системы заблаговременно, не позднее, чем за пять рабочих дней до даты начала проведения работ, путем направления Участникам соответствующих уведомлений посредством программно-аппаратного комплекса Системы Оператора системы. В уведомлении указываются дата и время начала проведения работ, предполагаемые дата и время окончания проведения работ.

10.2.4. О проведении внеплановых ремонтных работ, а также работ, вызванных необходимостью устранения чрезвычайных обстоятельств, повлиявших на работоспособность Платежной системы, Оператор платежной системы уведомляет Участников платежной системы не позднее одного рабочего дня с даты начала проведения работ, путем направления Участникам соответствующих уведомлений посредством программно-аппаратного комплекса Системы.

В уведомлении указываются предполагаемые дата и время окончания проведения работ.

10.2.5. Внесение изменений во временной регламент функционирования Платежной системы осуществляется в общем порядке, предусмотренном для внесения изменений в Правила.

11. Порядок обмена информацией, необходимой для управления рисками.

11.1. В целях управления рисками Оператор платежной системы вправе запрашивать и получать от Участников платежной системы и Операторов услуг платежной инфраструктуры информацию, необходимую для управления рисками Платежной системы, а также систематизировать, обрабатывать, накапливать и хранить такую информацию.

11.2. В случае если запрашиваемая информация содержит сведения, составляющие коммерческую тайну, Оператор платежной системы обязуется обеспечить сохранение такой информации в соответствии с требованиями законодательства Российской Федерации. Оператор платежной системы вправе предоставлять такую информацию третьим лицам в случаях, предусмотренных требованиями законодательства Российской Федерации.

11.3. Участники платежной системы и Операторы услуг платежной инфраструктуры не вправе необоснованно отказать Оператору платежной системы в предоставлении информации, требуемой в целях управления рисками в Платежной системе, если предоставление такой информации не противоречит требованиям законодательства РФ.

11.4. Оператор платежной системы обязуется предоставлять Участникам, Операторам услуг платежной инфраструктуры информацию, требуемую в целях управления рисками в Платежной системе как по собственной инициативе, так и по запросу последних.

12. Обеспечение защиты информации в Платежной системе «ХЕЛЛО».

12.1. Общие положения о защите информации в Платежной системе «ХЕЛЛО».

12.1.1. Правила устанавливают общие требования к защите информации, обрабатываемой Субъектами платежной системы, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, а также защите в соответствии с Правилами.

12.1.2. Защита информации осуществляется в соответствии с требованиями, установленными Правилами, а также требованиями, предусмотренными нормативными актами и законодательством Российской Федерации, в том числе с учетом специфики деятельности Субъекта платежной системы.

12.1.3. Защита информации обеспечивается путем реализации Субъектами платежной 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.

12.1.4. Субъекты платежной системы утверждают внутренние документы, устанавливающие порядок реализации требований к защите информации.

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

12.1.6. Оператор платежной системы, Участники платежной системы, Операторы услуг платежной инфраструктуры обязаны пересматривать действующий порядок обеспечения защиты информации при осуществлении переводов денежных средств в связи с изменениями требований к защите информации, определенных законодательными актами Российской Федерации, нормативными актами Правительства Российской Федерации и Банка России, Правилами, изменениями установленных в Правилах требований к защите информации, выявлением недостатков при осуществлении контроля выполнения порядка обеспечения защиты информации, в сроки, указанные в нормативных документах.

13. Защищаемая в Платежной системе «ХЕЛЛО» информация.

13.1. Требования к обеспечению защиты информации, установленные настоящими Правилами, при осуществлении переводов денежных средств применяются для обеспечения защиты следующей информации (далее - защищаемая информация):

- информации о совершенных переводах денежных средств, в том числе информации, содержащейся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений Участников платежной системы, а также в извещениях (подтверждениях), касающихся исполнения распоряжений Участников платежной системы;
- информации об остатках денежных средств на банковских счетах;
- информации, содержащейся в оформленных в рамках применяемой формы безналичных расчетов распоряжениях клиентов операторов по переводу денежных средств, распоряжениях Участников платежной системы, распоряжениях платежного клирингового центра;

- информации, хранящейся в операционных центрах платежной системы, о совершенных переводах денежных средств с использованием платежных карт;
- информации о платежных клиринговых позициях;
- информации, необходимой для удостоверения клиентами права распоряжения денежными средствами;
- информации о конфигурации, определяющей параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается оператором по переводу денежных средств, оператором услуг платежной инфраструктуры, и используемых для осуществления переводов денежных средств, а также информации о конфигурации, определяющей параметры работы технических средств по защите информации;
- ключевой информации средств криптографической защиты информации, используемых при осуществлении переводов денежных средств;
- информации ограниченного доступа, в том числе персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемой при осуществлении переводов денежных средств.

14. Требования к обеспечению защиты информации.

14.1. Оператор Платежной Системы предъявляет Участникам, а также операторам УПИ требования обеспечивать защиту информации при осуществлении переводов денежных средств, в т.ч. в соответствии с требованиями, установленными Банком России (Положение Банка России от 04 июня 2020 года № 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 № 719-П) и Правительством РФ (Постановление Правительства РФ от 13 июня 2012 года № 584 об утверждении «Положения о защите информации в платежной системе»), а также обеспечивать конфиденциальность информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством РФ.

14.2. Оператор Системы устанавливает распределение обязанностей по определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках Платежной Системы следующим образом:

- Оператор Платежной Системы самостоятельно определяет порядок обеспечения защиты информации для осуществления переводов денежных средств при выполнении им функций Операционного и Клирингового центров Системы, а также реализовывает его;
- Участник Платежной Системы самостоятельно определяет порядок обеспечения защиты информации для осуществления переводов денежных средств в рамках Платежной Системы в части обслуживания клиентов – физических и юридических лиц, в т.ч. банков – корреспондентов, а также реализовывает его;
- Привлеченный Оператором Платежной Системы Расчетный центр самостоятельно определяет порядок обеспечения защиты информации для осуществления переводов денежных средств при выполнении им функций Расчетного центра Платежной Системы, а также реализовывает его.

14.3. Оператор Правилами Системы определяет требования к обеспечению защиты информации при осуществлении переводов в системе и может вносить в них изменения в случаях:

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

14.3.1. Требования к обеспечению защиты информации при осуществлении переводов применяются для защиты информации, указанной в п.13.1. Правил, а также информации ограниченного доступа, определенной во внутренних документах Оператора, Расчетного центра и Участников, обрабатываемой при взаимодействии Субъектов в системе.

14.4. Общие требования к защите информации предусматривают:

- создание и организацию функционирования структурного подразделения по защите информации или назначение должностного лица (работника), ответственного за организацию защиты информации;
- включение в должностные обязанности работников, участвующих в обработке информации, обязанности по выполнению требований к защите информации;
- повышение осведомленности работников в области обеспечения защиты информации;
- осуществление мероприятий, имеющих целью определение угроз безопасности информации и анализ уязвимости информационных систем;
- проведение анализа рисков нарушения требований к защите информации и управление соответствующими рисками;
- разработка и реализация систем защиты информации в информационных системах;
- применение средств защиты информации (шифровальные (криптографические) средства, средства защиты информации от несанкционированного доступа, средства антивирусной защиты, средства межсетевого экранирования, системы обнаружения вторжений, средства контроля (анализа) защищенности);
- выявление инцидентов, связанных с нарушением требований к защите информации, реагирование на них;
- обеспечение защиты информации при использовании информационно-телекоммуникационных сетей общего пользования;
- определение порядка доступа к объектам инфраструктуры Платежной Системы, обрабатывающим информацию;
- организация и проведение контроля и оценки выполнения требований к защите информации на собственных объектах информационной инфраструктуры не реже 1 раза в 2 года.

14.5. В целях защиты автоматизированных рабочих мест Участника (далее – АРМ) от вредоносных компьютерных программ, влекущих нарушение работы в рамках Платежной Системы, Участник обязуется выполнять следующие основные требования по обеспечению информационной безопасности:

- соблюдать конфиденциальность в отношении логинов, паролей, сертификатов доступа, секретных ключей, не разглашать их третьим лицам, а также обязуется ограничить свободный доступ к ним со стороны любых третьих лиц;
- ограничить свободный доступ со стороны любых третьих лиц к АРМ, с которых осуществляется взаимодействие с Системой для исключения их несанкционированного использования;
- установить на АРМ лицензированное антивирусное программное обеспечение, своевременно его обновлять, а также обеспечить его непрерывное использование;
- установить на АРМ лицензированное средство разграничение доступа к аппаратным ресурсам;
- не переходить по ссылкам и не устанавливать приложения/обновления антивирусного программного обеспечения, пришедшие посредством SMS/электронной почты, в том числе от имени Оператора Платежной Системы;
- не использовать общественные (установленные для публичного использования неопределенным кругом лиц) АРМ для работы с Системой;
- загружать и устанавливать на АРМ прикладное программное обеспечение только из официальных источников в сети «Интернет» согласно инструкциям производителей;
- своевременно устанавливать обновления (в том числе обновления безопасности) операционной системы и прикладного программного обеспечения АРМ.

14.6. Требования к обеспечению защиты информации в Системе определяются в отношении следующих мероприятий, которые обязаны выполнять Участники – операторы по переводу денежных средств и привлеченные Расчетные центры:

- управление риском информационной безопасности в качестве субъекта Системы как одним из видов операционного риска, источниками реализации данного риска 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, привлеченными Расчетными центрами;
- установление состава показателей уровня риска информационной безопасности в Платежной Системе (Оператор Системы рекомендует устанавливать минимум два показателя: количество инцидентов нарушения информационной безопасности и размер убытков от инцидентов риска информационной безопасности);
- реализация процессов выявления и идентификации риска информационной безопасности в Платежной Системе в отношении своих объектов информационной инфраструктуры, задействованных при функционировании в Платежной Системе;
- выявление и анализ риска информационной безопасности в Платежной Системе. Включает в себя определение источников риска и событий, реализация которых может привести к возникновению инцидента (риск-события), и определение для каждого из выявленных риск-событий величины риска, характеризуемого вероятностью наступления риск-событий и величиной возможных последствий их реализации; анализ возможностей на проникновение, при тестировании каждой области оценивается процесс реагирования на инциденты информационной безопасности и возможности по восстановлению работоспособности, в случае возможной компрометации безопасности ИТ систем; использование специализированного программного обеспечения для выявления уязвимостей программного и аппаратного обеспечения; непрерывный мониторинг событий ИБ;
- реализация процессов реагирования на инциденты информационной безопасности и восстановления штатного функционирования объектов информационной инфраструктуры в случае реализации инцидентов защиты информации;
- реализация взаимодействия при обмене информацией об инцидентах информационной безопасности;
- при привлечении банковских платежных агентов (субагентов), на основе системы управления рисками определять для них критерии необходимости и периодичности тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры, проведения оценки соответствия защиты информации, сертификации или оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений;
- реализация мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента, определенных пунктами 2.2 и 2.4 Указания Банка России от 8 октября 2018 года № 4926-У "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»;
- проведение работ по разработке, сертификации и (или) оценке соответствия в отношении прикладного программного обеспечения автоматизированных систем и приложений, в том числе платежных приложений, предоставляемых поставщиками платежных приложений клиентам операторов по переводу денежных средств, являющихся Участниками Платежной Системы, осуществляется с учетом требований Положения № 719-П.

14.7. Оператор Платежной Системы берет на себя обязательства обеспечивать защиту информации при осуществлении переводов денежных средств, в т.ч. в соответствии с требованиями, установленными Банком России, а также обеспечивать конфиденциальность информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством РФ и нормативными актами Банка России.

14.8. Оператор устанавливает следующие показатели уровня риска ИБ:

	Количество инцидентов информационной безопасности в Системе	Размер убытков от инцидентов информационной безопасности, понесенных Оператором Системы	Ограничения по параметрам операций по осуществлению переводов денежных средств в случае выявления факта превышения значений показателей уровня риска информационной безопасности
Участники – операторы по переводу денежных средств	Не более 3-х в квартал	Не более 50 млн. в квартал.	Могут быть введены Оператором Системы ограничения на сумму единичной операции по переводу денежных средств.
Привлеченный Расчетный центр	Не более 3-х в квартал	Не более 50 млн. в квартал.	Могут быть введены Оператором Системы ограничения на временной период совершения операций.
Операционный центр	Не более 3-х в квартал	Не более 50 млн. в квартал.	Могут быть введены Оператором Системы ограничения на временной период совершения операций.
Платежно-клиринговый центр	Не более 3-х в квартал	Не более 50 млн. в квартал.	Могут быть введены Оператором Системы ограничения на временной период совершения операций.

14.9. Ограничения могут быть сняты:

- при условии отсутствия инцидентов в последующие два квартала;
- при условии предоставления документов и информации об устранении причин возникновения инцидентов;
- при условии возмещения убытка Оператора Системы со стороны Участника – оператора по переводу денежных средств, привлеченного Расчетного центра.

14.10. Порядок обеспечения защиты информации в Платежной системе «ХЕЛЛО».

14.10.1. В целях обеспечения защиты информации в Платежной системе при хранении, обработке, обмене защищаемой информации Субъекты Платежной Системы самостоятельно обеспечивают осуществление, включая, но, не ограничиваясь, следующих мер:

- соблюдение организационных мер защиты информации;
- поддержка программы управления уязвимостями;
- создание и поддержание безопасной сетевой инфраструктуры;
- мониторинг сетевой инфраструктуры;
- внедрение и поддержание мер по управлению доступом к защищаемой информации;
- иные меры, направленные на повышение защиты информации.

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

14.10.3. Использование установленных производителем программного обеспечения паролей иных параметров безопасности, устанавливаемых по умолчанию - не допускается.

14.10.4. В рамках реализации мер по поддержке программы управления уязвимостями Субъекты Платежной Системы обязаны выполнять установленные Правилами требования к обеспечению защиты информации от воздействия вредоносных кодов, обеспечить использование на всех компонентах системы, задействованных в хранении, обработке и обмене защищаемой информацией только актуальных версий программных обеспечений, разработанных для целей противодействия внешнему или внутреннему использованию уязвимостей.

14.10.5. В рамках реализации мер по внедрению и поддержание мер по управлению доступомк защищаемой информации Субъекты платежной системы обеспечивают ограничение доступа и учет лиц, имеющих доступ к защищаемой информации, в том числе:

- обеспечивают доступ к защищаемой информации только тем лицам, которым такой доступ необходим для выполнения возложенных на них функций;
- обеспечивают многокомпонентность и многоразрядность (не менее восьми символов) используемых паролей, а также периодическую смену паролей;
- обеспечивают предоставление доступа каждому сотруднику с использованием уникального имени, учетной записи, пароля и/или ключа проверки ЭП для доступа к защищаемой информации;
- обеспечивают ограничение доступа к материальным носителям, содержащим защищаемую информацию, строгий контроль за их хранением;
- обеспечивают немедленный отзыв доступа при прекращении полномочий лица на доступ к защищаемой информации.

14.10.6. В рамках реализации мер по мониторингу сетевой инфраструктуры субъекты платежной системы должны контролировать доступ к сетевым ресурсам и защищаемой информации, для чего организуют мониторинг событий, касающихся доступа к сетевым ресурсам, регистрируют действия пользователей, необходимых для проведения расследования и анализа причин инцидентов, обеспечивают хранение журналов событий не менее одного года, а в оперативном доступе не менее трех месяцев, обеспечивают плановую и внеплановую (при внесении изменений) проверку систем, процессов и программного обеспечения для поддержания их защищенности на должном уровне.

14.10.7. Субъекты платежной системы обеспечивают защиту информации при осуществлении переводов денежных средств с учетом распределения функциональных прав и обязанностей лиц, связанных с осуществлением переводов денежных средств в платежной системе.

14.10.8. Субъекты платежной системы с целью выполнения требований по защите информации определяют подразделение (сотрудника), ответственное за организацию и контроль обеспечения защиты информации, задачей которого, в том числе, является повышение осведомленности работников в области обеспечения защиты информации.

В части, не установленной в Правилах, Субъекты Платежной Системы, руководствуясь законодательством Российской Федерации, самостоятельно определяют порядок обеспечения защиты информации при выполнении своих функций в платежной 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.

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

14.10.10. Несоблюдение требований по защите информации, полученной Субъектом в связи свыполнением возложенных на него функций в соответствии с Правилами, приведшее к незаконному разглашению/компрометации указанной информации является существенным нарушением Правил и основанием для принятия Оператором платежной системы мер воздействия, предусмотренных Правилами, вплоть до решения о расторжении в одностороннем порядке договора участия с указанным Субъектом платежной системы и прекращением его функций.

14.11. Оператор Платежной Системы контролирует обеспечения информационной безопасности Участниками Платежной Системы и Операторами УПИ путем направления не реже одного раза в год Участникам Платежной Системы и Операторам УПИ Анкеты по форме Приложения №8. Оператор Платежной Системы на основании заполненных Анкет вправе запрашивать дополнительную информацию, касающуюся обеспечения информационной безопасности Субъектами Платежной Системы.

14.12. Противодействие осуществлению переводов денежных средств без согласия клиента.

14.12.1. Оператор платежной системы при реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента:

- создает систему выявления и мониторинга переводов денежных средств без согласия клиента в Системе;
- определяет порядок реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента для Участников Системы;
- использует выявленную информацию о технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры оператора по переводу денежных средств и (или) его клиентов, применительно к своей инфраструктуре в целях противодействия осуществлению переводов денежных средств без согласия клиента.

14.12.2. Система выявления и мониторинга переводов денежных средств без согласия клиента основывается на информации о переводах без согласия клиента, предоставляемой Банком России. Информация, предоставляемая Банком России, в т.ч. устанавливаемые Банком России признаки осуществления перевода без согласия клиента, интегрируется в Программный комплекс ХЕЛЛО (ПК ХЕЛЛО).

14.12.3. Процедуры выявления и мониторинга переводов денежных средств без согласия клиента совмещены с процедурами клиринга.

14.12.4. Оператор по переводу денежных средств, участник Платежной Системы, при реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента должен:

- выявлять операции по переводу денежных средств, соответствующие признакам осуществления перевода денежных средств без согласия клиента;
- выявлять операции по переводу денежных средств, совершенные в результате несанкционированного доступа к объектам информационной инфраструктуры оператора по переводу денежных средств;
- выявлять компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия клиента;
- осуществлять сбор технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, при их наличии;
- осуществлять сбор сведений об обращении плательщика в правоохранительные органы при их наличии;

- рассматривать случаи и (или) попытки осуществления переводов денежных средств без согласия клиента, вызванные компьютерными атаками, направленные на объекты информационной инфраструктуры участников информационного обмена;
- реализовывать меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия клиента;
- определять в документах, регламентирующих процедуры управления рисками, процедуры выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, на основе анализа характера, параметров и объема совершаемых клиентами оператора по переводу денежных средств операций (осуществляемой клиентами деятельности) в соответствии с частью 5.1 статьи 8 Федерального закона N 161-ФЗ;
- реализовывать в отношении клиента - получателя средств, в адрес которого ранее совершались операции по переводу денежных средств без согласия клиента, в случаях, предусмотренных договором банковского счета, ограничения по параметрам операций по осуществлению переводов денежных средств (переводов электронных денежных средств) с использованием платежных карт, а также ограничения на получение наличных денежных средств в банкоматах за одну операцию и (или) за определенный период времени;
- использовать выявленную оператором по переводу денежных средств информацию о технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры оператора по переводу денежных средств и (или) его клиентов, применительно к своей инфраструктуре в целях противодействия осуществлению переводов денежных средств без согласия клиента.

14.12.5. Оператор услуг платежной инфраструктуры при реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента должен:

- реализовывать меры по противодействию осуществлению переводов денежных средств без согласия клиента (Участника Платежной Системы) в соответствии с порядком, установленным Оператором Платежной Системы;
- выявлять компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия клиента;
- рассматривать случаи и (или) попытки осуществления переводов денежных средств без согласия клиента, вызванные компьютерными атаками, направленными на объекты информационной инфраструктуры участников информационного обмена;
- реализовывать меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия клиента;
- использовать информацию о переводах без согласия клиента (Участника Платежной Системы) для выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента (Участника Платежной Системы);
- осуществлять анализ операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента (Участника Платежной Системы), в рамках платежной системы.

14.12.6. При совершении операций, предполагающих автоматическое и моментальное исполнение распоряжений, и при одновременном наличии признаков осуществления перевода без согласия клиента, распоряжение к исполнению не принимается.

14.12.7. Порядок реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента для Участников Системы:

- При выявлении операций, имеющих признаки осуществления перевода денежных средств без согласия клиента, программным способом (посредством ПК ХЕЛЛО) выдается предупреждение о наличии таких признаков.

- Участник при получении предупреждения обязан до осуществления операции связаться с клиентом любым доступным способом в зависимости от способа обслуживания клиента, в т.ч. посредством устного обращения операционного состава к клиенту, выведения информации на экран средства ДБО, направления мгновенных текстовых и видео сообщений с использованием мобильных телефонов, персональных компьютеров (например, СМС-сообщения, мессенджеры), предоставления информации на бумажном носителе) для осуществления следующих действий:
  - ✓ проинформировать клиента о факте получения предупреждения:
  - ✓ запросить и получить от клиента согласие либо отказ в дальнейшем проведении операции,
  - ✓ дать рекомендации о мерах по безопасному осуществлению переводов денежных средств. Меры безопасного осуществления перевода публикуются на сайте Платежной Системы – www.hellopay.online
- В зависимости от имеющейся информации Участник имеет возможность приостановить осуществление операции, отказаться от осуществления операции либо подтвердить осуществление операции.
- В случае приостановления осуществления операции Участник самостоятельно соблюдает срок приостановления, который не может превышать два рабочих дня, следующих за днем выявления/приостановления операции.
- При подтверждении Участником совершения операции, имеющей признаки осуществления перевода денежных средств без согласия клиента, в т.ч. операции, осуществление которой было приостановлено ранее Участником самостоятельно, исполнение распоряжения приостанавливается Оператором Системы на два рабочих дня, следующих за днем выявления/приостановления операции. Переводу присваивается соответствующий статус.
- Участник в случае получения согласия клиента на совершение операции, а также в случае если операция была ранее приостановлена Участником самостоятельно на два рабочих дня, следующих за днем выявления/приостановления операции, обязан незамедлительно направить по адресу: info@hellopay.online информацию о необходимости возобновления исполнения приостановленного распоряжения. Оператор Системы при получении подтверждения операции незамедлительно возобновляет исполнение распоряжения.
- В случае, если Участник не направляет Оператору Системы подтверждение операции, исполнение распоряжения возобновляется Оператором Системы автоматически по истечению двух рабочих дней, следующих за днем выявления/приостановления операции (подтверждение операции).
- В случае, если Участник ошибочно направил подтверждение операции при получении отказа клиента на совершение операции, Участник обязан сообщить по адресу: info@hellopay.online информацию о необходимости аннулирования приостановленного распоряжения не позднее следующего за днем выявления/приостановления операции рабочего дня.

14.12.8. Операторы УПИ при реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента должны:

- самостоятельно в полном объеме реализовывать меры по противодействию осуществлению переводов денежных средств без согласия Участника, в т.ч. меры информационного взаимодействия с Участниками и Банком России, в соответствии с порядком, установленным законодательством РФ и Банком России;
- выявлять компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия клиента;
- рассматривать случаи и (или) попытки осуществления переводов денежных средств без согласия клиента, вызванные компьютерными атаками, направленными на объекты информационной инфраструктуры участников информационного обмена;
- реализовывать меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия клиента;

- использовать информацию о переводах без согласия клиента (участника платежной системы) для выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия Участника;
- осуществлять анализ операций, соответствующих признакам осуществления переводов денежных средств без согласия Участника, в рамках Системы.

14.13. Порядок, формы и сроки информирования Оператора Системы, Участников Системы и операторов УПИ о выявленных в Системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, порядок взаимодействия в случае выявления в Системе вышеуказанных инцидентов.

14.13.1. К инцидентам в сфере защиты информации относятся события, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, которые привели или могут привести к осуществлению переводов денежных средств без согласия клиента, неоказанию услуг по переводу денежных средств, в том числе включенные в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и размещаемый Банком России на официальном сайте Банка России в сети Интернет.

14.13.2. Оператор Системы устанавливает следующие требования к содержанию, форме и периодичности представления информации, направляемой Участниками и привлеченным Расчетным центром для целей анализа обеспечения в Системе защиты информации при осуществлении переводов денежных средств, а также в целях взаимодействия в случае выявления инцидентов в сфере защиты информации:

Содержание	**Форма**	**Периодичность**
1) о выполнении требований к обеспечению защиты информации, в т.ч. о результатах проведенных оценок соответствия	официальное письмо и/или опрос в электронной форме, проводимый Оператором Системы	по запросу Оператора Системы 1 раз в два года
2) о реализации порядка обеспечения защиты информации		
3) о выявленных угрозах и уязвимостях в обеспечении защиты информации		при выявлении
4) о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации	в оперативном режиме в части: несанкционированного доступа, операциях без согласия клиента – сообщение по электронной почте info@hellopay.online, звонок +7 (495) 968-0-986; компрометации ключей - действия в соответствии с Инструкцией по работе с ключевой информацией, сообщение по электронной почте: info@hellopay.online;	при выявлении
	в части вредоносного кода при наличии опасности распространения его последствий по Системе в целом - сообщение по электронной почте, сообщение по электронной почте info@hellopay.online, звонок +7 (495) 968-0-986; в части невозможности осуществления переводов денежных средств в течение 3-х часов и более по любым причинам – сообщение по электронной почте info@hellopay.online, звонок +7 (495) 968-0-986.	при выявлении
5) о применяемых СКЗИ	Официальное письмо	Не позднее 10 (десяти) рабочих дней с момента начала применения СКЗИ или изменения СКЗИ, либо по запросу Оператора.

14.13.3. Оператор Системы определяет следующие требования к взаимодействию в случае выявления инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках Системы:

Инциденты:	**Действия Участника, привлеченного Расчетного центра**	**Действия Оператора Системы**
1. При выявлении инцидентов.	Обеспечение: - информирования собственных служб информационной безопасности о выявлении инцидентов; - регистрации выявленных инцидентов; - применения организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для выявления инцидентов; - реагирования на выявленные инциденты, в т.ч. обращение в правоохранительные органы при выявлении осуществления перевода денежных средств по распоряжению лиц, не обладающих правом распоряжения этими денежными средствами; - анализа причин выявленных инцидентов, проведения оценки результатов реагирования на инциденты; - информирования Оператора Системы в оперативном порядке о выявленных инцидентах, в виде ежемесячного отчета; - реализация восстановления штатного функционирования объектов информационной инфраструктуры.	Предпринимает возможные и доступные в сложившихся обстоятельствах действия по: - минимизации последствий выявленных инцидентов; - пресечению возможности использования денежных средств Получателями при выявлении осуществления перевода денежных средств по распоряжению лиц, не обладающих правом распоряжения этими денежными средствами (*при необходимости Оператор Системы связывается по указанным контактам с Участниками, привлеченным Расчетным центром; принимает решение о необходимости блокировки Участников в Системе, аннулировании, блокировании переводов, приостановлении расчетов с привлеченным Расчетным центром, иные решения);* - проверке соблюдения требований к защите информации на стороне Оператора Системы и соблюдению требований при обработке переводов; - информированию Участника, Расчетного центра о результатах предпринятых действий. Полученную информацию Оператор Системы анализирует на предмет обеспечения в Системе защиты информации, формулирует при необходимости рекомендации по совершенствованию защиты информации, а также на основании анализа вносит изменения в требования по защите информации.
2. При выявлении факта компрометации ключевой информации средств криптографической защиты информации, используемых при осуществлении переводов денежных средств.	Действуют в соответствии с Инструкцией по работе с ключевой информацией Обеспечивают оперативное информирование Оператора Системы по адресу: info@hellopay.online и по телефону +7 (495) 968-0-986.	Блокирует для Участника возможность осуществления переводов в Системе.
3.При обнаружении вредоносного кода или факта воздействия вредоносного кода.	Обеспечивают принятие мер, направленных на предотвращение распространения вредоносного кода и устранение последствий воздействия. При необходимости приостанавливают осуществление переводов денежных средств на период устранения последствий заражения вредоносным кодом, а также последствий иных воздействий. Обеспечивают оперативное информирование Оператора Системы по адресу: info@hellopay.online и по телефону +7 (495) 968-0-986.	После получения сообщения от Участника, привлеченного Расчетного центра временно приостанавливает работу Участника в Системе. Приостанавливает расчеты с привлеченным Расчетным центром, также временно приостанавливая работу Участника, осуществляющего расчеты через него. В случае наличия проблем в функционировании Системы осуществляет рассылку по согласованным каналам связи. В случае обнаружении вредоносного кода или факта воздействия вредоносного кода в рамках Системы Оператор информирует Участника, привлеченный Расчетный центр по согласованным каналам связи.

14.13.4. Оператор Системы обеспечивает учет и доступность для Участника Системы и привлеченного Расчетного центра информации:

- о выявленных Оператором Системы инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- информация направляется по согласованным каналам связи ежемесячно при наличии инцидентов, отсутствие направленной информации признается отсутствием инцидентов;
- о методиках анализа и реагирования Оператора Системы на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.

  Методика анализа заключается в сборе, обобщении информации, анализе информации о причинах инцидентов на соответствие требованиям Положения № 719-П Правил Платежной Системы «ХЕЛЛО».

14.13.5. Оператор Системы на основе накопления и учета опыта реагирования на инциденты защиты информации и восстановления функционирования Системы после их реализации в целях снижения риска информационной безопасности реализовывает механизмы совершенствования в части обеспечения учета и доступности для операторов по переводу денежных средств, являющихся Участниками, и привлеченных Расчетных центров информации:

- о выявленных в платежной системе инцидентах защиты информации;
- о методиках анализа и реагирования на инциденты защиты информации.

15. Использование средств криптографической защиты информации.

15.1. Правилами, а также договорами, заключаемыми между Субъектами платежной системы, для защиты информации используются средства криптографической защиты информации (шифрования) либо программно-аппаратные средства, содержащие модули криптографической защиты информации.

15.2. В случае, если к выбору используемых средств криптографической защиты информации Правилами не предъявляются специальные требования, выбор осуществляется по соглашению сторон электронного обмена.

15.3. Для проведения работ, связанных с криптографическими средствами защиты информации Субъектами платежной системы, могут привлекаться на договорной основе организации, имеющие лицензии на соответствующие виды деятельности.

16. Требования к обеспечению защиты информации от воздействия вредоносного кода.

16.1. Субъекты платежных систем в целях снижения возможных потерь от воздействия вредоносного кода путем предотвращения проникновения и распространения, а также своевременного уничтожения вредоносного кода, обеспечивают выполнение следующих требований:

- использование технических средств защиты информации, предназначенных для выявления вредоносного кода и для предотвращения воздействия вредоносного кода на объекты информационной инфраструктуры (далее - технические средства защиты информации от воздействия вредоносного кода), на средствах вычислительной техники, включая банкоматы и платежные терминалы, при наличии технической возможности;
- регулярное обновление версий технических средств защиты информации от воздействия вредоносного кода и баз данных, используемых в работе технических средств защиты информации от воздействия вредоносного кода и содержащих описание вредоносных кодов и способы их обезвреживания;
- функционирование технических средств защиты информации от воздействия вредоносного кода в автоматическом режиме, при наличии технической возможности.

16.2. Оператор, Участник и Расчетный центр 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.

16.3. При наличии технической возможности Оператор, Участник и Расчетный центр обеспечивают выполнение:

- предварительной проверки на отсутствие вредоносного кода программного обеспечения, устанавливаемого или изменяемого на средствах вычислительной техники, включая банкоматы и платежные терминалы;
- проверки на отсутствие вредоносного кода средств вычислительной техники, включая банкоматы и платежные терминалы, выполняемой после установки или изменения программного обеспечения.

16.4. В случае обнаружения вредоносного кода или факта воздействия вредоносного кода, обнаруживший вредоносный код субъект системы, обеспечивают принятие мер, направленных на предотвращение распространения вредоносного кода и устранение последствий воздействия вредоносного кода.

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

В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают информирование оператора платежной системы; оператор платежной системы обеспечивает информирование операторов услуг платежной инфраструктуры и участников платежной системы.

16.5. При обнаружении Субъектом платежной системы проникновения вредоносных кодов в средства вычислительной техники, задействованные в информационном обмене в электронном виде между Субъектами платежной системы, он прекращает информационный обмен в электронном виде с другими Субъектами платежной системы, по любому из доступных каналов связи, в том числе посредством телефонной связи, по факсу информирует сторону в информационном обмене и Оператора платежной системы о возникшей ситуации, включая информирование о событиях, по его мнению, вызвавших указанное событие, его причинах и последствиях, после чего принимает меры реагирования, предусмотренные локальными актами на случай возникновения данного вида событий.

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

17. Обеспечение защиты персональных данных в Платежной системе «ХЕЛЛО».

17.1. Субъекты платежной 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.

17.2. Операторы по переводу денежных средств в случае, если указанное ниже предусмотрено законодательством Российской Федерации, информируют и, в случае необходимости, получают согласие лиц на обработку их персональных данных и предоставление их персональных данных Субъектам платежной системы

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

Субъект платежной системы при выявлении в платежной системе инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, принимает меры по снижению негативных последствий, вызванных нарушением требований, информирует Субъекта платежной системы, в функциональной зоне ответственности которого находится область возникновения инцидента, в порядке и сроки, определенные в порядке взаимодействия в рамках Платежной системы в чрезвычайных ситуациях. Субъект платежной системы, допустивший инцидент, реализует комплекс мер, направленных на устранение причин, вызвавших инцидент, и на недопущение его повторного возникновения, и последствий инцидента. Субъект платежной системы при выявлении в платежной системе инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств обязан информировать Оператора платежной системы о выявленных инцидентах согласно п. 25 Правил, а также обязан проинформировать Оператора платежной системы при выявлении в Платежной системе инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств по электронной почте на адрес info@hellopay.online

18.1. Оператор платежной системы информирует Операторов услуг платежной инфраструктуры и Участников платежной системы о выявленных в Платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, а также о рекомендуемых методиках анализа и реагирования на указанные инциденты путем размещения соответствующей информации на официальном сайте Оператора платежной системы в информационно-телекоммуникационной сети «Интернет» по адресу: www.hellopay.online в специальном разделе «Информационная безопасность и инциденты».

18.2. Операторы услуг платежной инфраструктуры, и Участники платежной системы в составе информации о своей деятельности, представляемой в порядке и сроки, определенные пунктом 26 Правил, представляют данные для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств. При этом состав указанных данных должен соответствовать требованиям нормативных актов Банка России (Положение Банка России №719-П), регламентирующих требования к обеспечению защиты информации в Платежной системе при осуществлении переводов денежных средств.

19. Обеспечение банковской и коммерческой тайны в Платежной системе «ХЕЛЛО».

19.1. Субъекты платежной системы гарантируют в своей деятельности соблюдение банковской тайны в отношении информации, ставшей известной Субъекту платежной системы в связи с выполнением возложенных на него функций в соответствии с Правилами.

19.2. Субъекты платежной системы гарантируют в своей деятельности соблюдение коммерческой тайны в отношении информации, ставшей известной Субъекту платежной системы в связи с выполнением возложенных на него функций в соответствии с Правилами.

20. Порядок взаимодействия в рамках Платежной системы «ХЕЛЛО» в чрезвычайных и нестандартных ситуациях.

20.1. В случае выявления в рамках Платежной системы чрезвычайных ситуаций, в том числе, событий, вызвавших системные сбои, Субъекты платежной системы, выявившие указанные обстоятельства, незамедлительно предпринимают все зависящие от них действия, направленные на снижение вредных последствий, незамедлительно информируют Оператора платежной системы и Субъекта платежной системы, в функциональной зоне ответственности которого находится область возникновения чрезвычайной/нестандартной 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/нестандартную ситуацию, операционные сбои, об их причинах и последствиях.

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

20.3. После восстановления нормального функционирования Платежной системы Оператор платежной системы информирует заинтересованных Субъектов платежной системы о предпринятых действиях и достигнутых результатах.

21. Порядок взаимодействия в рамках Платежной системы «ХЕЛЛО» в спорных ситуациях, порядок досудебного разрешения споров между Субъектами платежной системы.

21.1. Спорные ситуации, включая системные сбои, между Оператором платежной системы и Участниками платежной системы, между Оператором платежной системы и Операторами услуг платежной инфраструктуры, между Участником платежной системы и Оператором услуг платежной инфраструктуры разрешаются (урегулируются) в досудебном порядке: в рабочем порядке и/или по итогам работы комиссии по разрешению спорной ситуации (далее - комиссия).

21.2. 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 Правилами и законодательством Российской Федерации.

21.3. В случае возникновения обстоятельств, свидетельствующих, по мнению одного из Субъектов платежной 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.

21.4. Субъекты платежной системы, которым было направлено извещение о спорной ситуации, и, участвующие в разрешении спорной ситуации (далее – участники спора), обязаны не позднее чем в течение следующих пяти рабочих дней проверить наличие указанных в извещении

обстоятельств, и по необходимости принять меры по разрешению спорной ситуации, со своей стороны.

21.5. В тот же срок участники спора извещают доступными способами инициатора о результатах проверки и, при необходимости, о мерах, принятых для разрешения спорной ситуации.

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

22. Порядок разрешения споров между Субъектами платежной системы при участии комиссии.

22.1. В случае, если инициатор не удовлетворен информацией, полученной от участников спора, для рассмотрения спорной ситуации формируется комиссия.

22.2. Если спорная ситуация не была разрешена в порядке, указанном в пункте 21 Правил инициатор должен не позднее чем в течение трех рабочих дней после получения ответа на извещение о спорной ситуации, направить уведомление о спорной ситуации (далее - уведомление) и предложение о создании комиссии по разрешению спорной ситуации ответчику и Оператору платежной системы (если Оператор платежной системы не является инициатором или участником спора).

22.3. 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 в разрешении спорной ситуации.

22.4. Организацию формирования и деятельности комиссии осуществляет Оператор платежной системы. 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 определены за счет участников споров либо распределены между инициатором и участниками споров в определенной в решении комиссии пропорции.

22.5. Оператор платежной системы не позднее чем в течение двух рабочих дней после получения от инициатора уведомления направляет инициатору и участнику споров информацию о предлагаемом месте, дате и времени сбора комиссии, список предлагаемых для участия в работе комиссии представителей Оператора платежной системы с указанием фамилий, имен, отчеств, должностей, их контактной информации (телефон, факс, электронная почта), а также предлагает инициатору и участникам спора не позднее чем в течение трех рабочих дней после получения указанной информации сообщить список предлагаемых для участия в работе комиссии их представителей с указанием фамилий, имен, отчеств, должностей, их контактной информации (телефон, факс, электронная почта).

22.6. После получения информации от инициатора и участников спора, а также в случае неполучения информации в указанный выше срок, Оператор платежной системы не позднее чем на следующий рабочий день формирует комиссию.

22.7. Если стороны не договорятся об ином, в состав комиссии входит по три уполномоченных лица Оператора платежной системы, инициатора и каждого из участников спора, участвующих в разрешении спорной ситуации.

22.8. Устанавливается тридцатидневный срок работы комиссии. В исключительных случаях срок работы комиссии по решению членов комиссии может быть дополнительно продлен не более чем на тридцать дней. В случае необходимости решение о привлечении независимого эксперта

принимает комиссия, при этом сторона, чей представитель выступил с инициативой привлечения независимого эксперта, самостоятельно решает вопрос об оплате экспертных услуг.

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

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

22.11. Все действия, предпринимаемые комиссией для выяснения фактических обстоятельств, а также выводы, сделанные комиссией, заносятся в протокол работы комиссии.

22.12. 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.

22.13. 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.

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

22.15. 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.

22.16. 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 копию акта.

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

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

22.19. 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.

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

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

22.22. 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 участнику спора претензию.

22.23. Претензия должна содержать:

- изложение существа требований инициатора;
- 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;
- при необходимости денежной оценки претензии - ее сумму и расчет;
- 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.

22.24. 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 участника спора в установленном порядке, обеспечивающем подтверждение вручения корреспонденции; одновременно копии направленных участнику споров документов, направляется Оператору платежной системы.

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

23. Порядок разрешения спорных ситуаций в судебном порядке.

23.1. 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.

24. Перечень платежных систем, с которыми осуществляется взаимодействие, и порядок такого взаимодействия.

24.1. Платежная система «ХЕЛЛО» не осуществляет взаимодействие с другими платежными системами.

25. Порядок осуществления контроля за соблюдением Правил Платежной системы «ХЕЛЛО».

25.1. Контроль за соблюдением настоящих Правил Участниками Платежной системы осуществляет Оператор платежной системы на постоянной основе путем мониторинга деятельности Участников платежной системы в процессе оказания услуг в рамках Платежной системы, анализа жалоб и обращений Плательщиков и Получателей платежей.

25.2. Оператор платежной системы вправе для целей осуществления контроля за соблюдением Правил обязать Участников платежной системы (как всех, так и любого в отдельности):

- предоставлять отчет о соблюдении Правил, о спорных и конфликтных ситуациях между Участником платежной системы и Плательщиками, связанных с оказанием услуг, предусмотренных Правилами. Периодичность предоставления указанного отчета не может быть чаще, чем один раз в месяц;
- предоставлять документы и иную информацию относительно деятельности в качестве Участника платежной системы.

25.3. Оператор анализирует документы и информацию, которые касаются деятельности Участников и Расчетного центра, в том числе предоставляемые ими в соответствии с настоящими Правилами;

25.4. Оператор осуществляет действия и применяет меры принуждения в соответствии с пунктом 27 настоящих Правил в случае нарушения Участниками и Расчетным центром обязательств, принятых на себя в соответствии с настоящими Правилами.

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

26.1. Участники платежной системы и Операторы услуг платежной инфраструктуры, являющиеся кредитными организациями – резидентами Российской Федерации, предоставляют отчетность:

- Форма № 0409123 «Расчет собственных средств (капитала) («Базель III»)».
- Форма №0409101 «Оборотная ведомость по счетам бухгалтерского учета кредитной организации», Отчетность предоставляется Оператору платежной системы в электронном виде/на бумажном носителе, надлежаще оформленная, не позднее десятого рабочего дня с даты, установленной законодательством для предоставления данной отчетности.
- Форма №0403203 «Сведения о событиях, связанных с нарушением защиты информации при осуществлении переводов денежных средств» не позднее десятого рабочего дня с даты, установленной законодательством для предоставления данной отчетности.

По запросу Оператора платежной системы предоставляется надлежаще оформленная отчетность по форме №0409102 «Отчет о прибылях и убытках кредитной организации» в электронном виде/на бумажном носителе не позднее десятого рабочего дня с даты, установленной законодательством для предоставления данной отчетности.

В случае публикации отчетности на официальном сайте Участника платежной системы, Оператора услуг платежной инфраструктуры и/или Банка России отчетность не предоставляется.

26.2. Участники платежной системы и Операторы услуг платежной инфраструктуры, являющиеся кредитными организациями – нерезидентами Российской Федерации, предоставляют аналогичную – в п. 26.1. Правил отчетность, применимую к законодательству страны места нахождения (регистрации) кредитной организации, в порядке и сроки, предусмотренные в п. 26.1 Правил.

В случае публикации отчетности на официальном сайте Участника платежной системы и Операторы услуг платежной инфраструктуры и/или национального банка отчетность не предоставляется.

26.3. Дополнительно, по запросу Оператора платежной системы Участники платежной системы и Операторы услуг платежной инфраструктуры обязаны в срок, не превышающий тридцати календарных дней со дня получения указанного запроса, предоставлять Оператору платежной системы информацию о своей деятельности, связанной с оказанием услуг, предусмотренных Правилами, а также связанную с выполнением возложенных на них функций и обязанностей в рамках платежной системы.

27. Действия и меры принуждения, применяемые Оператором в отношении Участников и Расчетного центра в случае нарушения ими обязательств, принятых на себя в соответствии с настоящими Правилами.

27.1. В случаях, если нарушения Участников и Расчетного центра обязательств, принятых на себя в соответствии с настоящими Правилами, не влияют на бесперебойность функционирования Платежной системы, либо на оказываемые ими услуги, Оператор осуществляет следующие действия:

- доводит до сведения Участников и Расчетного центра информацию о выявленном нарушении в письменной форме с указанием допущенного нарушения и срока, в течение которого такое нарушение должно быть устранено, при этом указанный срок не может быть менее 5 (Пяти) рабочих дней;
- осуществляет контроль за устранением Участниками и Расчетным центром выявленного нарушения в установленный в уведомлении срок.

27.2. В случаях, если нарушения Участниками и Расчетным центром обязательств, принятых на себя в соответствии с настоящими Правилами, влияют на бесперебойность функционирования Платежной системы, либо на оказываемые ими услуги, Оператор применяет одну из следующих мер принуждения:

- направляет Участникам и Расчетному центру уведомление об устранении нарушения с указанием срока для его устранения;
- ограничивает (приостанавливает) оказание операционных услуг и (или) услуг Платежного клиринга и (или) иных услуг, установленных в Приложении №1 к Правилам (Тарифы), определяемых Оператором;
- приостанавливает участие в Платежной системе в соответствии с Правилами/ приостанавливает действие договора с Расчетным центром.

Меры принуждения, предусмотренные пунктом 2 настоящей статьи, применяются Оператором также в следующих случаях:

- при действиях (бездействии) Участников и Расчетного центра, повлекших (повлекшем) приостановление (прекращение) осуществления переводов денежных средств в рамках Платежной системы либо их несвоевременное осуществление;
- если уведомление Оператора об устранении выявленного нарушения, направленное в соответствии с пунктом 1 настоящей статьи, не было выполнено Участниками и Расчетным центром в установленный срок.

27.3. Меры принуждения вводятся на основании направляемого Оператором платежной системы уведомления. Уведомление идентифицирует нарушение и определяет срок, в течение которого нарушение должно быть устранено. Указанный срок не должен превышать 45 (Сорок пять) календарных дней.

27.4. В случае если по истечении срока действия мер принуждения, указанных в подпунктах 2 и 3 пункта 2 настоящей статьи, допущенные нарушения не устранены, срок действия данной меры принуждения может быть продлен Оператором платежной системы до устранения нарушения.

27.5. Уведомление Оператора платежной системы о применении мер принуждения, направляется Участнику платежной системы или Расчетному центру, в отношении которых вводится ограничение.

27.6. В случае неоднократного невыполнения уведомлений с требованием об устранении нарушения, влияющего на бесперебойность функционирования Платежной системы, в течение одного года со дня направления Оператором платежной системы первого уведомления об устранении такого нарушения Оператор платежной системы вправе прекратить участие Участника платежной системы в Платежной системе в соответствии с условиями приостановления и прекращения участия в Платежной системе, установленными Правилами.

28. Ответственность за несоблюдение Правил.

28.1. Субъекты Платежной системы несут ответственность за неисполнение или ненадлежащее исполнение своих обязательств в соответствии с законодательством Российской Федерации и Правилами.

28.2. В случае неисполнения Участником платежной системы предусмотренных Правилами и договором участия обязательств, связанных с обеспечением достаточности денежных (установленного лимита) средств на счете Участника платежной системы для осуществления расчетов по операциям, совершенным клиентами Участника платежной системы, а также в случае неисполнения обязательств по оплате оказанных услуг, указанных в Тарифах (Приложение №1 к Правилам), Оператор платежной системы на основании письменного требования вправе применить и начислить, а Участник платежной системы обязан (в случае начисления) уплатить пеню в размере 0,1% (Ноль целых одна десятая процентов) от недостающей суммы за каждый день просрочки.

28.3. В случае неоднократного нарушения Участником платежной системы Правил, Оператор платежной системы вправе лишить организацию статуса Участника платежной системы, расторгнув договор участия в одностороннем порядке с последующим уведомлением организации о расторжении договора участия.

28.4. В случае однократного неисполнения Участником платежной системы предусмотренных Правилами и договором участия обязательств, связанных с обеспечением завершения расчетов, Оператор платежной системы вправе лишить организацию статуса Участника платежной системы, расторгнув договор участия в одностороннем порядке с последующим уведомлением организации о расторжении договора участия.

28.5. В случае сбоев в Системе или наступления иных обстоятельств, повлекших излишнее перечисление, неперечисление или неполное перечисление денежных средств, связанных с работой в Системе, Оператор обязуется в кратчайшие сроки устранить последствия таких сбоев или обстоятельств. Штрафные санкции со стороны, допустившей неперечисление, перечисление в неполном объеме или перечисление излишних денежных средств, вызванное вышеуказанными сбоями или обстоятельствами, не взимаются.

28.6. Оператор несет ответственность по возмещению убытков в размере реального ущерба, подтвержденного документально, причиненного Участникам или Расчетному центру вследствие несоблюдения Оператором настоящих Правил, неисполнения или ненадлежащего исполнения своих обязательств.

28.7. Оператор не несет ответственности за наступление неблагоприятных последствий для третьих лиц, включая Клиентов, возникших в результате неисполнения Участником или Расчетным центром ненадлежащего/несвоевременного исполнения обязательств, предусмотренных Правилами Системы и договорами/соглашениями.

28.8. Оператор и Расчетный центр не несут ответственности за нарушения в работе Системы, произошедшие в следствие:

- неквалифицированного обслуживания или неисправности оборудования (в том числе каналов связи) Участников, третьих лиц, предназначенного для работы в системе;
- неквалифицированного использования Участниками, их сотрудниками программного обеспечения, предназначенного для использования в системе;
- неквалифицированных действий со стороны сотрудников Участника, взаимодействующих посредством автоматизированных рабочих мест, в том числе несанкционированного доступа неуполномоченных лиц к данным Системы.

28.9. Субъекты платежной 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 платежной системы разумными средствами, в том числе:

землетрясения, наводнения, пожары, эпидемии, аварии на транспорте, военные действия, массовые беспорядки и др.

Субъект платежной системы, подвергшийся действию обстоятельств непреодолимой силы и оказавшийся вследствие этого не в состоянии выполнить свои обязательства, должен сообщить об этом в течение одного рабочего дня с момента возникновения указанных обстоятельств в устной форме и в течение трех рабочих дней в письменной форме Оператору платежной системы, в противном случае Субъект платежной 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.

29. Порядок изменения Правил Платежной системы «ХЕЛЛО».

29.1. Изменения и/или дополнения в Правила вносятся Оператором платежной системы в одностороннем порядке.

29.1.1. Для внесения изменений и/или дополнений в Правила Оператор платежной системы обязан обеспечить Участникам платежной системы возможность предварительного ознакомления с предлагаемыми изменениями и/или дополнениями и направления своего мнения Оператору платежной системы в установленный им срок, который не может быть менее одного месяца. Возможность предварительного ознакомления с предлагаемыми изменениями и/или дополнениями обеспечивается путем размещения предлагаемых изменений и/или дополнений на официальном сайте Оператора платежной системы в информационно-телекоммуникационной сети «Интернет». Субъекты Системы самостоятельно на ежедневной основе осуществляют проверку информации, размещения документов об изменениях и/или дополнениях в Правила платежной системы на официальном сайте Оператора.

29.1.2. Изменения и/или дополнения в Правила вступают в силу в срок не менее одного месяца со дня окончания срока, указанного в п. 29.1.1 раздела 29 Правил.

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

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

- проект Правил Системы или предлагаемых изменений с указанием срока вступления изменений в силу;
- информацию о сроке (не менее 30 дней), в течение которого Субъекты могут направить Оператору уведомления о согласии или несогласии с вносимыми изменениями, и адрес для сбора уведомлений.

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

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

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

29.2.5. Правила Системы считаются согласованными всеми Субъектами Системы в случае, если в срок, указанный Оператором Системы, не поступило ни одного уведомления о несогласии с вносимыми изменениями. В данном случае, изменения вступают в силу не ранее, чем через 1 месяц, после окончания срока, указанного Оператором Системы.

29.3. В случае если Правила Системы не согласованы всеми сторонами, Оператор Системы имеет право инициировать повторную процедуру внесения изменений в Правила Системы по соглашению всех сторон либо инициировать внесение изменений в одностороннем порядке в соответствии с п. 29.1. настоящих Правил.

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

29.5. В Банк России, одновременно с Правилами, предоставляются все документы, составляющие Правила Платежной системы «ХЕЛЛО».

29.6. Срок вступления в силу Правил указывается в Правилах и публикуется на сайте Оператора в сети «Интернет» по адресу: www.hellopay.online

Приложения к Правилам, которые входят в состав настоящихПравил:

- Приложение №1 «Тарифы (перечень и стоимость услуг)».
- Приложение №2 «Регламент электронного документооборота».
- Приложение№3 «Перечень документов, предоставляемый Участниками ОператоруПлатежной системы «ХЕЛЛО»».
- Приложение №4 «Форма договора участия в Платежной системе «ХЕЛЛО» (для прямогоУчастника)».
- Приложение №5 «Форма договора участия в Платежной системе «ХЕЛЛО» (для косвенного Участника)».
- Приложение №6 «Протокол внесения изменений в Правила Платежной системы «ХЕЛЛО»».
- Приложение №7 «Положение по управлению рисками и бесперебойности функционирования ПС «ХЕЛЛО»».
- Приложение №8 Анкета «Выполнение требований по обеспечению защиты информации».

Приложение №1
к Правилам Платежной системы «ХЕЛЛО»

Т А Р И Ф Ы
Платежной системы
«ХЕЛЛО»

1. Общие положения

✓ Оператор имеет право устанавливать обменный курс, применяемый в Системе при осуществлении расчетов, как с Участниками Системы, так и с Клиентами, по переводам денежных средств при различии валюты, предоставленной Отправителем – физическим лицом, и валюты переводимых и/или выплачиваемых денежных средств.

✓ Используемые иностранные валюты: Азербайджанский манат (AZN), Алжирский динар (DZD), Армянский драм (AMD), Бахрейнский динар (BHD), Белорусский рубль (DYN), Бразильский реал (BRL), Вьетнамский донг (VND), Гонконгский доллар (HKD), Грузинский лари (GEL), Дирхамы ОАЭ (AED), Доллар США (USD), ЕВРО (EUR), Египетский фунт (EGP), Индийская рупия (INR), Индонезийская рупия (IDR), Казахстанский тенге (KZT), Китайский юань (CNY), Киргизский сом (KGS), Молдавский лей (MDL), Оманский риал (OMR), Сингапурский доллар (SGD), Таджикский сомони (TJS), Турецкая лира (TRY), Узбекский сум (UZS), Южноафриканский рэнд (ZAR).

✓ Оператор имеет право проводить различные акции лояльности и другие маркетинговые мероприятия, связанные с установлением соответствующего размера комиссионного вознаграждения, направленные на продвижение Услуг Платежной системы «ХЕЛЛО», стимулирование Участников и Клиентов. Данные мероприятия могут иметь ограниченный срок действия, Оператор имеет право в любой момент времени отменить, изменить условия проводимых акций, а также продлить срок действия указанных мероприятийнеограниченное количество раз. Информация о проводимых акциях доводится до Участников заблаговременно путем уведомления Участника по информационным каналамсвязи.

✓ В случаях, когда комиссионное вознаграждение с Отправителя не взимается, комиссию, причитающуюся Участнику – отправителю и Участнику-исполнителю, уплачивает Оператор, если иное не предусмотрено соглашением между участником (-ами) по условиям проведения акции.

✓ Оператор Системы имеет право вносить изменения в Тарифы Системы. При внесении в правила платежной системы изменений, предусматривающих введение новых тарифов или увеличение размера тарифов, оператор платежной системы обязан уведомить об этом Банк России в срок не менее чем за 30 календарных дней до дня введенияв действие изменений в правила платежной системы и предоставить обоснование указанных изменений. Оператор имеет право в пределах тарифной сетки, заявленной в Тарифах ПС ХЕЛЛО, в одностороннем порядке менять размер оплаты услуг операторов платежной инфраструктуры и размер комиссии, уплачиваемой Оператором Участникам за обслуживание Отправителей или Получателей. При этом, информацию об изменениях размера комиссий, причитающихся Операторам платежной инфраструктуры и Участникам, Оператор обязуется направить заблаговременно, по официальным каналам связи.

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

✓ Оператор Системы не устанавливает комиссию за участие в Платежной системе «ХЕЛЛО».

2.Общие принципы взимания комиссии с Отправителей:

- комиссия взимается в полном объеме участником, обслуживающим отправителя (Участником – отправителем);
- комиссия взимается сверх суммы Перевода.

2.1. Комиссия может быть выражена:

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

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

- от суммы перевода;
- от используемых отправителем средств осуществления перевода, в том числе электронных средств платежа, и форм безналичных расчетов;
- от выбранного отправителем места осуществления перевода;
- наличия/отсутствия дополнительных сопутствующих переводу услуг;
- наличия/отсутствия посредников в осуществлении перевода.

2.3. Тарифы Системы признаются Тарифами для обслуживания физических лиц каждого участника, оказывающего Услуги Платежной системы «ХЕЛЛО» отправителю.

2.4. При использовании участником при обслуживании отправителей различных средств дистанционного банковского обслуживания, банковских счетов, при привлечении банковских платежных агентов (субагентов), а также, осуществление денежных переводов через определенные ПОК участника, допускается установление комиссии для физических лиц самим участником, сверх комиссии за перевод, установленной Оператором, при условии согласования размера данных комиссий с Оператором Системы.

Размер комиссий, устанавливаемый участником сверх комиссии Оператора, не является Тарифами Системы.

2.5. Настоящая информация о Тарифах Системы за оказание Услуг Платежной системы «ХЕЛЛО», также доставляется участнику Оператором Системы в процессе совершения операции.

2.6. Тарифы Системы, а также самостоятельно установленные участником в соответствии с п.п. 2.4 настоящих Тарифов, доводятся до клиентов, обслуживаемых участником, в порядке, устанавливаемом участником, но обязательно до момента внесения/списания денежных средств клиентом.

3. Порядок определения комиссионного вознаграждения Участников, в т.ч. порядок оплаты услуг платежной инфраструктуры.

3.1. Размер комиссионного вознаграждения участников Системы определяется оператором Системы, за исключением вознаграждения участника, использующего право самостоятельного установления тарифов для физических лиц в соответствии с п.п. 2.4 Тарифов.

3.2. Комиссия, взимаемая Участником с физических лиц, распределяется следующим образом:

- вознаграждение участника остается в его распоряжении, если иное не предусмотрено соответствующим договором с оператором Системы;
- вознаграждение оператора Системы перечисляется участником, обслуживающим отправителя (т.е. инициирующего операцию), вместе с комиссионным вознаграждением участника, обслуживающего получателя;
- оператор Системы выплачивает комиссионное вознаграждение участнику, обслуживающему получателя, за окончательную доставку денежных средств получателю через Систему.

3.3. В случаях, когда комиссионное вознаграждение с отправителя не взимается или ниже установленного Тарифа для клиентов, Оператор системы уплачивает комиссионное вознаграждение участнику-отправителю, обслуживающему отправителя, за прием распоряжения клиента об осуществлении перевода денежных средств через Систему и участнику–исполнителю, обслуживающему получателя за выдачу денежных средств через Систему.

3.4. Общие принципы определения комиссионного вознаграждения для участников. Комиссия может быть выражена:

- в процентном отношении к сумме перевода;
- в процентном отношении к сумме перевода плюс фиксированная сумма;
- в фиксированной сумме;
- в процентном отношении к сумме комиссии, взимаемой с физического лица;
- в процентном отношении к сумме перевода, но не более чем определенная доля от суммы комиссии, взимаемой с физического лица;
- в процентном отношении к сумме комиссии, являющейся системно установленной.

3.5. Размер комиссии участников может варьироваться, в том числе в зависимости:

- от географического направления перевода;
- от суммы перевода;
- операций, осуществляемых участником в отношении перевода;
- от используемых участником средств осуществления перевода;
- валюты перевода;
- от выбранного Отправителем места осуществления перевода: с использованием средств дистанционного банковского обслуживания, в офисах третьих лиц, привлекаемых участниками и т.п.;
- от способа доставки перевода Получателю;
- различия валюты перевода и валюты выплаты.
- комиссия взимается в валюте перевода, если иное не установлено соответствующим договором участника с Оператором.
- от наличия/отсутствия дополнительных сопутствующих переводу услуг;
- от наличия/отсутствия посредников в переводе, сумма комиссии округляется по правилам, установленным Оператором Системы[i].

3.6. Процедуры расчета и уплаты комиссии осуществляются операторами услуг платежной инфраструктуры Системы в рамках общих процедур клиринга и расчетов, в частности, комиссии включаются в платежную клиринговую позицию по каждому Участнику.

3.7. Оплата комиссии Оператора осуществляется путем направления Оператором распоряжения в Расчетный центр для зачисления комиссионного вознаграждения на расчетный счет Оператора. Расчет комиссии Оператора осуществляется в соответствии с порядком, предусмотренным настоящими Тарифами.

4. Перечень и стоимость услуг[ii]

4.1. Комиссия Расчетного центра**.**

Оператор, на основании договора, заключенного с Расчетным центром, ежемесячно уплачивает Расчетному центру комиссию, в срок не позднее 5 числа месяца, следующего за отчетным или иного согласованного срока, порядка оплаты.

---

[i] Участники имеют право установить индивидуальные правила округления в связи с особенностями налично-денежного обращения страны местонахождения (регистрации) (за исключением Участников – резидентов РФ).

[ii] Данные услуги НДС не облагаются в соответствии с пп.4 п.3 ст.149 Налогового кодекса Российской Федерации «операции, осуществляемые организациями, обеспечивающими информационное и технологическое взаимодействие между участниками расчетов, включая оказание услуг по сбору, обработке и предоставлению участникам расчетов информации по операциям с банковскими картами».

Тарифы Платежной системы «ХЕЛЛО»

Категория перевода денежных средств	Тип операции	Тарифы для клиентов[iii] (ТДК)	Тарифы для Участников[iv] (ТУ)
Переводы в пределах Российской Федерации	Отправка Переводов денежных средств без открытия счета по территории Российской Федерации	- От 0% до 6% от суммы Перевода денежных средств; - и/или фиксированная сумма от 0 рублей до 1500 рублей	- От 0% до 45% от суммы комиссии, уплачиваемой Клиентом в соответствии с Тарифами для Клиентов; - и/или от 0% до 1% от суммы Перевода денежных средств; - и/или фиксированная сумма от 0 рублей до750 рублей.
	Выплата Переводов денежных средств без открытия счета по территории Российской Федерации	Плата не взимается	- От 0% до 35 % от суммы комиссии, уплачиваемой Клиентом в соответствии с Тарифами для Клиентов; - и/или от 0% до 1% от суммы Перевода денежных средств; - и/или фиксированная сумма от 0 рублей до750 рублей.
Трансграничные переводы	Отправка Переводов денежных средств без открытия счета из Российской Федерации	- От 0% до 6% от суммы Перевода денежных средств; -и/или фиксированная сумма от 0 рублей/долларов США до 6000 рублей/300 долларов США/эквивалент в валюте перевода	- От 0% до 45 % от суммы комиссии, уплачиваемой Клиентом в соответствии сТарифами для Клиентов; - и/или от 0% до 1,5% от суммы Переводаденежных средств -и/или фиксированная сумма от 0 рублей/долларов США до 3000 рублей/150 долларов США/ эквивалент в валюте перевода
	Выплата Переводов денежных средств без открытия счета	Плата не взимается	- От 0% до 45 % от суммы комиссии, уплачиваемой Клиентом в соответствии сТарифами для Клиентов; - и/или от 0% до 1,5% от суммы Переводаденежных средств -и/или фиксированная сумма от 0 рублей/долларов США до 3000 рублей/150 долларов США/ эквивалент в валюте перевода
Транзитные переводы	Отправка Переводов денежных средств без открытия счета за пределами РФ	- От 0% до 6% от суммы Перевода денежных средств; -и/или фиксированная сумма от 0 рублей/долларов США до 6000 рублей/300 долларов США/ эквивалент в валюте перевода	- От 0% до 45 % от суммы комиссии, уплачиваемой Клиентом в соответствии сТарифами для Клиентов; - и/или от 0% до 1,5% от суммы Переводаденежных средств -и/или фиксированная сумма от 0 рублей/долларов США до 3000 рублей/150 долларов США/ эквивалент в валюте перевода
	Выплата Переводов денежных средств без открытия счета за пределами РФ	Плата не взимается	- От 0% до 45 % от суммыкомиссии, уплачиваемой

			Клиентом в соответствии сТарифами для Клиентов; - и/или от 0% до 1,5% от суммы Переводаденежных средств -и/или фиксированная сумма от 0 рублей/долларов США до 3000 рублей/150 долларов США/ эквивалент в валюте перевода
Оплата в пользу юридических лиц за товары, работы, услуги	- от физических лиц с целью увеличения/уменьшения остатка электронных денежных средств; - от физических лиц для зачисления на счета физических лиц в кредитных организациях, в том числе переводы на карты Visa, MasterCard; - от физических лиц юридическим лицам/индивидуальным предпринимателям в счет оплаты услуг; - от физических лиц юридическим лицам, при предоставлении полных реквизитов платежа	- От 0% до 25% от суммы Перевода денежных средств; -и/или фиксированная сумма от 0 до 1000 рублей	- От 0% до 75% от суммы комиссии, уплачиваемой Клиентом в соответствии сТарифами для Клиентов; -и/или от 0% до 20% от суммы Переводаденежных средств; - и/или фиксированная сумма от 0 до 400рублей
Переводы денежных средств с использованием реквизитов банковской карты по реквизитам банковской карты Получателя	Отправка Переводов денежных средств с использованием реквизитов банковской карты Выплата Переводов денежных средств по реквизитам банковской карты Получателя	- От 0% до 20% от суммы Перевода денежных средств -и/или фиксированная сумма от 0 до 1000 рублей	- От 0% до 75% от суммы комиссии, уплачиваемой Клиентом в соответствии сТарифами для Клиентов; -и/или от 0% до 20% от суммы Переводаденежных средств; - и/или фиксированная сумма от 0 до 400рублей
Перевод денежных средств от юридических лиц в пользу физических лиц	- от юридических лиц физическим лицам, при предоставлении полных реквизитов платежа	- От 0% до 30% от суммы Перевода денежных средств -и/или фиксированная сумма от 0 до 10000 рублей	- От 0% до 75% от суммы комиссии, уплачиваемой Клиентом в соответствии сТарифами для Клиентов; -и/или от 0% до 20% от суммы Переводаденежных средств; - и/или фиксированная сумма от 0 до 4000рублей
Перевод денежных средств с использованием Платежных методов (способов), предоставленных	Перевод денежных средств с использованием реквизитов банковской карты: - от физических лиц с целью увеличения/уменьшения остатка электронных денежных средств;	- От 0,7% до 10 % от суммы Перевода денежных средств с использованием предоставленного Оператором платежной системы Платежного метода (способа).	- От 0,7% до 10 % от суммы комиссии, уплачиваемой Клиентом в соответствии сТарифами для Клиентов.

Оператором платежной системы (включая трансграничные переводы)	- от физических лиц для зачисления на счета физических лиц в кредитных организациях, в том числе переводы на карты Visa, MasterCard; - от физических лиц юридическим лицам/индивидуальным предпринимателям в счет оплаты товаров и услуг; - от физических лиц юридическим лицам, при предоставлении полных реквизитов платежа; - от юридических лиц физическим лицам, при предоставлении полных реквизитов платежа - от юридических лиц юридическим лицам при предоставлении полных реквизитов платежа.		

Тариф Оператора, выполняющего функции Операционного центра и ПКЦ рассчитывается по следующей формуле:
ТДК – ТУ – ТВПС = Тариф Оператора

Настоящие Тарифы входят в состав Правил Платежной системы «ХЕЛЛО»

[iii] Информация о конкретном размере комиссионного вознаграждения, взимаемого с Плательщика за осуществление Денежного перевода, размещается на официальном сайте ПС ХЕЛЛО, а также доводится до сведения Плательщика до момента осуществления Перевода денежных средств в письменном виде в Пунктах обслуживания Клиентов.

[iv] Перевода денежных средств в письменном виде в Пунктах обслуживания Клиентов.

Информация о конкретном размере комиссионного вознаграждения Участников ПС ХЕЛЛО определяется Оператором ПС ХЕЛЛО и фиксируется в ПК ХЕЛЛО.

[v] Конкретный размер комиссионного вознаграждения Взаимодействующих платежных систем определяется в договоре о взаимодействии платежных систем.

Приложение № 2
к Правилам Платежной системы «ХЕЛЛО»

Регламент электронного документооборота

С О Д Е Р Ж А Н И Е

№ пункта	Наименование раздела, пункта
	Термины и определения
1.	Общие положения
2.	Права и обязанности
3.	Правила подключения к Системе с использованием WEB-клиента «ХЕЛЛО»
4.	Правила подключения к Системе с использованием Протокола «ХЕЛЛО»
5.	Условия признания электронных документов
6.	Ответственность
7.	Порядок разрешения споров
8.	Требования к защите информации
	Приложения
1.	Заявление Пользователя Участника Платежной системы «ХЕЛЛО»
1.1.	Заявление Уполномоченного лица Участника Платежной системы «ХЕЛЛО»

2.	Запрос сертификата ключа проверки ЭП подписи
3.	Заявление на отзыв сертификата
4.	Акт о технологической готовности (к Заявке на интеграцию)
5.	Заявка на интеграцию с ИТ-платформой Платежной системы «ХЕЛЛО»
6.	Отчет об инцидентах

Термины и определения

Термины и определения, используемые в настоящем Регламенте электронного документооборота, соответствуют значению терминов и определений, указанных в Правилах Платежной системы «ХЕЛЛО» (далее - Правила Системы).

Регламент электронного документооборота (РЭД) – настоящий регламент, определяющий условия, порядок подключения и алгоритм обмена электронными документами с использованием Программного комплекса «ХЕЛЛО».

Договор – договор, на основании которого Участник присоединился к Правилам Системы.

Программный комплекс «ХЕЛЛО» (ПК «ХЕЛЛО») –программное обеспечение Системы (WEB- клиент «ХЕЛЛО», Протокол «ХЕЛЛО», средства СКЗИ), обеспечивающее доступ Участникам к Системе в целях осуществления деятельности в рамках заключенного Договора.

WEB-клиент «ХЕЛЛО» –Программное обеспечение Оператора Системы, используемое Участником для доступа к Системе.

Протокол «ХЕЛЛО» – технические условия, обеспечивающие возможность Участнику получитьдоступ к Системе с использованием программного обеспечения Участника.

Пользователь Системы (Пользователь) – лицо, назначенное и указанное Участником, осуществляющий обмен электронными документами в Системе и выполняющий функции:

- по управлению криптографическими ключами Участника;
- по регистрации и управлению полномочиями Пользователей Участника;
- по регистрации и управлению пунктами Участника;
- по информированию Оператора Системы о выявленных в Системе инцидентах.

Уполномоченное лицо (УЛ) – Пользователь, действующий на основании Заявления (Приложение 1.1. к РЭД) и выполняющий функции:

- по управлению криптографическими ключами Участника;
- по регистрации и управлению полномочиями Пользователей Участника;
- по регистрации и управлению пунктами Участника;
- по информированию Оператора Системы о выявленных в Системе инцидентах.

Удостоверяющий центр Оператора Системы (УЦ) – функциональное подразделение Оператора Системы, осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим РЭД.

Привлеченный Удостоверяющий центр – аккредитованная Оператором системы организация, имеющие лицензии на деятельность по технической защите конфиденциальной информации.

Электронный документ – информация, представленная в электронной форме подписанная электронной подписью.

Электронная подпись (ЭП) – информация в электронной форме, связанная с другой информацией в электронной форме (подписываемой информацией), которая используется для определения лица, подписавшего информацию.

Ключ электронной подписи (Ключ подписи) – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с Ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее – проверка электронной подписи).

Криптографические ключи – ключ подписи и соответствующий ему ключ проверки электронной подписи.

Сертификат ключа проверки электронной подписи (Сертификат ключа) – электронный документ с ЭП УЦ, подтверждающий принадлежность Ключа проверки электронной подписи Участнику.

Запрос сертификата – электронный документ (PKCS #10), содержащий ключ проверки электронной подписи, параметры алгоритма, данные Пользователя, данные Участника.

Копия запроса сертификата –документ на бумажном носителе, заверенный подписью руководителя и печатью Участника, содержащий данные запроса сертификата.

Средство электронной подписи – криптографические средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание Ключа электронной подписи и ключа проверки электронной подписи.
Компрометация ключа – факт или угроза несанкционированного использования ключа подписи неуполномоченными лицами.
Руководство пользователя - внутренний нормативный документ, утвержденный Оператором Системы, регламентирующий порядок работы Пользователя в ПК «ХЕЛЛО», являющийся неотъемлемой частью настоящего РЭД.
Руководство Уполномоченного лица - внутренний нормативный документ, утвержденный Оператором Системы, регламентирующий порядок работы Уполномоченного лица, являющийся неотъемлемой частью настоящего РЭД.
Сертификат соответствия «ХЕЛЛО» - документ на бумажном носителе, выданный Оператором Системы, подтверждающий соответствие программного обеспечения Участника требованиям Протокола «ХЕЛЛО».

1. Общие положения.

1.1. Действие РЭД:

1.1.1. Положения настоящего РЭД становятся обязательными для Участников и Пользователей Системы с момента подписания соответствующего Договора.

1.1.1.1. В случае предоставления Участником данных об Уполномоченном лице - положения настоящего РЭД становятся обязательными для Уполномоченного лица с момента подписания соответствующего Договора при наличии предоставления данных об Уполномоченном лице в соответствии с положениями настоящего РЭД, при этом применяется Руководство Уполномоченного лица.

1.1.2. Требования настоящего РЭД являются обязательными для Участников и Пользователей в течение срока действия Договора. Условия настоящего РЭД принимаются Участниками и Пользователями Системы полностью, без каких-либо изъятий, изменений, ограничений и протоколов разногласий.

1.1.2.1. В случае предоставления Участником данных об Уполномоченном лице - требования настоящего РЭД являются обязательными для Уполномоченного лица в течение срока действия Договора при наличии предоставления данных об Уполномоченном лице в соответствии с положениями настоящего РЭД. Условия настоящего РЭД принимаются Уполномоченным лицом Системы полностью, без каких-либо изъятий, изменений, ограничений и протоколов разногласий.

1.1.3. Оператор Системы имеет право в одностороннем порядке вносить изменения и дополнения в настоящий РЭД, включая приложения к нему, предварительно уведомив Участника о таких изменениях за 10 (десять) календарных дней до вступления в силу изменений в РЭД (новый РЭД).

1.1.4. В случае отсутствия заявлений со стороны Участника о назначении Пользователя (Пользователей), Уполномоченных лиц (Заявления по форме Приложений 1, 1.1. к РЭД), положения и требования РЭД применяются к лицу, подписавшему Договор (договор присоединения), применяемых к Пользователю, при этом Приложения (за исключением Приложений 1, 1.1. к РЭД) оформляются в качестве Участника.

1.2. Общие положения информационной безопасности

- Оператор Системы обеспечивает информационную безопасность при информационном взаимодействии Абонентов и операторов услуг платежной инфраструктуры в соответствии с Правилами Системы.
- Абоненты самостоятельно обеспечивают информационную безопасность при организации ЭДО внутри своей корпоративной информационной системы.

1.3. Для проведения работ по обеспечению защиты информации при осуществлении переводов денежных средств могут привлекаться организации, имеющие лицензии на

деятельность по технической защите конфиденциальной информации.

1.4. Электронный документооборот осуществляется в порядке и на условиях, определенных:

1) Настоящим Регламентом

2) Правилами аккредитованного Удостоверяющего центра Транскапиталбанка (www.tkbbank.ru)

1.5. Все Приложения к настоящему РЭД являются его неотъемлемой частью. Положения РЭД предусматривают возможность подписания и предоставления соответствующих Приложений к РЭД Пользователем, Уполномоченным лицом при условии наличия соответствующих Заявлений по форме Заявления 1, 1.1. к РЭД.

2. Права и обязанности.

2.1. Оператор Системы имеет право:

2.1.1. Вносить изменения в порядок функционирования ПК «ХЕЛЛО» с обязательным извещением об этом Участника не позднее, чем за 10 (десять) календарных дней до вступления в силу указанных изменений по согласованному каналу связи.

2.1.2. Отказать в изготовлении Сертификата ключа Участнику в случае ненадлежащего оформления запроса сертификата, нарушения «Правил Системы» или настоящего РЭД.

2.1.3. Запрашивать у Участника документы и сведения, которые связаны с исполнением: Договора, «Правил Системы» и настоящего РЭД.

2.1.4. Отозвать Сертификат ключа Участника в случае:

• обращения (по ПК «ХЕЛЛО», e-mail, письменно или по телефону) Участника;

•компрометации ключа подписи, с уведомлением Участника и указанием причин;

• указания лиц или органов, имеющих такое право в силу закона.

2.2. Участник имеет право:

2.2.1. Получать бесплатные консультации по работе в Системе.

2.2.2. Получить список отозванных Сертификатов ключей, изготовленный УЦ.

2.2.3. Направлять Оператору Системы запросы на изготовление Сертификатов ключей Пользователей.

2.2.4. Запрашивать у Оператора Системы любые сведения, необходимые для осуществления своих функций в соответствии с настоящим РЭД.

2.2.5. Назначить Пользователя (Пользователей), Уполномоченное лицо посредством предоставления Заявления Пользователя, УП (Приложения 1, 1.1. к РЭД). Уполномоченное лицо обязано исполнять положения РЭД по аналогии положений РЭД в полном объеме, применяемых к Пользователю, а также обязано исполнять Руководство Уполномоченного лица.

2.2.6. Положения и требования настоящего РЭД применяются к Уполномоченному лицу по аналогии положений РЭД, применяемых к Пользователю.

2.3. Пользователь имеет право:

2.3.1. Получать бесплатные консультации по работе в Системе.

2.3.2. Получить реквизиты доступа в Систему.

2.3.3. Самостоятельно формировать свои криптографические ключи.

2.3.4. Получить Сертификаты ключей УЦ.

2.3.5. Получить список отозванных Сертификатов ключей, изготовленный УЦ.

2.3.6. Направлять Оператору Системы запросы на изготовление Сертификатов ключей Пользователей.

2.3.7. Запрашивать у Оператора Системы и у Участника любые сведения, необходимые для осуществления своих функций в соответствии с настоящим РЭД.

2.4. Оператор Системы обязан:

2.4.1. Осуществлять техническую поддержку Системы, в том числе предоставлять

Участнику и Пользователям по телефону/E-mail консультации по вопросам, возникающим в процессе эксплуатации Системы.

2.4.2. Использовать Ключи подписи УЦ только для подписи издаваемых им сертификатов ключей Пользователей и Списков отозванных сертификатов.

2.4.3. Принять меры по защите ключей подписи УЦ от несанкционированного доступа.

2.4.4. Организовать свою работу по GMT (GreenwichMeanTime) с учетом часового пояса города Москвы.

2.4.5. Вести реестр изготовленных УЦ сертификатов.

2.4.6. Обеспечить изготовление и передачу Сертификата ключа Пользователя в соответствии с порядком, определенным в настоящем РЭД. Сертификат ключа Пользователя выпускается на срок 1 (один) год. По истечении указанного срока Сертификат ключа подлежит замене в порядке, установленном настоящим РЭД, «Руководством пользователя», «Руководством Уполномоченного лица» (в случае применения).

2.4.7. Принимать и обрабатывать заявления на отзыв Сертификатов ключей от Пользователей/УЛ/Участника. Форма заявления на отзыв приведена в Приложении 3 настоящего РЭД.

2.4.8. Своевременно и периодически информировать Уполномоченных лиц, Пользователей, Участника об отзыве Сертификатов ключей путем выпуска Списка отозванных сертификатов. УЦ вносит изменения в Список отозванных Сертификатов ключей незамедлительно после получения информации об отзыве Сертификата ключа. В случае отсутствия изменений в Списке отозванных Сертификатов ключей в течение месяца, УЦ по истечении месяца подтверждает Список отозванных Сертификатов ключей путем его перевыпуска.

2.4.9. Готовить заключения по запросам Участника и уполномоченных государственных органов о подлинности ЭП в электронных документах.

2.4.10. В случае расторжения Договора отозвать Сертификаты ключей всех Пользователей в день такого расторжения.

2.5. Участник обязан:

2.5.1. Эксплуатировать Систему в строгом соответствии с «Руководством пользователя», «Руководством Уполномоченного лица» (в случае применения при наличии УЛ) и настоящим РЭД.

2.5.2. По запросу Оператора Системы предоставлять документы, подтверждающие полномочия Пользователя, Уполномоченного лица, иные документы и сведения, которые связаны с исполнением Договора и настоящим РЭД, в течение 3 (трех) рабочих дней с даты получения указанного запроса.

2.5.3. Хранить документы, подтверждающие полномочия Пользователей не менее 5 (пяти) лет.

2.5.4. Предоставить Пользователям письменные полномочия на подписание электронной подписью электронных документов в Системе от имени Участника.

2.5.5. В случае лишения любого Пользователя полномочий на подписание Электронной подписью Электронных документов в Системе, незамедлительно уведомить об этом Оператора Системы, с обязательным последующим направлением соответствующего письменного заявления Оператору Системы.

2.5.6. В случае компрометации ключей Пользователей немедленно уведомить об этом Оператора Системы, с обязательным последующим направлением соответствующего письменного заявления Оператору Системы.

2.5.7. Обеспечить рабочие места Пользователей необходимыми для работы в Системе совместимыми аппаратными, системными, сетевыми и телекоммуникационными средствами, программным обеспечением, средствами защиты информации (средствами электронной подписи, защиты от несанкционированного доступа, антивирусными средствами).

2.6. Пользователь обязан:

2.6.1. Эксплуатировать Систему в строгом соответствии с «Руководством пользователя».

2.6.2. Хранить в тайне личный Ключ подписи, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

В случае потери, раскрытия, искажения личного Ключа подписи, а также в случае если Пользователю стало известно, что этот ключ используется или использовался ранее другими лицами, немедленно прекратить использование ключа подписи в Системе и обратиться к Оператору Системы, с заявлением на отзыв Сертификата ключа.

2.6.3. Надлежащим образом исполнять требования, установленные настоящим РЭД.

2.6.4. Подписать запрос на изготовление Сертификата ключа Пользователя своим ключом и отправить подписанный запрос Оператору Системы.

2.6.5. Регистрировать пункты обслуживания Участника в Системе в соответствии с «Руководством пользователя».

2.6.6. По запросу Оператора Системы предоставлять документы, подтверждающие полномочия Пользователя, иные документы и сведения, которые связаны с исполнением Договора и настоящим РЭД, в течение 3 (трех) рабочих дней с даты получения указанного запроса.

2.6.7. Контролировать срок действия Сертификатов ключей Пользователей. До истечения срока действия Сертификата ключа Пользователя направить Оператору Системы запрос на изготовление нового сертификата.

2.6.8. Незамедлительно исправлять информацию о пунктах обслуживания Участника (в случае регистрации нового пункта, изменения адреса местонахождения зарегистрированного пункта, прекращения работы пункта, изменения набора услуг пункта и др.).

2.6.9. В случае компрометации ключа Пользователя немедленно прекратить его использование в Системе и обратиться к Оператору Системы, с заявлением на отзыв Сертификата ключа Пользователя.

2.6.10. В случае выявления инцидентов в текущем месяце направить отчет Оператору Системы по форме Приложения 6 к РЭД, не позднее пятого рабочего дня следующего месяца.

3. Правила подключения к Системе с использованием WEB-клиента «ХЕЛЛО».

Положения, изложенные в разделе 3 РЭД, применяются в случае предоставления Участником Заявлений по форме 1, 1.1., в случае реализации права Участника, предусмотренного п. 2.2.5. РЭД. В случае отсутствия представления указанных Заявлений, то лицом со стороны Участника, осуществляющий обмен электронными документами в Системе и соответствующие предусмотренные РЭД функции, является лицо, подписавшее Договор (договор присоединения), к которому применяются положения и требования РЭД, применяемых к Пользователю, в т.ч. настоящий раздел РЭД. В данном случае настоящий раздел применяется в части, которая не предусматривает предоставление Заявления по форме Приложения 1, 1.1. к РЭД.

3.1. Участник передает Оператору Системы на бумажном носителе Заявление Пользователя (Приложение 1 к РЭД).

3.2. Оператор Системы регистрирует Пользователя в Системе и высылает реквизиты доступа на E-mail указанный в Заявлении Пользователя**.**

3.3. Пользователь самостоятельно осуществляет генерацию личных криптографических ключей, формирует запрос сертификата ключа и передает Оператору Системы на бумажном носителе Запрос сертификата ключа проверки ЭПУЛ (Приложение 2 к РЭД), подписанный Пользователем и скрепленный печатью Участника.

3.4. Оператор Системы на основании полученных документов изготавливает Сертификат ключа Пользователя, регистрирует сертификат в Системе.

3.5. Пользователь самостоятельно регистрирует пункты обслуживания Участника в ПК «ХЕЛЛО».

3.6. Участник предоставляет Оператору системы документы, подтверждающие полномочия Пользователей на подписание электронной подписью электронных документов в ПК «ХЕЛЛО» от имени Участника.

3.7. Оператор Системы на основании предоставленных документов, регистрирует Пользователей в ПК «ХЕЛЛО» и передает Пользователям реквизиты доступа.

3.8. Пользователь самостоятельно осуществляет генерацию личных криптографических ключей, формирует запрос сертификата ключа.

3.9. Пользователь подписывает своей электронной подписью запрос сертификата Пользователя в ПК «ХЕЛЛО» и отправляет запрос Оператору Системы.

3.10. Оператор Системы на основании полученного от Пользователя запроса изготавливает Сертификат ключа Пользователя, регистрирует сертификат в Системе.

3.11. Осуществление Участником Переводов посредством ПК «ХЕЛЛО» производитсяпосле включения пунктов обслуживания Участника в Системе в рабочий режим в соответствии
«Руководством пользователя».

3.12. Оператор Системы обеспечивает информационное взаимодействие между Пользователем и УЦ.

4. Правила подключения к Системе с использованием Протокола «ХЕЛЛО».

Положения, изложенные в разделе 4 РЭД, применяются в случае предоставления Участником Заявлений по форме 1, 1.1. В случае отсутствия представления указанных Заявлений, то лицом со стороны Участника, осуществляющий обмен электронными документами в Системе и соответствующие предусмотренные РЭД функции, является лицо, подписавшее Договор (договор присоединения), к которому применяются положения и требования РЭД, применяемых к Пользователю, в т.ч. настоящий раздел РЭД. В данном случае настоящий раздел применяется в части, которая не предусматривает предоставление Заявления по форме Приложения 1, 1.1. к РЭД.

4.1. Участник оформляет Заявку на интеграцию (Приложение 5 к РЭД) и направляет оригинал её Оператору Системы по согласованным каналам, указанным в Договоре.

4.2. Оператор Системы высылает необходимую техническую документацию и тестовые криптографические ключи для доступа к тестовому ПК «ХЕЛЛО».

4.3. Участник проводит интеграционные работы и выполняет тестирование программного обеспечения по методике, предоставленной Оператором Системы.

4.4. По результатам успешного тестирования Оператор Системы выдает Участнику Сертификат соответствия.

4.5. Участник передает Оператору Системы на бумажном носителе Заявление Пользователя (Приложение 1 к РЭД).

4.6. Оператор Системы регистрирует Пользователя в Системе и высылает реквизиты доступа на электронный адрес, указанный в Заявлении Пользователя**.**

4.7. Пользователь самостоятельно осуществляет генерацию личных криптографических ключей, и передает Оператору Системы на бумажном носителе Запрос сертификата ключа проверки ЭП (Приложение 2 к РЭД), подписанный Пользователем и скрепленный печатью Участника.

4.8. Оператор Системы на основании полученных документов изготавливает Сертификат ключа Пользователя, регистрирует сертификат в Системе.

4.9. Пользователь формирует криптографические ключи и запрос сертификата ключа для программного обеспечения Участника.

4.10. Пользователь подписывает своей электронной подписью запрос сертификата ключа и отправляет его Оператору Системы.

4.11. Оператор Системы на основании полученного от Пользователя запроса изготавливает Сертификат ключа для программного обеспечения Участника, регистрирует сертификат в ПК «ХЕЛЛО».

4.12. Оператор Системы высылает реквизиты доступа к ПК «ХЕЛЛО» на электронный адрес Участника/Пользователя/Уполномоченного лица, указанный в Заявке на интеграцию.

4.13. Участник регистрирует пункты обслуживания в Системе с использованием собственного программного обеспечения или в ПК «ХЕЛЛО».

4.14. Осуществление Переводов посредством ПК «ХЕЛЛО» производится после подписания Участником Акта о технологической готовности (Приложение 4 к РЭД).

4.15. Оператор Системы обеспечивает информационное взаимодействие между Пользователем/Уполномоченным лицом и УЦ.

5. Условия признания электронных документов.

5.1. Электронные документы используются и признаются Оператором Системы и Участником юридически эквивалентными соответствующим документам на бумажном носителе, подписанным собственноручной подписью соответствующего уполномоченного лица и заверенным печатью при одновременном наличии следующего:

5.1.1 Оператор Системы получил бумажные копии документов:

✓ Заявление Пользователя/Уполномоченного лица (Приложения 1, 1.1. к РЭД) (при наличии), с учетом положений раздела 1, п. 2.2.5, 1-ого абз. разделов 3, 4 РЭД;

✓ Запрос сертификата ключа проверки ЭП (Приложение 2 к РЭД).

5.1.2. Подтверждение подлинности ЭП Пользователя в электронном документе дало положительный результат;

5.1.3. Сертификат ключа соответствующего Пользователя, подписавшего Электронный документ, не отозван и его действие не истекло на момент формирования ЭП в соответствующем электронном документе.

5.2. Электронные документы подлежат хранению Сторонами Договора в электронном виде не менее 5 (пяти) лет, если более длительный срок не установлен законодательством РФ.

6. Ответственность.

6.1. Участник несет ответственность за соблюдение положений, установленных настоящим РЭД в соответствии с действующим законодательством Российской Федерации.

6.2. Участник обязуется обеспечить соблюдение правил, установленных настоящим РЭД и Пользователями.

6.3. Участник несет ответственность за действия/бездействие Пользователя как за свои собственные. Участник не вправе в спорах ссылаться на ненадлежащее исполнение Пользователем своих обязательств.

6.4. В случае возникновения у Оператора Системы убытков по вине Пользователя, Участник обязуется компенсировать все причиненные убытки в полном объеме незамедлительно после получения письменного требования о возмещении убытков от Оператора Системы.

7. Порядок разрешения споров.

7.1. Оператор Системы, Участник и Пользователи не несут ответственности за неисправности линии связи или оборудования, приводящие к невозможности передачи электронных документов.

7.2. Оператор Системы не несет ответственность за убытки Участника, возникшие в результате использования Системы неуполномоченными лицами Участника, если такое использование стало возможным по небрежности или умыслу Участника и/или соответствующего Пользователя Системы или третьих лиц.

7.3. Споры и разногласия о признании подлинности ЭП в электронном документе разрешаются Оператором Системы и Участником путем создания Экспертной комиссии в составе равного количества представителей с каждой стороны, но не менее двух, при этом Экспертная комиссия должна руководствоваться тем, что:

7.3.1. Оператор Системы и Участник признают используемые в Системе средства

криптографической защиты информации достаточными для защиты от несанкционированного доступа и подтверждения подлинности ЭП в электронном документе.

7.3.2. Оператор Системы, Участники Пользователь признают, что внесение произвольных изменений в Электронный документ влечет за собой отрицательный результат проверки подлинности ЭП в электронном документе.

7.3.3. Оператор Системы, Участник и Пользователь признают, что создание ЭП в электронном документе невозможно без доступа к Ключу подписи.

7.4. Экспертная комиссия должна быть создана в течение 10 (десяти) рабочих дней с момента получения Оператором Системы/Участником письменного предложения о создании Экспертной комиссии от Оператора Системы/Участника. Расходы по созданию Экспертной комиссии несет сторона, предложившая ее создание.

7.5. Срок работы Экспертной комиссии не должен превышать 10 (десяти) рабочих дней, результат работы оформляется Экспертным заключением о признании подлинности ЭП в электронном документе.

7.6. В случае несогласия Оператора Системы/Участника с Экспертным заключением о признании подлинности ЭП в электронном документе, а также в случае уклонения от досудебного порядка рассмотрения споров, связанных с признанием подлинности ЭП в электронном документе, эти споры подлежат рассмотрению в Арбитражном суде г. Москвы в соответствии с законодательством РФ, при этом бремя доказывания тех или иных фактов и достоверности ЭП лежит на лице, которое на данные факты или доказательства ссылается.

8. Требования к защите информации.

8.1. Участник обеспечивает выполнение требований к обеспечению защиты информации, определенных в Правилах Системы, на объектах информационной инфраструктуры Участника, а также при выполнении Участником операций доступа, хранения, обработки и передачи защищаемой информации.

8.2. Оператор Системы обеспечивает защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного доступа и (или) уничтожения, ложной авторизации средствами Программного комплекса «ХЕЛЛО».

8.3. Оператор Системы определяет в Руководстве Пользователя и Руководстве Уполномоченного лица Программного Комплекса «ХЕЛЛО»: наименования используемых СКЗИ, порядок формирования/использования криптографических ключей, необходимые конфигурации программного обеспечения Участника, требования к информационной безопасности рабочих мест.

Приложения к настоящему РЭД:

Приложение 1 - Заявление Пользователя Участника Платежной системы «ХЕЛЛО».
Приложение 1.1. - Заявление Уполномоченного лица Участника Платежной системы «ХЕЛЛО».
Приложение 2 - Запрос сертификата ключа проверки ЭП.
Приложение 3 - Заявление на отзыв сертификата.
Приложение 4 - Акт о технологической готовности (к Заявке на интеграцию).
Приложение 5 - Заявка на интеграцию с ИТ-платформой Системы «ХЕЛЛО».
Приложение 6 - Форма отчета об инцидентах.

Регламент электронного документооборота входит в состав Правил Платежной системы «ХЕЛЛО».

Приложение 1
к Регламенту электронного документооборота

Заявление Пользователя
Участника Платежной системы
«ХЕЛЛО»

«___»_____20___г.

Настоящим Участник _____

_____

(Наименование, ОГРН, ИНН, адрес местонахождения)

в лице_____,

(Должность ФИО полностью)

действующего на основании_____, уполномочивает_____,

_____

(Должность ФИО Уполномоченного лица полностью)

выполнять функции Пользователя Участника Системы в рамках исполнения обязательств Участника Системы по Договору _____№_____ от «____»_____20___г., заключенного между

_____и

(наименование Участника)

_____,

(наименование Оператора Системы/Участника Системы, заключившего Договор)

а также поручается за соблюдение и исполнение Пользователем требований Платежной системы «ХЕЛЛО», Регламента электронного документооборота, Руководства пользователя Программного Комплекса «ХЕЛЛО».

Участник настоящим подтверждает, что отвечает за действия Пользователя, как за свои собственные, что в случае возникновения у Оператора Системы/Участника Системы убытков по вине Пользователя, обязуется компенсировать все причиненные убытки в полном объеме незамедлительно после получения письменного требования о возмещении убытков от Оператора Системы/Участника Системы.

Контактные данные Пользователя:
E-Mail:_____.
Контактный телефон:_____.

_____ _____

(Фамилия И.О. Пользователя) (Подпись)

_____ _____

(Фамилия И.О. Пользователя) (Подпись)

М. П.

Согласие прямого Участника

_____

_____(Наименование, ОГРН, ИНН, адрес местонахождения)

_____

Руководитель _____ _____

(Подпись)

М.П.

Приложение 1.1.
к Регламенту электронного документооборота

Заявление Уполномоченного лица
Участника Платежной системы
«ХЕЛЛО»

«___»_____20___г.

Настоящим Участник _____

_____

(Наименование, ОГРН, ИНН, адрес местонахождения)

в лице_____,

(Должность ФИО полностью)

действующего на основании_____, уполномочивает_____,

_____

(Должность ФИО Уполномоченного лица полностью)

выполнять функции Уполномоченного лица Участника Системы в рамках исполнения обязательств Участника Системы по Договору_____№_____от «____»_____20___г., заключенного между

_____и

(наименование Участника)

_____,

(наименование Оператора Системы/Участника Системы, заключившего Договор)

а также поручается за соблюдение и исполнение Уполномоченным лицом требований Платежной системы «ХЕЛЛО», Регламента электронного документооборота, Руководства Уполномоченного лица и Руководства пользователя Программного Комплекса «ХЕЛЛО».
Участник настоящим подтверждает, что отвечает за действия Уполномоченного лица, как за свои собственные, что в случае возникновения у Оператора Системы/Участника Системы убытков по вине Уполномоченного лица, обязуется компенсировать все причиненные убытки в полном объеме незамедлительно после получения письменного требования о возмещении убытков от Оператора Системы/Участника Системы.

Контактные данные Уполномоченного лица:
E-Mail:_____.
Контактный телефон:_____.

_____ _____
(Фамилия И.О. Уполномоченного лица) (Подпись)

_____ _____
(Фамилия И.О. Руководителя Участника) (Подпись)

М. П.

Согласие прямого Участника

_____

_____(Наименование, ОГРН, ИНН, адрес местонахождения)

_____

Руководитель _____ _____

(Подпись)

М.П.

Приложение 2 к Регламенту электронного документооборота

Запрос сертификата ключа проверки электронной подписи

«___» _____ 202___ г.

Сведения об организации:

1. Наименование организации _____
2. Юридический адрес _____
3. Почтовый адрес _____
4. Телефон _____
5. Факс _____

Сведения об абоненте:

1. Фамилия, Имя, Отчество _____
2. Должность _____
3. Удостоверение личности _____

Личная подпись абонента _____

Подпись руководителя _____

МП

Параметры ключа:
Алгоритм:

Текст открытого ключа

Дополнительные поля открытого ключа (сертификата):

Имя владельца ключа: Дополнительная информация о владельце ключа: Код страны: Страна: Город: Организация: Подразделение в организации: E-mail:

Приложение 3

к Регламенту электронного документооборота

Заявление на отзыв сертификата

Прошу отозвать Сертификат ключа подписи, в связи:
_____.

(указать причину)

Отзываемый сертификат содержит следующие данные:
Серийный номер:
Фамилия, Имя, Отчество:
E-mail:

«___»_____20__г.

Уполномоченное лицо/Пользователь/Руководитель Участника

_____ _____

(Фамилия И.О. Уполномоченного лица/Пользователь/ Руководителя Участника) (Подпись)

Приложение 4к Регламенту электронного документооборота

Акт о технологической готовности
(к Заявке на интеграцию)___

г. Москва «___»_____20__г.

Общество с ограниченной ответственностью «ХЕЛЛО» (ООО «ХЕЛЛО»), именуемое вдальнейшем «ХЕЛЛО», в лице Генерального директора_____, действующего на основании Устава, с одной стороны, и _____, именуемое в дальнейшем «Участник», в лице_____, действующего на основании_____, с другой стороны, вместе именуемые Стороны, составили Акт о нижеследующем:

- 1. Утверждены электронные адреса Сторон для взаимообмена электронными документами во исполнение обязательств по Договору Участника:
  - ХЕЛЛО: **edo@_____.___**;
  - Участник:_____;
- 2. Стороны подтверждают, что все работы по внедрению услуги выполнены в полном объеме, в том числе:
- 2.1. Работы по интеграции программного обеспечения для осуществления деятельности Участника в _____, выполнены
  - (тип пункта обслуживания: касса, терминал, банкомат, интернет-банк и т.д.)
-
- согласно Протоколу взаимодействия внешних систем с ХЕЛЛО версии _____.
- 2.2. Тестовые работы выполнены согласно требованиям Протокола взаимодействия внешних систем с ХЕЛЛО версии_____и Методики тестирования Системы.
- 2.3. Пункты обслуживания Участника зарегистрированы в соответствующем формате. Участником получены идентификаторы Пунктов обслуживания и авторизованный доступ к работе в Системе.

3. Стороны претензий друг к другу не имеют и технологически полностью готовы к исполнению обязательств по Договору.
4. Участник подтверждает, что с «_____»_____20__г. готов приступить к работе с Платежной системой «ХЕЛЛО».

Дополнительно: _____
(замечания: есть /нет)

От ООО «ХЕЛЛО»: Генеральный директор	От Участника: Руководитель
_____/_____/ М.П.	_____/_____/ М.П.

Приложение 5
к Регламенту электронного документооборота

на фирменном бланке организации

ООО «ХЕЛЛО»
_____

Заявка на интеграцию
с ИТ-платформой Платежной системы «ХЕЛЛО»
№_____от_____

_____
(версия платформы)

Просим рассмотреть возможность интеграции систем взаимообмена:

Участник: _____
(полное наименование организации)

Договор_____№_____от «___»_____20___г.
(наименование договора)

Интеграция с:

_____
(название системы учета Участника)

Отметить поле:
- ☐ собственная разработка;
- ☐ сторонний поставщик (3 лицо)

Компания-поставщик (3 лицо):

_____
(полное наименование стороннего поставщика)

Ответственные лица от Участника:

	Контакты
1	Куратор/менеджер, ФИО *E-mail* *Контактный телефон*
2	Специалист по информационным технологиям – специалист, ФИО E-mail Контактный телефон

При распределении ответственности по участкам, укажите данные сотрудников по информационным технологиям дополнительно:

Специалист по
информационным
технологиям – специалист,
ФИО
E-mail
Контактный телефон

Ответственные лица от Поставщика (3 лицо):

	Контакты
1	Куратор/менеджер, ФИО E-Mail Контактный телефон
2	IT – специалист, ФИО E-Mail Контактный телефон

При распределении ответственности по участкам, укажите данные сотрудников по информационным технологиям дополнительно:

Специалист по
информационным
технологиям – специалист,
ФИО
E-Mail
Контактный телефон

Проектные сроки запуска услуг переводов и платежей в сети Участника:

_____

Отметить поле:

- ☐ Расходы по интеграции на стороне Участника;
- ☐ Расходы по интеграции с участием Платежной системы «ХЕЛЛО»:

_____

(проектная сумма затрат, руб.)

От Участника:
Руководитель
_____/_____/
М.П.

Приложение 6
к Регламенту электронного документооборота

Отчет об инцидентах

Дата выявления инцидента	Дата устранения инцидента	Описание инцидента	Принятые меры по устранению и предупреждению	Обращение в правоохранительные органы

«___»_____20___г.

Уполномоченное лицо/Пользователь/Руководитель Участника

_____ _____

(Фамилия ИО Уполномоченного лица/ Руководителя Участника) (Подпись)

Приложение №3
к Правилам Платежной системы
«ХЕЛЛО»

ПЕРЕЧЕНЬ ДОКУМЕНТОВ,
предоставляемых Участниками Оператору
Платежной системы «ХЕЛЛО»

I. Перечень документов, предоставляемых Участниками – резидентами Российской Федерации:

ОРИГИНАЛЫ, НОТАРИАЛЬНО ЗАВЕРЕННЫЕ ИЛИ ЗАВЕРЕННЫЕ КОМПЕТЕНТНЫМ ОРГАНОМ, ЗАРЕГИСТРИРОВАВШИМ И/ИЛИ ВЫДАВШИМ ДОКУМЕНТ:
▪ Устав (Положение) со всеми изменениями и дополнениями ▪ Свидетельства о государственной регистрации изменений, вносимых в учредительные документы юридического лица ко всем изменениям в учредительные документы ▪ Лицензии (разрешения), выданные юридическому лицу в установленном законодательством Российской Федерации порядке, предоставляющие право осуществления деятельности, подлежащей лицензированию в соответствии с законодательством Российской Федерации. ▪ Свидетельство о государственной регистрации: - Свидетельство о государственной регистрации юридических лиц, зарегистрированных до 01.07.2002 г. и Свидетельство о внесении записи в Единый государственный реестр юридических лиц о юридическом лице, зарегистрированном до 01.07.2002г. - Свидетельство о государственной регистрации юридических лиц, зарегистрированных после 01.07.2002г. ▪ Свидетельство о постановке на учет в налоговом органе
ОРИГИНАЛЫ ДОКУМЕНТОВ/КОПИИ, ЗАВЕРЕННЫЕ ПЕЧАТЬЮ ЮРИДИЧЕСКОГО ЛИЦА И ПОДПИСЬЮ УПОЛНОМОЧЕННОГО ДОЛЖНОСТНОГО ЛИЦА

- Протокол (решение) участников, акционеров (участника, акционера) об избрании руководителя.
- Приказы о назначении на должность (вступлении в должность), доверенности, подтверждающие полномочия лиц, подписывающих документы, представляемые Оператору.

Также Оператор вправе запросить, а юридическое лицо обязан предоставить следующие документы:

- карточку с образцами подписей/альбом с подписями
- годовой отчет за истекший отчетный год
- бухгалтерский баланс и отчет о прибылях и убытках

II. <u>Перечень документов, предоставляемых Участниками – нерезидентами Российской Федерации:</u>

ОРИГИНАЛЫ, НОТАРИАЛЬНО ЗАВЕРЕННЫЕ ИЛИ ЗАВЕРЕННЫЕ УПОЛНОМОЧЕННЫМ ОРГАНОМ, ЗАРЕГИСТРИРОВАВШИМ И/ИЛИ ВЫДАВШИМ ДОКУМЕНТ:
▪ Устав (Положение) со всеми изменениями и дополнениями ▪ Свидетельства о государственной регистрации изменений, вносимых в учредительные документы юридического лица ко всем изменениям в учредительные документы ▪ Лицензии (разрешения), выданные юридическому лицу в установленном законодательством Российской Федерации порядке, предоставляющие право осуществления деятельности, подлежащей лицензированию в соответствии с законодательством Российской Федерации. ▪ Свидетельство о государственной регистрации: - Свидетельство о государственной регистрации юридических лиц, зарегистрированных до 01.07.2002 г. и Свидетельство о внесении записи в Единый государственный реестр юридических лиц о юридическом лице, зарегистрированном до 01.07.2002г. - Свидетельство о государственной регистрации юридических лиц, зарегистрированных после 01.07.2002г. ▪ Свидетельство о постановке на учет в налоговом органе
ОРИГИНАЛЫ ДОКУМЕНТОВ/КОПИИ, ЗАВЕРЕННЫЕ ПЕЧАТЬЮ ЮРИДИЧЕСКОГО ЛИЦА И ПОДПИСЬЮ УПОЛНОМОЧЕННОГО ДОЛЖНОСТНОГО ЛИЦА
▪ Протокол (решение) участников, акционеров (участника, акционера) об избрании руководителя. ▪ Приказы о назначении на должность (вступлении в должность), доверенности, подтверждающие полномочия лиц, подписывающих документы, представляемые Оператору. <u>Также Оператор вправе запросить, а юридическое лицо обязано предоставить следующие документы:</u> ▪ карточку с образцами подписей/альбом с подписями ▪ годовой отчет за истекший отчетный год ▪ бухгалтерский баланс и отчет о прибылях и убытках

Настоящий перечень входит в состав Правил Платежной системы «ХЕЛЛО».

Приложение №4
к Правилам Платежной системы
«ХЕЛЛО»

ФОРМА
ДОГОВОР УЧАСТИЯ №_____
в Платежной системе «ХЕЛЛО»
(для прямого Участника)

г. Москва «___»_____20___г.

Общество с ограниченной ответственностью «ХЕЛЛО», именуемое в дальнейшем «Оператор Системы», в лице_____, действующего на основании_____, с одной стороны, и_____, именуемый в дальнейшем «Участник», в лице действующего на основании, с другой стороны, совместно в дальнейшем именуемые «Стороны», а по отдельности - «Сторона», заключили настоящий договор (далее – «Договор») о нижеследующем:

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

Термины в тексте настоящего Договора имеют значение, изложенное в Правилах Платежной системы «ХЕЛЛО».

2. ПРЕДМЕТ ДОГОВОРА.

2.1. Участник присоединяется к Правилам Платежной системы «ХЕЛЛО» (далее – «Правила») путем принятия их в целом и на условиях, приведенных в Правилах.
2.2. Оператор Платежной системы «ХЕЛЛО» (далее – «Система») уполномочивает Участникапредоставлять клиентам Услуги Платежной системы «ХЕЛЛО».
2.3. Правила Системы публикуются на официальном сайте Оператора в сети интернет по адресу www.hellopay.online

3. ОБЩИЕ ПОЛОЖЕНИЯ.

3.1. Права и обязанности Сторон:
3.1.1. Оператор обязан обеспечить Участнику возможность предоставления клиентам Услуг Платежной системы «ХЕЛЛО» на условиях Правил Системы посредством:
- регистрации Участника в Системе и информирования других Участников о данном включении;
- обеспечения технологического и информационного обслуживания Участника.
3.1.2. Оператор обязан информировать Участника об изменении Правил, публикуя новую редакцию на официальном сайте Системы в сети интернет в порядке и сроки, указанные в Правилах Системы.
3.1.3. Оператор вправе вносить изменения в Правила и контролировать выполнение Правил Системы Участниками.
3.1.4. Оператор вправе без предварительного уведомления Участника временно приостановить по собственной инициативе полностью или частично работу Участника в Системе в случаях неисполнения им своих обязательств в рамках настоящего Договора, а также в случае нарушения положений Правил. О данном факте Оператор Системы незамедлительно уведомляет Участника по согласованному каналу связи.
3.1.5. Участник обязуется открыть счет в Расчетном центре Системы.
3.1.6. Участник обязуется самостоятельно организовать и поддерживать финансовое, техническое и технологическое обеспечение предоставления Услуг ПС «ХЕЛЛО».

3.1.7. Участник обязуется предоставлять Услуги системы «ХЕЛЛО» в полном соответствии с Правилами.
3.2. Порядок расчетов регламентируется Правилами Системы.
3.3. За предоставление Услуг Платежной системы «ХЕЛЛО» Участник получает комиссию в размере, указанном в Тарифах Системы.

4. КОНФИДЕНЦИАЛЬНОСТЬ.

4.1. Стороны обязуются сохранять конфиденциальность данных, получаемых при работе в Системе, в т.ч. и персональных данных, и предоставлять доступ к информации третьим лицам только с согласия владельца информации, за исключением случаев, когда предоставление информации осуществляется в соответствии с требованиями законодательства страны местонахождения Участника или условиями, изложенными в Правилах Системы**.**
4.2. Участники, соглашаются с тем, что осуществляемая Оператором Системы деятельность по сбору и хранению информации, необходимой для функционирования Системы, не нарушает условий конфиденциальности.
4.3. В случае расторжения настоящего Договора участия в Платежной системе «ХЕЛЛО» Стороны обязаны соблюдать требования о конфиденциальности информации и сведений, полученных ими в период срока его действия, в течение пяти лет с даты его расторжения (окончание срока действия, признания недействительным).

5. ДЕЙСТВИЕ ДОГОВОРА И ПОРЯДОК ЕГО ПРЕКРАЩЕНИЯ И ИЗМЕНЕНИЯ.

5.1. Договор вступает в силу с даты его подписания обеими Сторонами и действует в течение неопределенного периода времени, до его расторжения по соглашению Сторон, или отказа одной из Сторон от его исполнения, либо до момента прекращения настоящего Договора по иным основаниям. Договор считается заключенным с момента его подписания обеими Сторонами.
5.2. Настоящий Договор может быть изменен и/или дополнен по взаимному согласию Сторон, путем подписания дополнительного соглашения.
5.3. Настоящий Договор составлен в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.
5.4. Договор может быть расторгнут по соглашению Сторон, или по инициативе одной из Сторон при условии полного урегулирования всех финансовых и иных обязательств до даты расторжения настоящего Договора. О намерении расторгнуть настоящий Договор заинтересованная Сторона обязана предупредить другую Сторону не менее чем за 30 (Тридцать) календарных дней до даты предполагаемого расторжения, и полностью урегулировать финансовые обязательства. Предупреждение о намерении расторгнуть настоящий Договор направляется заинтересованной Стороной в письменном виде за подписью уполномоченного лица, по адресам, Сторон, указанным в разделе 6 настоящего Договора.

6. АДРЕСА, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН.

Настоящий договор входит в состав Правил Платежной системы «ХЕЛЛО».

Приложение №5
к Правилам Платежной системы
«ХЕЛЛО»

ФОРМА
ДОГОВОР УЧАСТИЯ №_____
в Платежной системе «ХЕЛЛО»
(для косвенного Участника)

г. Москва «___»_____20___г.

Общество с ограниченной ответственностью «ХЕЛЛО», именуемое в дальнейшем «Оператор Системы», в лице_____, действующего на основании_____, с одной стороны, и_____, именуемый в дальнейшем «Участник», в лице действующего на основании, с другой стороны, совместно в дальнейшем именуемые «Стороны», а по отдельности - «Сторона», заключили настоящий договор (далее – «Договор») о нижеследующем:

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

Термины в тексте настоящего Договора имеют значение, изложенное в Правилах Платежной системы «ХЕЛЛО».

2. ПРЕДМЕТ ДОГОВОРА.

2.1. Участник присоединяется к Правилам Платежной системы «ХЕЛЛО» (далее – «Правила») путем принятия их в целом и на условиях, приведенных в Правилах.
2.2. Оператор Платежной системы «ХЕЛЛО» (далее – «Система») уполномочивает Участникапредоставлять клиентам Услуги Платежной системы «ХЕЛЛО».
2.3. Правила Системы публикуются на официальном сайте Оператора в сети интернет по адресу www.hellopay.online

3. ОБЩИЕ ПОЛОЖЕНИЯ.

3.1. Права и обязанности Сторон:
3.1.1. Оператор обязан обеспечить Участнику возможность предоставления клиентам Услуг Платежной системы «ХЕЛЛО» на условиях Правил Системы посредством:
- регистрации Участника в Системе и информирования других Участников о данном включении;
- обеспечения технологического и информационного обслуживания Участника.
3.1.2. Оператор обязан информировать Участника об изменении Правил, публикуя новую редакцию на официальном сайте Системы в сети интернет в порядке и сроки, указанные в Правилах Системы.
3.1.3. Оператор вправе вносить изменения в Правила и контролировать выполнение Правил Системы Участниками.
3.1.4. Оператор вправе без предварительного уведомления Участника временно приостановить по собственной инициативе полностью или частично работу Участника в Системе в случаях неисполнения им своих обязательств в рамках настоящего Договора, а также в случае нарушения положений Правил. О данном факте Оператор Системы незамедлительно уведомляет Участника по согласованному каналу связи.
3.1.5. Участник обязуется открыть счет у Прямого Участника Системы.
3.1.6. Участник обязуется самостоятельно организовать и поддерживать финансовое, техническое и технологическое обеспечение предоставления Услуг ПС «ХЕЛЛО».

3.1.7. Участник обязуется предоставлять Услуги Платежной системы «ХЕЛЛО» в полном соответствии сПравилами.
3.2. Порядок расчетов регламентируется Правилами Системы.
3.3. За предоставление Услуг Платежной системы «ХЕЛЛО» Участник получает комиссию в размере,указанном в Тарифах Системы.

4. КОНФИДЕНЦИАЛЬНОСТЬ.

4.1. Стороны обязуются сохранять конфиденциальность данных, получаемых при работе в Системе, в т.ч. и персональных данных, и предоставлять доступ к информации третьим лицам только с согласия владельца информации, за исключением случаев, когда предоставление информации осуществляется в соответствии с требованиями законодательства страны местонахождения Участника или условиями, изложенными в Правилах Системы**.**
4.2. Участники, соглашаются с тем, что осуществляемая Оператором Системы деятельность по сбору и хранению информации, необходимой для функционирования Системы, не нарушает условий конфиденциальности.
4.3. В случае расторжения настоящего Договора участия в Платежной системе «ХЕЛЛО» Стороны обязаны соблюдать требования о конфиденциальности информации и сведений, полученных ими в период срока его действия, в течение пяти лет с даты его расторжения (окончание срока действия, признания недействительным).

5. ДЕЙСТВИЕ ДОГОВОРА И ПОРЯДОК ЕГО ПРЕКРАЩЕНИЯ И ИЗМЕНЕНИЯ.

5.1. Договор вступает в силу с даты его подписания обеими Сторонами и действует в течение неопределенного периода времени, до его расторжения по соглашению Сторон, или отказа одной из Сторон от его исполнения, либо до момента прекращения настоящего Договора по иным основаниям. Договор считается заключенным с момента его подписания обеими Сторонами.
5.2. Настоящий Договор может быть изменен и/или дополнен по взаимному согласию Сторон, путем подписания дополнительного соглашения.
5.3. Настоящий Договор составлен в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.
5.4. Договор может быть расторгнут по соглашению Сторон, или по инициативе одной из Сторон при условии полного урегулирования всех финансовых и иных обязательств до даты расторжения настоящего Договора. О намерении расторгнуть настоящий Договор заинтересованная Сторона обязана предупредить другую Сторону не менее чем за 30 (Тридцать) календарных дней до даты предполагаемого расторжения, и полностью урегулировать финансовые обязательства. Предупреждение о намерении расторгнуть настоящий Договор направляется заинтересованной Стороной в письменном виде за подписью уполномоченного лица, по адресам, Сторон, указанным в разделе 6 настоящего Договора.

6. АДРЕСА, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН.

Настоящий договор входит в состав Правил Платежной системы «ХЕЛЛО».

Приложение №6
к Правилам Платежной системы «ХЕЛЛО»

Протокол внесения изменений в Правила Платежной системы «ХЕЛЛО»

Дата вступления в силу	Номер редакции Правил	Описание

Настоящий Протокол входит в состав Правил Платежной системы «ХЕЛЛО»

Приложение № 7 к
Правилам Платежной системы «ХЕЛЛО»

Положение по управлению рисками и обеспечению бесперебойности функционирования Платежной системы «ХЕЛЛО»

Оглавление

1. Общие положения
2. Термины и сокращения
3. Общие принципы построения процесса управления рисками ПС. Показатели БФПС
4. Классификация рисков Платежной системы
5. Порядок управления рисками нарушений БФПС
6. Организационная модель взаимодействия субъектов ПС при осуществлении деятельности по обеспечению БФПС. Управление непрерывностью функционирования Платежной системы
7. Требования к содержанию деятельности по обеспечению БФПС
8. Разграничение ответственности и полномочий между Участниками Платежной системы по осуществлению процесса управления рисками нарушения бесперебойности функционирования Платежной системы «ХЕЛЛО»
9. Порядок взаимодействия Субъектов ПС по обеспечению БФПС
10. Требования к планам обеспечения непрерывности деятельности и восстановления деятельности
11. Организационная модель взаимодействия Участников Платежной системы «ХЕЛЛО» при осуществлении деятельности по обеспечению бесперебойности функционирования Платежной системы «ХЕЛЛО»
12. Контроль за соблюдением Операторами услуг платежной инфраструктуры и Участниками Платежной системы порядка обеспечения БФПС
13. Требования к методикам анализа рисков в Платежной системе, включая профили рисков
14. Заключительные положения

Приложение № 1. Методика оценки рисков в Платежной системе «ХЕЛЛО»
Приложение № 2. Методы управления рисками в Платежной системе «ХЕЛЛО»
Приложение № 3. Самооценка эффективности СУР Платёжной системы «ХЕЛЛО»
Приложение № 4. План обеспечения непрерывности деятельности и восстановления деятельности
Приложение № 5. Методика оценки рисков Участников ПС (кредитные организации)
Приложение № 6. Перечень регламентных работ, проводимых в ОЦ, по обеспечению бесперебойности функционирования ПС «ХЕЛЛО»
Приложение № 7. Порядок информационного взаимодействия внутри Операционного центра Платежной системы «ХЕЛЛО»
Приложение № 8. Порядок определения показателей БФПС
Приложение № 9. Пороговые уровни показателей БФПС Платежной системы «ХЕЛЛО»
Приложение № 10. Бизнес-процессы Платежной системы «ХЕЛЛО»
Приложение № 11. Профиль риска
Приложение № 12. Профиль риска нарушения БФПС

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение по управлению рисками и обеспечению бесперебойности функционирования Платежной системы «ХЕЛЛО» (далее – Положение по БФПС) разработано в соответствии с Федеральным законом от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (далее – Закон о НПС), Федеральным законом от 02 декабря 1990 года № 395-1-ФЗ «О банках и банковской деятельности», Письмом Банка России от 3 мая 2011 года № 67-Т «О системном риске расчетной системы», Положением Банка России от 03 октября 2017 года № 607-П «О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков» (далее – Положение Банка России № 607-П), Положением Банка России от 04 июня 2020 года № 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), Указанием Банка России от 11 июня 2014 года № 3280-У «О порядке информирования оператором платежной системы Банка России, участников платежной системы о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры» (далее - Указание Банка России № 3280-У), Указанием Банка России от 09 июня 2012 года № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств», а также в соответствии с требованиями, установленными Правилами Платежной системы «ХЕЛЛО».

1.2. Положение по БФПС устанавливает требования к порядку обеспечения бесперебойности функционирования Платежной системы «ХЕЛЛО», показателям бесперебойности функционирования ПС и методикам анализа рисков в Платежной системе «ХЕЛЛО», включая профили рисков.

1.3. Требования Положения по БФПС применяются к Оператору Платежной системы «ХЕЛЛО» при обеспечении бесперебойности функционирования платежной системы, которая достигается при условии оказания Участникам Платежной системы «ХЕЛЛО» услуг платежной инфраструктуры согласно требованиям Закона о НПС и принятых в соответствии сним нормативных актов Банка России, а также положениям Правил Платежной системы «ХЕЛЛО», договоров об оказании УПИ, документов Оператора Платежной системы «ХЕЛЛО» и привлеченных им Операторов УПИ и (или) восстановленияоказания УПИ, соответствующего требованиям к оказанию услуг, и восстановления оказания УПИ в случае приостановления их оказания в течение периодов времени, установленных Оператором ПС в Правилах Платежной системы «ХЕЛЛО».

1.4. Под системой управления рисками в Платежной системе «ХЕЛЛО» понимается комплекс мероприятий и способов снижения вероятности возникновения неблагоприятных последствий для бесперебойности функционирования Платежной системы «ХЕЛЛО» с учетом размера причиняемого ущерба.

1.5. Оператор ПС обеспечивает БФПС путем осуществления скоординированной с Операторами УПИ и Участниками ПС «ХЕЛЛО» деятельности:

- по управлению рисками в Платежной системе «ХЕЛЛО»;
- по управлению непрерывностью функционирования Платежной системы «ХЕЛЛО».

1.6. Порядок обеспечения БФПС определен в Правилах Платежной системы «ХЕЛЛО»,а также в разработанных в соответствии с ними документах Оператора ПС и в документах привлеченных Операторов УПИ.

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

- управление рисками в Платежной системе;
- управление непрерывностью функционирования Платежной системы;

- организацию взаимодействия Субъектов ПС по обеспечению БФПС;
- контроль за соблюдением Операторами УПИ и Участниками ПС Порядка обеспечения БФПС.
-

2. ТЕРМИНЫ И СОКРАЩЕНИЯ

ПС – Платежная система «ХЕЛЛО».

Правила ПС - Правила Платежной системы «ХЕЛЛО».

БФПС - бесперебойность функционирования ПС.

Инцидент - событие, которое привело к нарушению оказания УПИ, соответствующего требованиям к оказанию услуг, в том числе вследствие нарушений требований к обеспечению защиты информации при осуществлении переводов денежных средств.

Оператор ПС - Общество с ограниченной ответственностью «ХЕЛЛО».

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

Операционный центр (ОЦ) – Общество с ограниченной ответственностью «ХЕЛЛО», обеспечивающее в рамках платежной 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, содержащих распоряжения Участников платежной системы (далее - операционные услуги).

Платежный клиринговый центр (ПКЦ) – Общество с ограниченной ответственностью «ХЕЛЛО», созданное в соответствии с законодательством Российской Федерации, обеспечивающее в рамках Платежной системы прием к исполнению распоряжений Участников Платежной системы об осуществлении перевода денежныхсредств и выполнение иных действий, предусмотренных Законом о НПС (далее – услуги платежного клиринга).

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

Субъекты ПС - Оператор ПС, Операторы услуг платежной инфраструктуры и Участники ПС.

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

Управление непрерывностью функционирования ПС – выявление оказания услуг платежной инфраструктуры, не соответствующих требованиям к оказанию услуг, обеспечению функционирования Платежной системы «ХЕЛЛО» 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 ПС в Правилах Платежной системы «ХЕЛЛО».

Управление рисками в платежной системе - организация СУР в ПС, оценке и управлению рисками в ПС.

Участники ПС – операторы по переводу денежных средств – кредитные организации.

СУР — система управления рисками.

3. ОБЩИЕ ПРИНЦИПЫ ПОСТРОЕНИЯ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ ПС. ПОКАЗАТЕЛИ БФПС.

3.1. Общие принципы построения процесса управления рисками ПС определены Правилами Платежной системы «ХЕЛЛО». Оператор ПС управляет рисками в ПС с учетом следующих требований.

3.1.1. Оператор ПС организует систему управления рисками в ПС с учетом организационной модели управления рисками в платежной системе, определенной в соответствии с требованиями Закона о НПС и Правил ПС.

3.1.2. Оператор ПС проводит оценку рисков в ПС «ХЕЛЛО» не реже одного раза в год с использованием методик анализа рисков в ПС, включая профили рисков (Приложение № 11 к настоящему Положению БФПС), требования к которым определены в настоящем Положении о БФПС.

3.1.3. В Правилах ПС Оператор ПС определяет способы управления рисками в ПС «ХЕЛЛО».

3.1.4. Оператор ПС в соответствии с требованиями, указанными в нормативных документах Банка России, определяет следующие показатели БФПС:

Показатель 1 (П1) - показатель продолжительности восстановления оказания услуг платежной инфраструктуры, характеризующий период времени восстановления оказания услуг Операторами услуг платежной инфраструктуры, в случае приостановления оказания услуг платежной инфраструктуры, в том числе вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России № 719-П;

Показатель 2 (П2) - показатель непрерывности оказания услуг платежной инфраструктуры, характеризующий период времени между двумя последовательно произошедшими в ПС инцидентами, в результате которых приостанавливалось оказание услуг платежной инфраструктуры;

Показатель 3 (П3) - показатель соблюдения регламента, характеризующий соблюдение Операторами услуг платежной инфраструктуры, времени начала, времени окончания, продолжительности и последовательности процедур, выполняемых Операторами услуг платежной инфраструктуры, при оказании операционных услуг, услуг платежногоклиринга и расчетных услуг;

Показатель 4 (П4) - показатель доступности Операционного центра ПС, характеризующий оказание операционных услуг ОЦ ПС «ХЕЛЛО»;

Показатель 5 (П5) - показатель изменения частоты инцидентов, характеризующий темп прироста частоты инцидентов.

Порядок определения показателей БФПС указан в Приложении № 8 к настоящему Положению по БФПС.

3.1.5. Оператор ПС устанавливает и пересматривает с использованием результатов оценки рисков в ПС «ХЕЛЛО» пороговые уровни показателей БФПС. Установленные Оператором ПС пороговые уровни показателей БФПС раскрыты в Приложении № 9 к настоящему Положению о БФПС.

3.1.6. Оператор ПС рассчитывает и анализирует значения показателей БФПС, в том числе путем их сравнения с пороговыми уровнями показателей БФПС, и использует результаты указанного анализа при оценке системы управления рисками в ПС «ХЕЛЛО» и при оценке влияния инцидентов на БФПС.

3.1.7. Оператор ПС проводит оценку СУР в ПС «ХЕЛЛО», в том числе используемых методов оценки рисков в ПС «ХЕЛЛО», результатов применения способов управления рисками в ПС, не реже одного раза в два года и документально оформляет результаты указанной оценки.

Оценка СУР в ПС проводится Комитетом по управлению рисками ПС «ХЕЛЛО» методом экспертных оценок.

3.1.8. Оператор ПС вносит изменения в СУР ПС «ХЕЛЛО» в случае, если действующая

СУР в ПС не позволила предотвратить нарушение оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, а также восстановить оказание услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, в течение 24 часов и (или) восстановить оказание услуг платежной инфраструктуры в случае приостановления их оказания в течение 6 часов.

3.2. В целях снижения уровня рисков ПС процесс управления рисками направлен на предупреждение нарушений бесперебойного функционирования ПС и организацию оперативного устранения нарушений функционирования ПС. Для реализации указанной цели Оператор ПС организует процесс управления рисками, включающий следующие процедуры:

- выявление факторов риска;
- анализ рисков;
- определение степени и характера влияния указанных факторов на ПС;
- оценка присущего уровня рисков[1];
- принятие мер, направленных на минимизацию риска и поддержание допустимого уровня рисков;
- мониторинг рисков (выявление текущих изменений присущего уровня риска);
- информационное взаимодействие Участников ПС в целях управления рисками.

[1] Размер возможного ущерба, причиняемого Участникам ПС, их клиентам вследствие нарушений надлежащего функционирования ПС, с учетом вероятности возникновения указанных нарушений в течение прогнозируемого периода времени.

4. КЛАССИФИКАЦИЯ РИСКОВ ПС.

Основными рисками, которые могут привести к нарушению БФПС, принимаются риски:

- расчетный (кредитный + ликвидности);
- операционный, в том числе риск информационной безопасности;
- правовой;
- общий коммерческий риск;
- системный риск.

4.1. **Расчетный риск:** кредитный риск и риск ликвидности – риски ПС, обусловленные влиянием на БФПС финансового состояния Участников ПС. Расчетный риск включает:

- Кредитный риск – это риск оказания УПИ, не соответствующего требованиям к оказанию услуг, центральным платежным клиринговым контрагентом или расчетным центром ПС вследствие невыполнения Участниками ПС договорных обязательств перед указанными организациями в установленный срок или в будущем;
- Риск ликвидности – это риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие отсутствия у центрального платежного клирингового контрагента и (или) у Участников ПС денежных средств, достаточных для своевременного выполнения их обязательств перед другими Субъектами ПС.

Вероятность наступления расчетного риска	- минимальная

Оценка вероятности наступления расчетного риска на минимальном уровне обусловлена тем, что Участники ПС имеют возможность совершать операции в ПС тольков пределах остатка денежных средств на банковских счетах, открытых в РЦ.

Общие принципы управления расчетным риском состоят в контроле соблюдения Оператором ПС следующих процедур:

- выполнение Участниками ПС требований по финансовому обеспечению расчетов в ПС, контроля Оператором ПС лимитов авторизации участников ПС;
- выполнение Оператором ПС мониторинга объемов операций между Участниками ПС, оперативный контроль резкого роста объемов операций того или иного Участника ПС;
- возможность блокирования в случае угрозы возникновения риска Оператором ПС операций между Участниками ПС.

Все операции по переводу денежных средств в ПС осуществляются только при обязательном соблюдении следующих условий: сумма авторизованного запроса не превышает сумму расходного лимита, установленного Расчетным центром на Участника ПС.

Операционный риск - это риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие возникновения у Субъектов ПС 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 ПС либо вследствие воздействия событий, причины возникновения которых не связаны с деятельностью Субъектов, включая чрезвычайные ситуации, ошибочные или противоправные действия третьих лиц.

Риск информационной безопасности (как один из видов операционного риска) - это потенциальная возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации. Возникает вследствие недостатков процессов обеспечения защиты информации, в том числе недостатков применяемых технологических мер защиты информации, недостатков прикладного программного обеспечения автоматизированных систем и приложений, а также несоблюдения требований к указанным процессам деятельности

Участниками, операторами УПИ.

Операционный риск обусловлен влиянием на ПС операционных факторов в части неисправностей технологического обеспечения или возникшими операционными ошибками.

Оценка вероятности наступления операционного риска обусловлена многообразием факторов и источников данного вида риска:

- случайные или преднамеренные действия физических и (или) юридических лиц, направленные против интересов ПС;
- несовершенство организационной структуры Участников ПС в части распределения полномочий подразделений и сотрудников, порядков и процедур совершения операций в рамках ПС, их документирования и отражения в учете;
- несоблюдение сотрудниками Участников ПС установленных порядков и процедур, неэффективность внутреннего контроля;
- сбои в функционировании информационных систем и оборудования; неблагоприятные внешние обстоятельства, находящиеся вне контроля Участников ПС.

Вероятность наступления операционного риска для ПС	– средняя

Общие принципы управления операционным риском состоят в применении ОператоромПС, Операторами услуг платежной инфраструктуры и Участниками ПС следующих мер:

- регламентирование порядка выполнения основных процессов в Правилах и внутренних документах;
- регламентирование порядка совершения операций в рамках внутренних нормативно-методологических документах;
- учет и контроль совершаемых операций, регулярные выверки расчетных документов по операциям;
- применение принципов разделения и ограничения функций в целях определения предела полномочий сотрудников, осуществляющих операции;
- использование механизмов усиления контроля за совершением операций, установление ограничений на сроки и объемы операций;
- реализация процедур административного и финансового внутреннего контроля (предварительного, текущего и последующего) за организацией бизнес-процессов, деятельностью Участников ПС и совершением операций сотрудниками, соблюдением установленных лимитов по проводимым операциям;
- обеспечение информационной безопасности, контроль над доступом к информации, применение многоуровневой защиты информации с использованием сертифицированных средств защиты информации, а также с аттестацией объектов информатизации ПС по требованиям информационной безопасности;
- создание необходимых организационных и технических условий для обеспечения БФПС при совершении операций (на случай аварий, пожаров, терактов и других непредвиденных ситуаций);
- обеспечение работоспособности аппаратно-программных комплексов всех Участников ПС, в том числе:
  - ✓ разработка технических требований на создание, внедрение и эксплуатацию аппаратно-программных комплексов с учетом требований к показателям бесперебойности;
  - ✓ тестирование аппаратно-программных комплексов перед их внедрением;
  - ✓ регулярный мониторинг системного, прикладного программного обеспечения и доступа к информационным ресурсам;
  - ✓ обеспечение целостности информационных активов;
  - ✓ обеспечение резервирования критичных информационных активов;

- ✓ разработка, поддержание в актуальном состоянии планов обеспечения непрерывности деятельности и восстановления деятельности после сбоев;
- ✓ проведение регулярной оценки качества и надежности функционирования информационных систем, операционных и технологических средств, соответствие их отраслевым нормативным актам;
- ✓ проведение регламентных работ.

- снижение рисков, связанных с персоналом, методом установления критериев по его отбору и проведения предварительной проверки, реализации мероприятий по подготовке и обучению персонала, повышению его квалификации.

4.2. **Правовой риск –** это риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие несоблюдения Субъектами ПС требований законодательства Российской Федерации, Правил Платежной системы «ХЕЛЛО», договоров, заключенных между Субъектами ПС, документов Оператора и документов Операторов УПИ либо вследствие наличия правовых коллизий и (или) правовой неопределенности в законодательстве Российской Федерации, нормативных актах Банка России, Правилах Платежной системы «ХЕЛЛО» и договорах, заключенных между Субъектами ПС, а также вследствие нахождения Операторов УПИ и Участников ПС под юрисдикцией различных государств.

Оценка вероятности наступления правого риска обусловлена определением количества выявленных фактов в заданный временной интервал претензий правового характера к Субъектам Платежной системы со стороны:

- других Субъектов ПС;
- государственных органов власти;
- клиентов Участников ПС.

Вероятность наступления правового риска для ПС	– средняя

Система управления правовым риском состоят в применении Оператором ПС, Операторами услуг платежной инфраструктуры и другими Участниками ПС следующих способов минимизации данного вида рисков:

- предварительная проверка Оператором ПС потенциальных Участников ПС и Операторов услуг платежной инфраструктуры на обладание необходимой правоспособностью;
- периодическая, не реже одного раза в год, выборочная проверка Оператором ПС Участников и Операторов услуг платежной инфраструктуры на обладание необходимой правоспособностью путем запросов на предоставление необходимой информации об их деятельности и документов, в том числе внутренних документов и договоров.

4.3. **Общий коммерческий риск** – это риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие ухудшения финансового состояния Оператора и/или Операторов УПИ, не связанного с реализацией кредитного риска ПС и риска ликвидности ПС.

Общие принципы управления общим коммерческим риском состоят в применении Оператором ПС, Операторами услуг платежной инфраструктуры и Участниками ПС следующих мер:

- использование прогрессивных технологий;
- поддержание позитивной деловой репутации.

Вероятность наступления общего коммерческого риска для ПС	– минимальная

4.4. **Системный риск** – это риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие неспособности одного или нескольких Субъектов ПС исполнить принятые на себя обязательства или нарушений в самой ПС, который вызовет неспособность большинства или всех Субъектов ПС исполнить свои обязательства в срок. Таким образом, возникновение системного риска является следствием возникновения одного из рисков, приведенных в п.4.1 - п.4.4 настоящего Положения о БФПС.

Вероятность наступления системного риска для ПС	– минимальная

5. ПОРЯДОК УПРАВЛЕНИЯ РИСКАМИ НАРУШЕНИЙ БФПС.

5.1. В ПС установлены следующие уровни рисков нарушения БФПС с учетом влияния потенциального негативного эффекта (потерь):

Категория риска	**Допустимый уровень значения показателя**
Операционный риск	<=6
Расчетный риск	<=3
Правовой риск	<=9
Общий коммерческий риск	<=3
Системный риск	<=18

Допустимые уровни рисков нарушения БФПС могут быть изменены путем внесенияизменений в настоящее Положение на основе рекомендаций участников СУР.

5.2. В процессе функционирования Оператором ПС могут быть дополнительно выявлены иные риски и установлены иные показатели БФПС, к которым могут относиться:

- ✓ финансовое состояние Операторов услуг платежной инфраструктуры2;
- ✓ технологическое обеспечение Операторов услуг платежной инфраструктуры;
- ✓ зависимость от Платежных систем, с Операторами которых заключены договора (соглашения) о взаимодействии Платежных систем;
- ✓ зависимость от внешних поставщиков (провайдеров) услуг;
- ✓ возможность возникновения конфликта интересов Субъектов Платежной системы, связанных с деятельностью в рамках Платежной системы и связанных с иной деятельностью;

Для каждого нового устанавливаемого показателя БФПС определяется процедура и методика его формирования (порядок расчета) на основе первичной информации о функционировании ПС, а также допустимые уровни соответствующих рисков нарушения БФПС[3].

5.3. Анализ рисков нарушения БФПС включает в себя следующие этапы.

- Выявление факторов риска нарушения БФПС. В результате выявления фактора риска определяются неблагоприятные события, которые могут произойти в результате воздействия этого фактора, локализация (место проявления), форма проявления.

Категория риска	***Без риска***	***Низкий***	***Средний***	***Высокий***
Уровень риска (u)	0	1	2	3

- Определение степени и характера влияния указанных факторов на БФПС. Количественная оценка степени и характера влияния факторов риска на БФПС производится расчетом показателей БФПС (доступности - d), где d = (1 — t / T) с учетом особенностей значений показателей *t* (средняя длительность нарушений

работоспособности в течение заданного временного интервала) и *T (*продолжительность заданного временного интервала), характерных для каждого риска.

- Оценка присущего уровня рисков нарушения БФПС производится в соответствии с принятой классификацией с учетом попадания рассчитанного конкретного значения показателя БФПС (d) в заданный интервал, соответствующий уровню риска

Баллы (Б)	**Негативный эффект (Нэ)**
1	***Незначительный***
2	***Допустимый***
3	***Значительный***

Для учета последствий размера потенциального негативного эффекта (потерь) для Платежной системы вследствие наступления конкретного риска полученные значения уровней риска корректируются с учетом негативного эффекта.

- Подтверждение соответствия присущего уровня рисков нарушения БФПС установленному допустимому уровню осуществляется путем сопоставления значений уровней риска с допустимыми уровнями. Для удобства сопоставления используется таблица пункта 5.1.

5.4. Принятие мер, необходимых для достижения или поддержания допустимого уровня рисков нарушения БФПС.

В соответствии с основными рисками, которые могут привести к нарушению БФПС, применяются следующие меры.

5.4.1. Для поддержания допустимого уровня операционного риска:

- регламентирование порядка и времени выполнения основных операций;
- учет и регулярные сверки по операциям;
- контроль за деятельностью Участников ПС;
- контроль учета требований к показателям бесперебойности при разработке технических требований на создание, внедрение и эксплуатацию аппаратно-программных комплексов;
- регулярный мониторинг системного, прикладного программного обеспечения и доступа к информационным ресурсам;
- периодическая проверка обеспечения целостности информационных активов, средств идентификации и аутентификации, процедур протоколирования и аудита, криптографической защиты информации, резервного копирования и архивирования информационных ресурсов;
- проверка планов обеспечения непрерывности деятельности и восстановления деятельности после сбоев;
- проведение регулярной оценки качества и надежности функционирования информационных систем, операционных и технологических средств.
- обеспечение информационной безопасности;
- проверка подготовки и обучения персонала Субъектами ПС.

5.4.2. Для поддержания допустимого уровня расчетного (кредитного и риска ликвидности) риска:

- установление предельных размеров (лимитов) обязательств Участникам ПС с учетом уровня риска;
- установление ограничений на объемы операций;
- изучение финансового состояния Участника ПС;
- контроль выполнения ПКЦ и РЦ регламента осуществления платежного клиринга.

5.4.3. Для поддержания допустимого уровня правового риска:

- предварительная проверка потенциальных Участников ПС и Операторов услуг

платежной инфраструктуры на обладание необходимой правоспособностью;

- периодическая, не реже одного раза в год, выборочная проверка Участников Платежной системы и Операторов услуг платежной инфраструктуры на обладание необходимой правоспособностью путем запросов на предоставление необходимой информации об их деятельности и документов, в том числе внутренних документов и договоров.

5.4.4. Выявление текущих изменений присущего уровня риска нарушения БФПС (далее-мониторинг рисков нарушения БФПС);

- ежемесячный расчет показателей БФПС и уровней рисков;
- сравнение расчетных значений уровней рисков с допустимыми значениями и выявление текущих изменений уровней рисков;
- анализ динамики изменений уровней рисков;
- доведение до органов управления Оператора ПС информации о текущих изменениях уровней рисков нарушения БФПС;
- выработка рекомендаций по снижению уровней рисков и доведение их до Субъектов ПС.

---

[2] В целях минимизации рисков нарушения БФПС Оператор ПС проводит ежемесячный мониторинг оценки финансового состояния РЦ и Участников ПС (кредитные организации) (Приложение № 5).

[3] Подробное описание Методики оценки рисков нарушения БФПС изложено в Приложении № 1.

6. ОРГАНИЗАЦИОННАЯ МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ СУБЪЕКТОВ ПС ПРИОСУЩЕСТВЛЕНИИ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ БФПС. УПРАВЛЕНИЕ НЕПРЕРЫВНОСТЬЮ ФУНКЦИОНИРОВАНИЯ ПЛАТЕЖНОЙСИСТЕМЫ.

6.1. В ПС определена следующая организационная модель управления рисками: функции по оценке и управлению рисками распределяются между Оператором ПС, Операторами услуг платёжной инфраструктуры и Участниками ПС.

6.2. Оператор ПС управляет непрерывностью функционирования ПС «ХЕЛЛО» с учетом следующих требований.

6.2.1. Оператор ПС организует деятельность по управлению непрерывностью функционирования ПС, в том числе путем установления прав и обязанностей Субъектов ПС по управлению непрерывностью функционирования ПС в зависимости от организационной модели управления рисками в ПС «ХЕЛЛО».

6.2.2. Оператор ПС организует сбор и обработку сведений, в том числе от привлеченных Операторов услуг платежной инфраструктуры, используемых для расчета показателей БФПС, а также следующих сведений об инцидентах:

- время и дата возникновения инцидента (в случае невозможности установить время возникновения инцидента указывается время его выявления);
- краткое описание инцидента (характеристика произошедшего события и его последствия);
- наименование взаимосвязанных последовательных технологических процедур, выполняемых при оказании услуг платежной инфраструктуры (далее - бизнес-процесс), в ходе которых произошел инцидент (Приложение № 10 к настоящему Положению о БФПС);
- наименование бизнес-процесса, на который оказал влияние инцидент;
- наличие (отсутствие) факта приостановления (прекращения) оказания услуг платежной инфраструктуры в результате инцидента;
- влияние инцидента на БФПС, определяемое с учетом требований, предусмотренных настоящим Положением о БФПС;
- степень влияния инцидента на функционирование ПС в зависимости от количества Операторов услуг платежной инфраструктуры, и (или) количества и значимости Участников ПС, на которых оказал непосредственное влияние инцидент, и (или) количества и суммы неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных распоряжений Участников ПС, и иных факторов;
- время и дата восстановления оказания услуг платежной инфраструктуры в случае приостановления их оказания;
- мероприятия по устранению инцидента и его неблагоприятных последствий с указанием планируемой и фактической продолжительности проведения данных мероприятий;
- дата восстановления оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг;
- неблагоприятные последствия инцидента по Субъектам ПС, в том числе:
  - сумма денежных средств, уплаченных Оператором ПС и (или) взысканных с ОператораПС,
  - сумма денежных средств, уплаченных Оператором (Операторами) услуг платежной инфраструктуры и (или) взысканных с Оператора (Операторов) услуг платежной инфраструктуры,
  - количество и сумма неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных распоряжений Участников ПС, на исполнение которых оказал влияние инцидент,
  - продолжительность приостановления оказания услуг платежной инфраструктуры.

6.2.3. Оператор ПС обеспечивает хранение сведений по ПС и сведений об инцидентах не менее трех лет с даты получения указанных сведений.

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

6.2.5. Оператор ПС проводит оценку влияния на БФПС каждого произошедшего в ПС инцидента в течение 24 часов с момента его возникновения (выявления), а также в течение 24 часов после устранения инцидента (восстановления оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг).

В случае если вследствие произошедшего в ПС инцидента нарушен регламент выполнения процедур, но при этом не нарушен пороговый уровень каждого из показателейП1, П2, данный инцидент признается непосредственно не влияющим на БФПС.

Произошедший в ПС 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 ПС времени, в течение которого должно быть восстановлено оказание услуг платежной инфраструктуры, соответствующее требованиям к оказанию услуг.

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

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

В случае если вследствие произошедших в ПС в течение календарного месяца инцидентов не нарушен пороговый уровень показателя П4, рассчитанного по данным инцидентам, и одновременно нарушен пороговый уровень показателя П3 и (или) показателяП5, рассчитанных по этим же инцидентам, данные инциденты признаются непосредственно не влияющими на БФПС.

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

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

6.2.7. Оператор ПС установил в Правилах Платежной системы «ХЕЛЛО» период времени, в течение которого должно быть восстановлено оказание УПИ в случае приостановления их оказания (6 часов), и период времени, в течение которого должно быть восстановлено оказание УПИ, соответствующее требованиям к оказанию услуг, в случае нарушенияуказанных требований (24 часа).

6.2.8. Оператор ПС обеспечивает оказание услуг платежной инфраструктуры при возникновении инцидентов, а также организовать в течение установленных периодов времени восстановление оказания услуг Операторами услуг платежной инфраструктуры в случае приостановления их оказания и восстановление оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, в случае нарушения указанных требований.

6.2.9. Оператор ПС устанавливает уровни оказания услуг платежной инфраструктуры, характеризующие качество функционирования операционных и технологических средств

платежной инфраструктуры, которые должны быть обеспечены Операторами услуг платежной инфраструктуры:

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

6.2.10. Оператор ПС разрабатывает, тестирует и пересматривает План действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности (далее - план ОНиВД) Оператора платежной системы.

6.2.11. Оператор ПС организует разработку и контролирует наличие планов ОНиВД у операторов УПИ, проведение ими тестирования и пересмотра планов ОНиВД.

6.2.12. Оператор ПС анализирует эффективность мероприятий по восстановлению оказания УПИ, соответствующего требованиям к оказанию услуг, и использовать полученные результаты при управлении рисками в платежной системе.

6.3. Оператор ПС передает часть функций по реализации мероприятий по управлению рисками и управлению непрерывностью функционирования ПС Операторам УПИ и Участникам ПС «ХЕЛЛО».

6.4. Деятельность по обеспечению БФПС осуществляется Субъектами ПС в соответствии с настоящим Положением обеспечения БФПС и контролируется Оператором ПС[4].

6.5. В обязанности Оператора ПС входят функции указанные в п.6.2, а также:

- осуществление координации деятельности Субъектов ПС по обеспечению БФПС;
- осуществление контроля соблюдения Участниками ПС, Операторами услуг платёжной инфраструктуры путём постоянного мониторинга допустимого уровня рисков нарушения БФПС.

6.6. Субъекты ПС организуют деятельность по реализации порядка обеспечения БФПС в рамках внутренних систем управления рисками своей деятельности.

6.7. В обязанности Субъектов ПС входит:

- осуществление управлением рисками нарушения БФПС, в том числе связанными с расчетным риском, правовым риском, операционным риском и другими рисками, в отношении их самих в соответствии с их внутренними документами;
- информирование Оператора ПС в случае увеличения рисков нарушения БФПС о мерах, принимаемых по обеспечению бесперебойности оказания услуг платёжной инфраструктуры (в случае непредоставления Субъектами ПС вышеуказанной информации, Оператор считает, что риски нарушения БФПС не увеличивались);
- в случае выявления Оператором ПС фактов, свидетельствующих об увеличении рисков нарушения БФПС Субъектами ПС, предоставлять разъяснения и принимать меры, направленные на снижение выявленных рисков.

6.8. Порядок и формы координации деятельности Субъектов ПС по обеспечению БФПС и реализации ими мероприятий системы управления рисками (далее—СУР) ПС предусматривает следующее:

- принятие субъектами платёжной системы критериев оценки СУР;
- внесение на рассмотрение предложений по совершенствованию СУР в ПС, основанных на опыте реализации внутренних СУР Субъектами ПС;
- использование методик оценки бесперебойности функционирования и оценки рисков нарушения бесперебойности, изложенных в настоящем Положении, при реализации внутренних СУР;
- выполнение регламента информационного взаимодействия Субъектов ПС в целях управления рисками нарушения БФПС в соответствии настоящим Положением;

---

[4] Подробно Методы управления рисками нарушения БФПС Оператором ПС изложены в Приложении № 2.

- выработка и реализация Субъектами ПС мероприятий по снижению уровней рисков на основании рекомендаций Оператора ПС в соответствии с настоящим Положением.

6.7. Контроль соблюдения порядка обеспечения БФПС Участниками ПС, Операторами услуг платёжной инфраструктуры осуществляет Оператор ПС в следующем порядке:

- сбор и накопление информации о текущих нарушениях и неисправностях в работе ПС путём заполнения журнала нарушений и неисправностей в соответствии с настоящим Положением;
- проведение на основе полученной информации анализа рисков нарушения БФПС;
- выявление текущих изменений присущих уровней рисков нарушения;
- выработка рекомендаций по снижению уровней рисков и доведение их до Субъектов ПС.

6.8. Обязанности каждого из привлечённых Операторов услуг платёжной инфраструктуры по обеспечению бесперебойности оказания услуг платёжной инфраструктуры, предоставляемых ими Участникам ПС и их клиентам, а также по организации управления рисками нарушения БФПС в части полномочий, делегированных им Оператором ПС:

- осуществлять свою деятельность в соответствии с требованиями Правил ПС, настоящего Положения и действующих нормативных документов;
- при реализации внутренних систем управления рисками учитывать требования настоящего Положения;
- доводить до Оператора ПС информацию о возникновении нарушений и неисправностей при оказании услуг, о возможных рисках для функционирования ПС, о принятии оперативных мер по устранению возникших нарушений и неисправностей;
- осуществлять самооценку уровня БФПС и уровня риска нарушения БФПС при оказании услуг в соответствии с внутренними методиками;
- обеспечивать при оказании услуг уровень БФПС не ниже, а уровень риска нарушения БФПС не выше значений, установленных в п. 5.1.;
- обеспечивать информационное взаимодействие в целях управления рисками нарушения БФПС;
- совершенствовать операционные и технологические средства и процедуры, информационные системы в целях снижения рисков нарушения БФПС.

6.9. Разграничение ответственности и полномочий между Субъектами ПС по осуществлению управления рисками нарушения БФПС.

6.9.1. Участник платёжной системы уполномочен и несёт ответственность за управление расчетным риском, риском информационной безопасности. Участник ПС обеспечивает уровень БФПС не ниже, а уровень риска нарушения БФПС не выше значений, установленных в настоящем Положении.

6.9.2. Оператор ПС уполномочен и несёт ответственность за управление операционным риском, в том числе риском информационной безопасности. Операционный центр обеспечивает уровень БФПС не ниже, ауровень риска нарушения БФПС не выше значений, установленных настоящим Положением. Снижение риска нарушения БФПС обеспечивается Операционным центром бесперебойным предоставлением операционных услуг (работой аппаратно-программных комплексов).

6.9.3. Платёжный Клиринговый Центр (ПКЦ) уполномочен и несёт ответственность за управление расчетным (кредитным риском и риском потери ликвидности) риском, риском информационной безопасности. ПКЦ обеспечивает уровень БФПС не ниже, а уровень риска нарушения БФПС не выше значений, установленных настоящим Положением. Снижение риска нарушения БФПС обеспечивается ПКЦ исключением задержек времени окончания клирингового цикла, возникших по вине ПКЦ.

6.9.4. Расчётный Центр уполномочен и несёт ответственность за управление кредитным риском, риском потери ликвидности, риском информационной безопасности. Расчётный Центр обеспечивает уровень БФПС не ниже, а уровень риска нарушения БФПС

не выше значений, установленных настоящим Положением. Снижение риска нарушения БФПС обеспечивается РЦ исключением задержек времени окончания расчётного цикла, возникших по вине РЦ.

6.9.5. Все Субъекты ПС уполномочены и несут ответственность за управление правовым риском. Субъект ПС обеспечивает уровень БФПС не ниже, а уровень риска нарушения БФПС не выше значений, установленных настоящим Положением. Снижение риска нарушения БФПС обеспечивается Субъектом ПС соблюдением требований законодательства, нормативных актов, заключённых договоров (исключением случаев предъявления претензий).

6.9.6. Все Субъекты ПС уполномочены и несут ответственность за управление общим коммерческим риском. Субъекты ПС обеспечивают уровень общего коммерческого риска не выше значений, установленных настоящим Положением.

6.9.7. Оператор ПС уполномочен и несет ответственность за управление системным риском. Оператор ПС обеспечивает уровень системного риска не выше значений, установленных настоящим Положением. Для снижения системного риска Оператор ПС организует СУР, направленную на снижение основных рисков.

6.10. Порядок оценки эффективности СУР Платёжной системы в целях ее совершенствования.

6.10.1. Оценка эффективности СУР ПС при анализе рисков нарушения БФПС производится Оператором ПС ежегодно путём проведения самооценки.

6.10.2. Основными показателями, характеризующими СУР ПС, принимаются:

- уровни рисков, рассчитываемых в соответствии с настоящим Положением;
- значения показателей П1-П5.

6.10.3. Полученные при расчётах значения уровней рисков попадают в один из двух интервалов:

Уровни рисков и значения показателей	Присущие уровни рисков не превышают допустимые, значения показателей в пределах пороговых значений	Присущие уровни рисков превышают допустимые, значения показателей в пределах пороговых значений
Уровень правового риска	ПР <=9	9 < ПР
Уровень операционного риска	ОР <=6	6 < ОР
Уровень расчетного риска	РР <=3	3 < РР
Уровень общего коммерческого риска	ОКР <=3	3 < ОКР
Уровень системного риска	СР <=18	18 < ОКР
Значения показателей П1-П5	Не превышают пороговые уровни	Превышают пороговые уровни
Оценка эффективности СУР	Удовлетворительно	Неудовлетворительно

6.10.4. Если в результате расчётов эффективность СУР ПС оценивается как «Неудовлетворительная» необходимо принятие Оператором ПС экстренных управленческих решений.

6.10.5. В целях повышения качества оценки СУР Оператор ПС организует и проводит самооценку эффективности СУР ПС.

6.10.6. Самооценка эффективности СУР платёжной системы – это процесс, позволяющий Оператору ПС на периодичной основе оценивать уровень эффективности СУР.

6.10.7. Процесс самооценки основан на балльно-весовом методе. Алгоритм проведения

самооценки и формат отчёта приведены в Приложении № 3 к настоящему Положению.

7. ТРЕБОВАНИЯ К СОДЕРЖАНИЮ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ БФПС.

7.1. Требования к детализации допустимого уровня рисков нарушения БФПС в разрезе категорий Субъектов ПС: операторов услуг платёжной инфраструктуры – по видам услуг, участников платёжной системы – по видам участия в Платёжной системе.

7.1.1. Допустимые уровни рисков нарушения БФПС приведены в п. 5.1. настоящего Положения.

7.1.2. Ответственность за обеспечение допустимого уровня риска нарушения БФПС в разрезе категорий Субъектов Платёжной системы установлена в разделе 8 Положения.

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

7.2.1. Операторами услуг платёжной инфраструктуры:

- накопление информации о возникших в процессе работы информационных систем, операционных и технологических средств нарушениях и неисправностях;
- выполнение самооценки уровня БФПС и уровня риска нарушения БФПС, связанного с функционированием информационных систем, операционных и технологических;
- сравнение расчётных значений уровня риска с допустимыми;
- составление динамики изменения уровня риска;
- в случае превышения уровнем риска допустимых значений или негативной динамики уровня риска, принятие решения о модернизации или замене используемых информационных систем, операционных и технологических средств.
- дополнительно для оценки качества используются следующие технологические показатели: среднее время реакции на восстановление после инцидента; среднее время решения инцидента; количество инцидентов, решение которых превышает установленное время; общее количество инцидентов за период.

7.2.2. Независимой организацией:

- принятие Оператором ПС решения о привлечении независимой сторонней организации для осуществления оценки качества и надёжности функционирования информационных систем, операционных и технологических средств ПС в целом или отдельных операторов услуг платёжной инфраструктуры;
- выбор Оператором ПС сторонней независимой организации;
- заключение Оператором ПС договора со сторонней независимой организацией;
- предоставление Оператором ПС сторонней независимой организации информации, необходимой для выполнения работ;
- выполнение сторонней независимой организацией работ по оценке качества и надёжности функционирования информационных систем, операционных и технологических средств;
- представление сторонней независимой организацией отчёта о выполнении работ с рекомендациями по совершенствованию информационных систем, операционных и технологических средств;
- принятие Оператором ПС решения о модернизации или замене используемых информационных систем, операционных и технологических средств в соответствии с рекомендациями сторонней независимой организации.

7.2.3. Порядок выбора и реализации мероприятий и способов достижения и поддержания допустимого уровня рисков нарушения БФПС, порядок оценки их эффективности и совершенствования:

- действующие мероприятия и способы по управлению рисками нарушения БФПС определены в Приложении №1 к настоящему Положению;

- определены способы достижения и поддержания допустимых уровней рисков нарушения;
- новые мероприятия и способы достижения и поддержания допустимого уровня рисков нарушения БФПС Оператором ПС на основании предложений Субъектов Платёжной системы;
- разработка новых мероприятий и способов достижения и поддержания.

8. РАЗГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ И ПОЛНОМОЧИЙ МЕЖДУ УЧАСТНИКАМИ ПЛАТЕЖНОЙ СИСТЕМЫ ПО ОСУЩЕСТВЛЕНИЮ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ НАРУШЕНИЯ БЕСПЕРЕБОЙНОСТИ ФУНКЦИОНИРОВАНИЯ ПЛАТЕЖНОЙ СИСТЕМЫ «ХЕЛЛО».

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

Оператор Платежной системы:

- координирует деятельность Участников ПС по обеспечению бесперебойности функционирования ПС;
- разрабатывает внутренние документы по управления рисками в ПС и доводит их до сведения Участников;
- инициирует при необходимости проведение рабочих совещаний Участников по вопросу управлению рисками в ПС;
- определяет мероприятия по управлению рисками;
- определяет и внедряет способы управления рисками;
- контролирует соблюдение участниками ПС порядка обеспечения бесперебойности функционировании ПС «ХЕЛЛО»;
- определяет показатели бесперебойности функционирования ПС;
- устанавливает требования к содержанию деятельности по обеспечению бесперебойности функционирования ПС, осуществляемой Участниками ПС;
- устанавливает допустимый уровень рисков нарушения бесперебойности функционирования Платежной системы;
- осуществляет анализ рисков нарушения бесперебойности функционирования ПС;
- принимает меры, необходимые для достижения или поддержания допустимого уровня рисков нарушения бесперебойности функционирования ПС;
- уполномочен и несет ответственность за управление рисками ПС и обеспечивает допустимый уровень воздействия рисков;
- выявляет текущие изменения присущего уровня риска нарушения бесперебойности функционирования (далее- мониторинг) Платежной системы;
- осуществляет информационное взаимодействие Участников ПС в целях управления рисками нарушения бесперебойности функционирования ПС.

Кредитная организация - участник ПС:

- обеспечивают соблюдение Правил ПС, заключенных договоров, законодательных требований;
- обеспечивают надлежащее функционирование операционных и технологических средств, устройств, информационных систем, используемых в работе ПС;
- обеспечивают надлежащую защиту информации;
- предпринимают меры по поддержанию необходимого остатка денежных средств на своих банковских счетах в Расчетном центре, используемых для расчетов в рамках ПС либо предпринимают другие меры для соблюдения порядка и своевременности расчетов, предусмотренные договорами, на основании которых Участники осуществляют свою деятельность в ПС.
- Банк-участник ПС уполномочен и несет ответственность за управление кредитным риском, риском потери ликвидности, риском информационной безопасности.

Операционный центр ПС:

- Операционный центр уполномочен и несет ответственность за управление операционным риском, в том числе риском информационной безопасности.
- Операционный центр обеспечивает уровень бесперебойности функционирования Платежной системы не ниже, а уровень риска нарушения бесперебойности функционирования ПС не выше значений, установленных в настоящем Положении;
- снижение риска нарушения бесперебойности функционирования ПС обеспечивается Операционным центром беспрерывным круглосуточным предоставлением операционных услуг (работой аппаратно-программных комплексов).

Платежный клиринговый центр:

- Платежный клиринговый центр уполномочен и несет ответственность за управление кредитным риском, риском ликвидности, риском информационной безопасности;
- снижение риска нарушения бесперебойности функционирования ПС обеспечивается Платежным клиринговым центром исключением задержек времени окончания клирингового цикла, возникших по вине Платежного клирингового центра.

Расчетный центр:

- Расчетный центр уполномочен и несет ответственность за управление кредитным риском, риском ликвидности, риском информационной безопасности;
- Снижение риска нарушения бесперебойности функционирования Платежной системы обеспечивается исключением задержек времени окончания клирингового цикла, возникших по вине Расчетного центра.

Все Участники Платежной системы «ХЕЛЛО» несут ответственность за управление рисками в пределах своих полномочий. Снижение риска нарушения бесперебойности функционирования ПС обеспечивается Участниками Платежной системы «ХЕЛЛО» соблюдением требований законодательства, нормативных актов, заключенных договоров (исключением случаев предъявления претензий).

9. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ СУБЪЕКТОВ ПС ПО ОБЕСПЕЧЕНИЮ БФПС.

9.1. Субъекты платёжной системы при осуществлении деятельности по обеспечению БФПС руководствуются настоящим Положением, а также внутренними документами, разработанными в соответствии с требованиями настоящего Положения. Оператор ПС организует взаимодействие Субъектов ПС по обеспечению БФПС.

9.1.1. Оператор ПС определяет порядок взаимодействия Субъектов ПС при реализации

мероприятий по управлению рисками и управлению непрерывностью функционирования ПС.

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

Операторы услуг платежной инфраструктуры незамедлительно и оперативно информируют Оператора о нарушении оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, при котором превышено время восстановления оказания услуг платежной инфраструктуры, в случае их приостановления и (или) время восстановления оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг посредством электронной почты, а также по согласованным каналам связи.

Информация о нарушении оказания услуг платежной инфраструктуры незамедлительно предоставляется исполнительным органом или должностным лицом (структурным подразделением), ответственным за управление рисками, Оператора услуг платежной инфраструктуры исполнительному органу и/или должностному лицу (структурному подразделению), ответственному за управление рисками, Оператора.

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

- Банк России и Участников ПС в порядке, установленном Указанием Банка России № 3280-У;
- Операторов услуг платежной инфраструктуры в порядке, аналогичном установленному Указанием Банка России № 3280-У для Участников ПС.

9.2. В случае возникновения событий, вызвавших спорные, нестандартные и чрезвычайные ситуации, включая случаи системных сбоев, результатах расследования указанных событий, анализа их причин и последствий, Субъекты ПС обязаны в разумные сроки проинформировать Оператора ПС, используя любые доступные средства связи, предусмотренные Правилами ПС.

9.3. Участники ПС обязаны незамедлительно проинформировать Оператора ПС о неисполнении или ненадлежащем исполнении обязательств Участников ПС, используя любые доступные средства связи, предусмотренные Правилами ПС.

9.4. Оператором ПС фиксирует поступившую информацию с указанием: даты и времени поступления информации, даты и времени возникновения нарушений и неисправностей работы платёжной системы, характера нарушений и неисправностей, контактных данных отправителя информации.

9.5. Оператором ПС проверяет информацию, полученную в соответствии с пунктом 9.3., путём обращения по телефонным каналам связи или по электронной почте с установленного адреса на установленные адреса к Участникам ПС или Операторам услуг платёжной инфраструктуры (в зоне ответственности которых находятся заявленные нарушения и неисправности) не позднее 11:00 часов рабочего дня, следующего за датой получения.

9.6. Подтверждение (или опровержение) Участником ПС или Оператором услуг платёжной инфраструктуры (в зоне ответственности которого находятся заявленные нарушения и неисправности) Оператору ПС факта нарушения (с указанием даты, времени возникновения, времени устранения, характера нарушений и неисправностей, причин их возникновения и принятых мерах по их устранению, результатах расследования указанных событий, анализа последствий), производится путём обращения по телефонным каналам связи или по электронной почте с установленных адресов на установленный адрес не позднее 14:00 часов рабочего дня, следующего за датой получения информации.

9.7. Фиксирование оператором платёжной системы информации, поступившей в соответствии с пунктом 9.6., производится не позднее 15:00 часов дня обращения Оператора ПС путём заполнения журнала нарушений и неисправностей в работе ПС по форме:

№ п/п	**Дата и время начала нарушений в работе ПС**	**Дата и время окончания нарушений в работе ПС**	**Характер нарушений в работе ПС**	**Источник получения информации о нарушении в работе ПС**	**Дата и время поступления информации о нарушении в работе ПС**	**Ответственный за устранение нарушения в работе ПС**	**Выполненные мероприятия по устранению нарушения в работе ПС**	**Результат устранения нарушения в работе ПС**
1	2	3	4	5	6	7	8	9

10. ТРЕБОВАНИЯ К ПЛАНАМ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ ДЕЯТЕЛЬНОСТИ И ВОССТАНОВЛЕНИЯ ДЕЯТЕЛЬНОСТИ.

10.1. Требования к Плану обеспечения непрерывности деятельности и восстановления деятельности Оператора ПС.

10.1.1. Оператор ПС разрабатывает, тестирует и пересматривает План ОНиВД Оператора ПС, с периодичностью не реже одного раза в два года.

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

- при наличии в ПС двух и более РЦ - мероприятия по обеспечению взаимозаменяемости Операторов услуг платежной инфраструктуры;
- при наличии в ПС одного ОЦ и (или) ПКЦ - мероприятия по привлечению другого Оператора услуг платежной инфраструктуры и по переходу Участников ПС на обслуживание к вновь привлеченному Оператору УПИ в течение срока, установленного Правилами Платежной системы «ХЕЛЛО» (10 рабочих дней), в случаях:
- превышения Оператором услуг платежной инфраструктуры времени восстановления оказания услуг платежной инфраструктуры при приостановлении их оказания более двух раз в течение трех месяцев подряд,
- нарушения Правил Платежной системы «ХЕЛЛО», выразившегося в отказе Оператора услуг платежной инфраструктуры в одностороннем порядке от оказания услуг Участнику (Участникам) ПС, не связанного с приостановлением (прекращением) участия в ПС в случаях, предусмотренных Правилами Платежной системы «ХЕЛЛО».

10.1.3. Оператор ПС обеспечивает реализацию указанных выше мероприятий.

10.1.4. Оператор ПС организует разработку и контролирует наличие планов ОНиВД у Операторов услуг платежной инфраструктуры, проведение ими проверки (тестирования) и пересмотра планов ОНиВД с периодичностью не реже одного раза в два года.

10.2. Требования к планам обеспечения непрерывности деятельности и восстановления деятельности Операторов услуг платежной инфраструктуры.

10.2.1. Операторы услуг платёжной инфраструктуры обязаны иметь самостоятельно разработанные планы обеспечения непрерывности своей деятельности и восстановления деятельности.

10.2.2. Планы[5] обеспечения непрерывности деятельности и восстановления деятельности Операторов услуг платёжной инфраструктуры разрабатываются в целях:

- поддержания работоспособности, т.е. способности выполнять принятые на себя обязательства;
- предупреждения и предотвращения возможного нарушения режима функционирования;
- снижения тяжести последствий в случае возможного нарушения режима функционирования;
- своевременной ликвидации последствий возможного нарушения режима функционирования;
- обеспечения информационной безопасности.

10.2.3. Планы обеспечения непрерывности деятельности и восстановления деятельности операторов услуг платёжной инфраструктуры должны предусматривать действия персонала в следующих ситуациях:

- при угрозе взрыва, обнаружении подозрительных предметов, похожих на взрывные устройства;
- при обнаружении очага пожара;
- при вооруженном нападении;
- при возникновении технических неисправностей информационных компьютерных систем (серверов, системного и прикладного программного обеспечения, систем электронного обмена данными), нарушении целостности баз данных, обнаружении компьютерных вирусов в локальной вычислительной сети и возникновении сбоев в электропитании.
- В случае если Оператор услуг платежной инфраструктуры является кредитной организацией, разработка, тестирование и пересмотр плана ОНиВД осуществляется в порядке, предусмотренном Положением Банка России от 16 декабря 2003 года № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах» (далее - Положение Банка России № 242-П), с учетом требований к плану ОНиВД, содержащихся в настоящем Положении о БФПС.

[5] План обеспечения непрерывности деятельности и восстановления деятельности см. в Приложении № 4.

11. ОРГАНИЗАЦИОННАЯ МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ УЧАСТНИКОВ ПЛАТЕЖНОЙ СИСТЕМЫ «ХЕЛЛО» ПРИ ОСУЩЕСТВЛЕНИИ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ БЕСПЕРЕБОЙНОСТИ ФУНКЦИОНИРОВАНИЯ ПЛАТЕЖНОЙ СИСТЕМЫ «ХЕЛЛО».

Организационные аспекты взаимодействия Участников Платежной системы «ХЕЛЛО» при осуществлении деятельности по обеспечению бесперебойности функционирования Платежной системы «ХЕЛЛО» включают:

11.1. Координация деятельности Участников Платежной системы «ХЕЛЛО» регламентируется договорами, соглашениями и Правилами Платежной системы, которые содержат общие принципы функционирования Платежной системы «ХЕЛЛО» и ее Участников, управление рисками, обеспечения бесперебойности и зашиты информации, порядок разрешения споров и взаимодействия в чрезвычайных ситуациях.

11.2. Контроль за соблюдением порядка обеспечения бесперебойности функционирования Платежной системы «ХЕЛЛО» Участниками Платежной системы осуществляет Оператор Платежной системы в соответствии с определениями раздела 8 настоящего Положения.

11.3. Ответственность и полномочия Участников ПС разграничиваются в соответствии с применяемой организационной моделью управления рисками Платежной системы «ХЕЛЛО». Все Участники Платежной системы «ХЕЛЛО» уполномочены и несут ответственность за управление рисками в соответствии с классификацией, утвержденной Оператором ПС.

11.4. Оператор ПС информирует о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры Участников ПС в порядке, установленном Указанием Банка России № 3280-У.

12. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ОПЕРАТОРАМИ УПИ И УЧАСТНИКАМИ ПЛАТЕЖНОЙ СИСТЕМЫ ПОРЯДКА ОБЕСПЕЧЕНИЯ БФПС.

12.1. Оператор ПС в рамках осуществления контроля за соблюдением Правил Платежной системы «ХЕЛЛО» проверяет соблюдение Операторами услуг платежной инфраструктуры и Участниками ПС порядка обеспечения БФПС.

12.2. Порядок контроля выполнения Участниками ПС и Операторами услуг платежной инфраструктуры требований по соблюдению процедур управления рисками и контроля управления непрерывностью функционирования ПС предусмотрен разделом 8 Положения.

12.3. Оператор ПС контролирует соответствие документов Операторов услуг платежной инфраструктуры порядку обеспечения БФПС и при выявлении несоответствия направляет рекомендации Операторам услуг платежной инфраструктуры по устранению выявленных несоответствий.

12.4. Оператор ПС при выявлении нарушения порядка обеспечения БФПС Операторами услуг платежной инфраструктуры и Участниками ПС:

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

12.5. Оператор определяет ответственность Операторов услуг платежной инфраструктуры и Участников за неисполнение порядка обеспечения БФПС. Каждый Субъект Платежной системы несет индивидуальную ответственность за невыполнение/ несоблюдение мер по обеспечению БФПС соответственно выполняемому функционалу, определенному в Правилах и настоящем Положении по БФПС. Операторы услуг платежной инфраструктуры и Участники ПС несут ответственность за неисполнение порядка

обеспечения БФПС, меру Ответственности устанавливает Оператор.

12.6. Оператор несет ответственность за реальный ущерб, причиненный Участникам платежной системы вследствие неоказания (ненадлежащего оказания) услуг платежной инфраструктуры в случае их осуществления (за исключением услуг Расчетного центра), при этом ответственность Оператора за реальный ущерб ограничена размером неустойки, за исключением случаев умышленного неоказания (ненадлежащего оказания) услуг платежной инфраструктуры (за исключением услуг Расчетного центра). Размер неустойки определяется как размер реального ущерба, причиненного Участнику платежной системы.Факт причинения и размер реального ущерба доказывается Участником самостоятельно

13. ТРЕБОВАНИЯ К МЕТОДИКАМ АНАЛИЗА РИСКОВ В ПЛАТЕЖНОЙ СИСТЕМЕ, ВКЛЮЧАЯ ПРОФИЛИ РИСКОВ.

13.1. Оператор ПС в целях управления рисками в ПС разрабатывает методики анализа рисков в платежной системе, включая риск нарушения БФПС.

13.2. Методики анализа рисков в ПС обеспечивают:

- выявление и анализ рисков в ПС, включая выявление событий, реализация которых может привести к возникновению инцидента (далее - риск-события), и определение для каждого из выявленных риск-событий величины риска, характеризуемого вероятностью наступления риск-событий и величиной возможных последствий их реализации (далее - уровень риска);

- определение для каждого из выявленных рисков в ПС уровня риска, имеющегося до применения способов управления рисками в ПС (далее - уровень присущего риска), а также максимального уровня риска, при котором восстановление оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, включая восстановление оказания услуг платежной инфраструктуры, в случае приостановления их оказания, осуществляется в течение периодов времени, установленных Оператором ПС, и предполагаемый ущерб от которого Оператор ПС готов принять без применения способов управления рисками в ПС (далее - уровень допустимого риска);

- определение рисков в ПС, для которых уровень присущего риска выше уровня допустимого риска (далее - значимые для платежной системы риски);

- определение уровня каждого из значимых для ПС после применения способов управления рисками в ПС (далее - уровень остаточного риска).

13.3. Методики анализа рисков в ПС предусматривают выполнение следующих мероприятий:

- формирование и поддержание в актуальном состоянии перечней бизнес-процессов (Приложение № 10 к настоящему Положению о БФПС);

- разработку и поддержание в актуальном состоянии классификаторов (структурированных перечней) рисков в ПС, риск-событий, причин риск-событий;

- проведение анализа бизнес-процессов в ПС, включая анализ и оценку технологического обеспечения Операторов услуг платежной инфраструктуры и других факторов, влияющих на БФПС;

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

- определение уровня присущего риска для каждого из выявленных рисков в ПС и установление уровня допустимого риска;

- сопоставление определенного уровня присущего риска и установленного уровня допустимого риска по каждому из выявленных рисков в ПС для выделения значимых для ПС рисков;

- применение способов управления рисками в ПС для каждого из значимых для ПС рисков и последующее определение уровня остаточного риска для каждого из значимых для ПС рисков;

- сопоставление уровней остаточного риска и допустимого риска для каждого из значимых для ПС рисков и принятие решения о необходимости применения других способов управления рисками в ПС в дополнение к ранее примененным способам;

- мониторинг рисков в ПС, в том числе уровней остаточных рисков в ПС, их соответствия уровню допустимого риска;

- составление и пересмотр (актуализацию) по результатам оценки рисков в ПС и анализа эффективности мероприятий по восстановлению оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, профиля каждого из выявленных рисков в ПС, включая профиль риска нарушения БФПС (далее - профили рисков) (Приложение № 11 и Приложение № 12 к настоящему Положению о БФПС).

13.4. Оператор ПС составляет профили рисков в соответствии со следующими требованиями.

13.4.1. Профили рисков составляются по всем выявленным рискам в ПС, в том числе по следующим рискам:

- по риску оказания услуг платежной инфраструктуры, не соответствующего требованиям к оказанию услуг, вследствие несоблюдения Субъектами ПС требований законодательства Российской Федерации, Правил Платежной системы «ХЕЛЛО», договоров,заключенных между Субъектами ПС, документов Оператора ПС и документов Операторовуслуг платежной инфраструктуры либо вследствие наличия правовых коллизий и (или) правовой неопределенности в законодательстве Российской Федерации, нормативных актах Банка России, Правилах Платежной системы «ХЕЛЛО» и договорах, заключенных между Субъектами ПС, а также вследствие нахождения Операторов услуг платежной инфраструктуры и Участников ПС под юрисдикцией различных государств (правовой рискПС);

- по риску оказания услуг платежной инфраструктуры, не соответствующего требованиям к оказанию услуг, вследствие возникновения у Субъектов ПС 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 ПС либо вследствие воздействия событий, причины возникновения которых не связаны с деятельностью Субъектов ПС, включая чрезвычайные ситуации, ошибочные или противоправные действия третьих лиц (операционный риск ПС);

- по риску оказания услуг платежной инфраструктуры, не соответствующего требованиям к оказанию услуг, РЦ ПС вследствие невыполнения Участниками ПС договорных обязательств перед указанной организацией в установленный срок или в будущем (кредитный риск ПС);

- по риску оказания услуг платежной инфраструктуры, не соответствующего требованиям к оказанию услуг, вследствие отсутствия у Участников ПС денежных средств, достаточных для своевременного выполнения их обязательств перед другими Субъектами Платежной системы (риск ликвидности ПС);

- по риску оказания услуг платежной инфраструктуры, не соответствующего требованиям к оказанию услуг, вследствие ухудшения финансового состояния Оператора ПС и (или) Операторов услуг платежной инфраструктуры, не связанного с реализацией кредитного риска ПС и риска ликвидности ПС (общий коммерческий риск ПС).

13.4.2. Профиль каждого из выявленных рисков в ПС содержит:

- описание риск-событий, выявленных с применением не менее одного метода из числа предусмотренных национальным Стандартом Российской Федерации ГОСТ Р 58771-2019 "Менеджмент риска. Технологии оценки риска" с датой введения в действие 1 марта 2020 г. (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 ПС 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 Платежной системы, на которые влияет риск-событие;
- уровень присущего риска;
- уровень допустимого риска;
- уровень остаточного риска;
- перечень способов управления рисками в ПС, позволяющих снизить уровень присущего или остаточного риска.

13.5. Профиль риска нарушения БФПС составляется в отношении значимых для ПС рисков. Форма профиля риска определена в Приложении № 12 к настоящему Положению о БФПС.

13.6. Профили рисков пересматриваются (актуализируются) их не реже одного раза в год. В случае возникновения инцидента, приведшего к приостановлению оказания услуг платежной инфраструктуры, который не отражен в профилях рисков как риск-событие, профили рисков должны пересматриваться (актуализироваться) в срок, не превышающий трех месяцев со дня возникновения данного инцидента.

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

14. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.

14.1. Настоящее положение вступает в силу со дня его утверждения генеральным директором ООО «Хелло» и действует в течение всего времени до вступления в силу новой редакции.

14.2. Все вопросы, не урегулированные в настоящем Положении, регулируются действующим законодательством Российской Федерации, нормативными документами Банка России, Правилами Платежной системы «ХЕЛЛО» и иными внутренними документами ООО «Хелло».

14.3. Если в результате изменения законодательства Российской Федерации и нормативных документов Банка России отдельные статьи настоящего Положения вступают в противоречие с ними, эти статьи утрачивают силу.

Настоящее Положение входит в состав Правил Платежной системы «ХЕЛЛО»

Приложение № 1
к Положение по УР и обеспечению БФПС

Методика оценки рисков в Платежной системе «ХЕЛЛО»

1. Выявление и анализ рисков в Платежной системе проводится Оператором с применением следующих элементов методик, основанных на статистическом и сценарном анализе функционирования системы и соответствующих «ГОСТ Р ИСО/МЭК 31010-2011. Национальный стандарт Российской Федерации. Менеджмент риска. Методы оценки риска» (далее – Стандарт), в том числе:

- анализ, отслеживание и фиксирование параметров работы Участников в Платежной системе, в т. ч. соблюдение порядка расчетов;
- 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 Платежной системы.

Также, при оценке рисков Оператор, в соответствии со Стандартом, использует метод индексов риска - смешанный метод оценки риска. Индекс риска — это мера риска, представляющая собой количественную оценку риска, полученную с применением балльных оценок.

2. В соответствии с принятой классификацией рисков ПС в целях проведения оценки устанавливаются следующие уровни рисков:

Категория риска	***Без риска***	***Низкий***	***Средний***	***Высокий***
Уровень риска (u)	0	1	2	3

3. Оценка уровня риска нарушения БФПС рассчитывается на основе оценок основных рисков.

3.1. Для оценки применяется показатель доступности (услуги, Субъекта платежной системы в целом и др.) в среднем в течение заданного временного интервала (срок оказания услуги в соответствии с регламентом, операционный день и др.). Показатель доступности рассчитывается по следующей формуле:

$$d = (1 — t / T)$$

где d – показатель доступности;

T – продолжительность заданного временного интервала;

t – средняя длительность нарушений работоспособности в течение заданного временного интервала. Показатель доступности принимает значения из интервала [0,1]. При этомзначение

$d = 1$ соответствует функционированию без сбоев в течение заданного временного интервала. Значение $d = 0$ возможно в случае неработоспособности в течение заданного временного интервала.

3.2. Уровень риска нарушения БФПС устанавливается в соответствии с конкретными значениями показателей доступности, попадающими в заданные интервалы.

3.3. Процедуру анализа рисков нарушения БФПС осуществляют внутренние

структурные подразделения Оператора ПС, ответственные за анализ и контроль рисков в соответствии с принятой классификацией. Данная процедура включает:

- выявление факторов риска нарушения БФПС;
- определение степени и характера влияния указанных факторов на БФПС;
- оценка присущего уровня рисков нарушения БФПС (размер возможного ущерба);
- оценка вероятности возникновения указанных нарушений;
- подтверждение соответствия присущего уровня рисков допустимому уровню;

3.4. Принятие мер, необходимых для достижения или поддержания допустимого уровня каждого из видов рисков нарушения БФПС, осуществляется внутренним структурным подразделением Оператора ПС, ответственным за анализ и контроль соответствующего риска. Управление рисками осуществляют уполномоченные органы и подразделения оператора в соответствии со своими полномочиями.

3.5. Выявление текущих изменений присущего уровня риска нарушения БФПС осуществляется ответственными структурными подразделениями Оператора ПС на регулярной основе в сроки, предусмотренные регламентирующими процесс управления рисками внутренними нормативными документами.

3.6. В целях управления рисками нарушения БФПС Оператор ПС осуществляет информационное взаимодействие с Субъектами ПС в соответствии с порядком информационного взаимодействия Субъектов ПС и документационного обеспечения их деятельности по обеспечению БФПС.

3.7. Оценка последствий реализации рисков в ПС. Для оценки последствий размера потенциального негативного эффекта (Нэ) для ПС вследствие реализации риска применяется следующая шкала бальной оценки:

Баллы (b)	**Негативный эффект (Нэ)**	**Расшифровка**
1	***Незначительный***	Реализация риска практически не повлияет на функционирование ПС
2	***Допустимый***	Реализация риска приведет к незначительным неблагоприятным последствиям для функционирования ПС
3	***Значительный***	Реализация риска приведет к значительным неблагоприятным последствиям для функционирования ПС

Баллы используются для корректировки уровней риска нарушения БФПС (u) с учетом потенциального негативного эффекта (Нэ). Корректировка осуществляется умножением полученного значения уровня риска (УР) на балл (Б), соответствующий выбранному потенциальному негативному эффекту (потерь).

4. Операционный риск.

4.1. Источником операционного риска является нарушение работоспособности аппаратно-программных комплексов, ненадлежащие действия персонала, а также неэффективная деятельность Службы внутреннего контроля (например, возможные сбои, отказы аппаратно-программных средств, отсутствие резервных схем работы, противоправные действия или ошибки сотрудников Субъектов Платежной системы, несвоевременное выявление допущенных ошибок или иных результатов действий, способных привести к неблагоприятным событиям).

4.2. Локализацией (местом проявления) операционного риска являются структурные подразделения и аппаратно-программные комплексы Субъектов ПС, в разрезе которых осуществляется контроль проявления операционного риска.

4.3. Формой реализации операционного риска являются нарушения функционирования ПС в результате нарушения работоспособности аппаратно-

программных комплексов Субъектов ПС, выполнения недопустимых операций или ошибочного выполнения операций в ПС.

4.4. Оценка уровня показателя БФПС при реализации операционного риска (ОР) и уровня операционного риска (УОР) рассчитываются в соответствии с пунктами 4. и 5.1. Показатель бесперебойности оказания операционных услуг (ОР) применяется к оценке оказания услуг в случаях нарушения работоспособности аппаратно-программных комплексов и ненадлежащих действий персонала с учетом того, что операционный риск может проявляться круглосуточно, Т = 1440 мин. Показатель бесперебойности может применяться к оценке оказания услуг (с учетом иных временных интервалов t и Т, соответствующих временному регламенту их функционирования).

Категория риска	***Без риска***	***Низкий***	***Средний***	***Высокий***[6]
Пороговые значения t (мин.)	0	10	30	60
Пороговые значения ОР	0,993	0,979	0,958	0,957
Интервалы t (мин.)	t<=10	11<t<=30	31<t<=60	t>60
Интервалы ОР	ОР>=0,993	0,994<ОР<=0,979	0,980<ОР<=0,958	ОР<0,958
Уровень риска (УОР)	0	1	2	3
Уровень риска с учетом негативного эффекта (УОР*2)	0	2	4	6

Размер потенциального негативного эффекта (потерь) в случае наступления операционного риска – допустимый (Б = 2 балла). Реализация риска приведет к незначительным неблагоприятным последствиям для функционирования ПС.

Допустимый уровень операционного риска нарушения БФПС с учетом негативного эффекта (потерь) устанавливается не более 6.

4.5. Система управления операционным риском предусматривает следующие способы и мероприятия по управлению риском:

4.5.1. По обеспечению работоспособности аппаратно-программных комплексов:

- разработка технических требований на создание, внедрение и эксплуатацию аппаратно-программных комплексов с учетом требований к показателям бесперебойности;
- тестирование аппаратно-программных комплексов перед их внедрением;
- регулярный мониторинг системного, прикладного программного обеспечения и доступа к информационным ресурсам;
- обеспечение целостности информационных активов путем применения: средств идентификации и аутентификации; процедур протоколирования и аудита; криптографической защиты информации; резервного копирования и архивирования информационных ресурсов;
- обеспечение резервирования критичных информационных активов;
- разработка, поддержание в актуальном состоянии планов обеспечения непрерывности деятельности и восстановления деятельности после сбоев;
- проведение регулярной оценки качества и надежности функционирования информационных систем, операционных и технологических средств, соответствие их отраслевым нормативным актам;
- проведение регламентных работ.

[6] Принимаются меры, решения по усмотрению Оператора

4.5.2. По персоналу:

- ограничение функций и полномочий сотрудников;
- обучение персонала новым информационным технологиям, повышение его квалификации, периодическое тестирование.

5. **Расчетный риск** (кредитный риск и риск ликвидности).

5.1. Источником расчетного риска (РР) является недостаточность (отсутствие) средств у Участника или нескольких Участников ПС для своевременного выполнения ими своих расчетных обязательств перед другими Участниками ПС, финансовая несостоятельность Участника ПС, концентрация значительного объема расчетных документов в определенные моменты и (или) периоды времени в течение дня, вероятность возникновения которых обусловлена особенностями ПС и внешними факторами (например: наличие разрыва во времени между моментами приема расчетных документов для проверки на соответствие установленным требованиям и проведения расчета по этим документам, отсутствие требований о предварительном депонировании денежных средств, выполнение процедур неттинга, процедуры управления очередью расчетных документов).

5.2. Локализацией (местом проявления) расчетного риска являются счета Участников ПС, показатели состояния этих счетов, контроль за которыми позволяет выявить предпосылки реализации риска (например, количество и величина дебетовых позиций отдельных Участников, наличие, состав и величина очередей неисполненных расчетных документов).

5.3. Формой реализации кредитного риска и риска ликвидности являются нежелательные изменения показателей, характеризующих несвоевременность проведения Участником платежной системы расчетов (например, время задержки исполнения расчетных документов, отсутствие денежных средств на корреспондентских счетах Участников ПС или невозможность использования имеющихся на этих счетах остатков денежных средств, невозможность исполнения Участником своих обязательств в ПС).

5.4. Оценка уровня БФПС при реализации **расчетного** риска.

5.4.1. Оценка уровня БФПС при урегулировании Участником ПС «чистых» дебетовых позиций в пределах клирингового цикла (РР) и уровень риска (УРР) рассчитываются в соответствии с пунктами 4 и 5.1. с учетом того, что t — число операционных дней нарушения БФПС, Т — среднее число операционных дней в течение месяца, Т = 21 день.

Категория риска	***Без риска***	***Низкий***	***Средний***	***Высокий***
Пороговые значения t (мин.)	0	5	10	15
Пороговые значения РР	1,00	0,76	0,52	0,28
Интервалы t (мин.)	t<=5	5<t<=10	10<t<=15	t>15
Интервалы РР	РР>=0,76	0,75<РР<=0,52	0,51<РР<=0,27	РР<0,28
Уровень риска (УРР)	0	1	2	3
Уровень риска с учетом негативного эффекта (УРР*1)	0	1	2	3

Для одновременной оценки уровня БФПС при урегулировании всеми Участниками Платежной системы «чистых» дебетовых позиций в пределах клирингового цикла в приведенном выше расчете вместо t применяется tcp. — среднее число операционных дней нарушения БФПС в течение месяца, T — среднее число операционных дней в течение месяца, T = 21 день. Величина tcp рассчитывается по следующей формуле (2):

$$tcp. = (t1 + t2 + \dots + tn) / n, \quad (2)$$

где ti - число операционных дней в течение месяца, когда i-й Участник ПС нарушал БФПС, (i=1, 2, … , n),

n — число Участников ПС.

Размер потенциального негативного эффекта (потерь) в случае наступления расчетного риска – незначительный (b = 1 балл). Реализация риска практически не повлияет на функционирование Платежной системы.

Допустимый уровень расчетного риска нарушения БФПС с учетом негативного эффекта (потерь) в ПС устанавливается не более 3.

5.5. Система управления расчетным риском предусматривает следующие способы и мероприятия по управлению рисками:

5.5.1. Установление предельных размеров (лимитов) обязательств Участникам платежной системы с учетом уровня риска.

5.5.2. Финансовый анализ и мониторинг деятельности участника ПС.

6. Правовой риск.

6.1. Источником правового риска является несоблюдение Субъектами Платежной системы требований законодательства, нормативных актов и заключенных договоров, внутренних документов, регламентирующих их деятельность, а также наличие недостатков внутренних документов.

6.2. Локализацией (местом проявления) правового риска являются:

- Субъекты Платежной системы, которым могут быть предъявлены претензии правового характера, связанные с несоблюдением требований законодательства, нормативных актов и заключенных договоров;
- внутренние документы Субъектов ПС и договоры, содержание которых подлежит постоянному контролю на соответствие законодательству и нормативным актам, с учетом вносимых в них изменений.

6.3. Формой реализации правового риска являются претензии правового характера к Субъектам платежной системы со стороны других Субъектов ПС, со стороны государственных органов, со стороны клиентов Участников ПС.

6.3.1. Оценка уровня БФПС при реализации правового риска (ПР) и уровень риска (УПР) рассчитываются в соответствии с пунктами 4. и 5.1. с учетом того, что t — число претензий к Субъектам ПС в течение года, T = 365 дней.

Применяется к оценке несоблюдения Субъектами Платежной системы требований законодательства, нормативных актов и заключенных договоров.

Категория риска	***Без риска***	***Низкий***	***Средний***	***Высокий***
Пороговые значения t (раз)	0	1	2	3
Пороговые значения ПР	1,00	0,997	0,995	0,992
Интервалы t (раз)	t<=1	1,1<t<=2	2,1<t<=3	t>3
Интервалы ПР	d4>=0,997	0,996<d4<=0,995	0,994<d4<=0,992	d4<0,992
Уровень риска (УПР)	0	1	2	3

Уровень риска с учетом негативного эффекта (УПР*3)	0	3	6	9

Размер потенциального негативного эффекта (потерь) в случае наступления правового риска – значительный (Б = 3 балла). Реализация риска приведет к значительным неблагоприятным последствиям для функционирования ПС.

Допустимый уровень правового риска нарушения БФПС с учетом негативного эффекта (потерь) в Платежной системе устанавливается не более 9.

6.4. Система управления правовым риском предусматривает следующие мероприятия по управлению риском:

6.4.1. Предварительная проверка Оператором ПС потенциальных Участников ПС на обладание необходимой правоспособностью (в соответствии с Правилами Платежной системы).

6.4.2. Периодическая, не реже одного раза в год, выборочная проверка Оператором ПС Участников ПС на обладание необходимой правоспособностью путем запросов на предоставление необходимой информации об их деятельности и документов, в том числе внутренних документов и договоров.

7. Общий коммерческий риск.

7.1. Источником общего коммерческого риска является наличие негативной информации о Субъектах Платежной системы.

7.2. Локализацией (местом проявления) общего коммерческого риска являются:

- наличие негативной информации о Субъектах Платежной системы в информационно-телекоммуникационной сети «Интернет», других СМИ;
- технологическое отставание Субъектов ПС.

7.3. Формой реализации общего коммерческого риска являются сокращение количества Клиентов, сокращение количества Участников.

7.3.1. Оценка уровня БФПС при реализации общего коммерческого риска (ОКР) и уровень риска (УОКР) рассчитываются в соответствии с пунктами 4. и 5.1. с учетом того, что t — число негативных публикаций о Субъектах ПС в течение года, Т = 365 дней.

Категория риска	***Без риска***	***Низкий***	***Средний***	***Высокий***
Пороговые значения t (раз)	0	1	2	3
Пороговые значения ОКР	1,00	0,997	0,995	0,992
Интервалы t (раз)	t<=1	1,1<t<=2	2,1<t<=3	t>3
Интервалы ОКР	d4>=0,997	0,996<d4<=0,995	0,994<d4<=0,992	d4<0,992
Уровень риска (УПР)	0	1	2	3
Уровень риска с учетом негативного эффекта (УПР*1)	0	1	2	3

Размер потенциального негативного эффекта (потерь) в случае наступления общего коммерческого риска – незначительный (b = 1 балл). Реализация риска практически не повлияет на функционирование Платежной системы. Допустимый уровень общего коммерческого риска нарушения БФПС с учетом негативного эффекта (потерь) в Платежной системе устанавливается не более 3.

7.4. Система управления правовым риском предусматривает следующие мероприятия по управлению риском:

7.4.1. Поддержание положительной деловой репутации Субъектов ПС, выполнение требований законодательных, нормативных документов, Правил, договоров, публикации в СМИ руководителей Субъектов ПС.

7.4.2. Использование современного технологического обеспечения и технических средств.

8. Системный риск.

8.1. Источником системного риска является реализация одновременно нескольких или всех рисков, указанных в п.4 – п.7 настоящего Приложения №1 к Положению по БФПС. Системный риск возникает вследствие неспособности одного или нескольких Субъектов ПС исполнить принятые на себя обязательства или нарушений в самой ПС, который вызовет неспособность большинства или всех Субъектов ПС исполнить свои обязательства в срок.

8.2. Локализацией (местом проявления) системного риска являются элементы ПС, контроль за которыми позволяет выявить предпосылки реализации системного риска (например, количество и величина наиболее крупных дебетовых позиций Участников ПС, наличие, состав и величина очередей неисполненных распоряжений, работоспособность основных аппаратно-программных комплексов и др.).

8.3. Формой реализации системного риска является распространение между Субъектами ПС последствий основных рисков, указанных в п.4 – п.7 настоящего Приложения №1 к Положению по БФПС, вызывающих нарушения функционирования ПС.

Уровень системного риска рассчитывается как сумма уровней основных рисков, указанных в п.4 – п.7 настоящего Приложения №1 к Положению по БФПС.

Размер потенциального негативного эффекта (потерь) в случае наступления системного риска – незначительный (b = 1 балл). Реализация риска практически не повлияет на функционирование Платежной системы. Допустимый уровень системного риска с учетом негативного эффекта (потерь) в Платежной системе устанавливается не более 18.

8.4. Система управления рисками в целях предотвращения и минимизации системного риска предусматривает предотвращение и минимизацию основных рисков указанных в п.4 – п.7 настоящего Приложения №1 к Положению по БФПС.

Приложение № 2
к Положение по УР и обеспечению БФПС

Методы управления рисками в Платежной системе «ХЕЛЛО»

1. Для управления рисками в Платежной системе «ХЕЛЛО» Оператором предусматривается проведение следующих мероприятий:

- определение организационной структуры управления рисками, обеспечивающей контроль за выполнением Участниками требований к управлению рисками, установленных Правилами ПС;
- определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений Оператора ПС;
- доведение до органов управления Оператора ПС соответствующей информации о состоянии рисков;
- определение показателей бесперебойности функционирования ПС в соответствии с требованиями нормативных актов Банка России;
- определение методик анализа рисков в ПС, включая профили рисков в соответствии с требованиями нормативных актов Банка России;
- определение порядка обмена информацией, необходимой для управления рисками;
- определение процедуры взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев;
- определение порядка изменения операционных и технологических средств и процедур;
- определение порядка оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией;
- определение порядка обеспечения защиты информации в ПС.

2. Организационная модель управления рисками.

2.1. В соответствии с выбранной моделью управления рисками, установленной Правилами Платежной системы «ХЕЛЛО», функции по оценке и управлению рисками ПС распределены между Участниками ПС.

2.2. Оператор ПС разрабатывает и утверждает внутренние документы в области управления рисками и доводятся до Расчетного центра и Участников ПС, которые самостоятельно осуществляют управление рисками, присущими их виду деятельности и несут ответственность за последствия реализации указанных рисков.

2.3. Контроль за соблюдением Участниками ПС законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, осуществляется непосредственно самим Участником.

3. Организационная структура управления рисками.

3.1. Управление рисками в Платежной системе «ХЕЛЛО» осуществляется следующими органами и структурными подразделениями Оператора Платежной системы в рамках их полномочий:

- ✓ Генеральным директором;
- ✓ Отделом управления рисками;
- ✓ Отделом информационных технологий.

3.2. В целях реализации выбранной модели управления рисками структурные подразделения ПС выполняют следующие функции:

<u>Генеральный директор:</u>

- ✓ утверждает основные принципы управления рисками;
- ✓ организует процесс управления рисками;

- ✓ утверждает форму, методику и срок составления отчетов, рассматривает отчеты Департамента рисков о состоянии системы управления рисками и оценке принимаемых рисков;
- ✓ обеспечивает условия для эффективной реализации политики в сфере управления рисками;
- ✓ определяет подразделения, ответственные за управление отдельными видами рисков;
- ✓ принимает необходимые решения и планирует мероприятия в случае признания уровня риска повышенным.

Отдел управления рисками:

- ✓ реализует процесс управления рисками;
- ✓ осуществляет разработку процедур и методов эффективного управления рисками;
- ✓ проводит постоянный мониторинг и оценку рисков ПС;
- ✓ своевременно информирует руководство ПС с целью принятия оперативных решений по локализации возникающих рисков;
- ✓ осуществляет контроль исполнения Участниками ПС установленных процедур управления рисками.

ОТдел информационных технологий:

- ✓ участвует в процессе управления рисками в пределах должностных обязанностей и полномочий.

На ***руководителей структурных подразделений*** возлагается ответственность за оперативное управление операционным риском, в том числе:

- ✓ участие в разработке мер, процедур, механизмов и технологий по ограничению и снижению возникающих рисков по своим подразделениям и направлениям работы, курируемым своими подразделениями;
- ✓ за проведение процедур выявления, оценки, мониторинга, минимизации операционного риска по своим подразделениям и по направлениям работы, курируемым своими подразделениями.

3.3. Полномочия и ответственность сотрудников Оператора ПС в процессе управления рисками устанавливаются внутренними документами, определяющими правила и процедуры управления отдельными видами рисков, а также положениями о структурных подразделениях.

4. Функциональные обязанности лиц или соответствующих подразделений Оператора ПС, ответственных за управление рисками.

4.1. В обязанности лиц или соответствующих структурных подразделений, ответственных за управление рисками в ПС, включаются следующие функциональные обязанности:

- выявление, измерение и определение допустимого уровня риска по каждому из видов рисков;
- постоянное наблюдение за рисками;
- принятие мер по поддержанию на приемлемом уровне финансовой устойчивости ПС и интересам Участников платежной инфраструктуры уровне каждого из видов рисков;
- соблюдение всеми Участниками Правил ПС;
- обеспечение бесперебойности функционирования ПС;
- сбор и обработка информации в рамках Системы управления рисками, в том числе информации, поступающей от Участников и Операторов услуг платежной инфраструктуры;
- внесение изменений в Правила в целях управления рисками в ПС;
- регулярная оценка уровня риска по каждому из видов рисков;
- исполнение иных обязанностей в целях управления рисками в ПС.

Распределение обязанностей по управлению рисками в ПС между подразделениями и

работниками Оператора ПС устанавливается Оператором ПС в положениях, приказах, должностных инструкциях и иных внутренних документах Оператора.

5. Доведение до органов управления Оператора ПС соответствующей информации о рисках.

5.1. Оперативная информация о возникающих рисках незамедлительно доводится до сведения Генерального директора ПС в порядке и сроки, установленные Оператором ПС «ХЕЛЛО» в его внутренних документах.

5.2. Информация об общем уровне рисков ПС доводится до сведения генерального директора не реже одного раза в год.

Приложение № 3
к Положение по УР и обеспечению БФПС

Самооценка эффективности СУР Платёжной системы «ХЕЛЛО»

№ п.п.	**Параметр самооценки**	**Вес**	Балл*	Значение**
1.	Непрерывность выявления величины рисков	2		
2.	Непрерывность оценки величины рисков	2		
3	Внесение оперативных изменений в управление рисками в случае изменения внешних и внутренних факторов	1		
4.	Соблюдение пороговых величин рисков	3		
5.	Соблюдение пороговых уровней показателей БФПС	3		
6.	Поддержание информационной системы в актуальном состоянии	1		
7.	Соблюдение полномочий и системы принятия решений	2		
8.	Подготовка управленческой отчётности	2		
	Самооценка управления (итого) ***			

* При оценке параметров рекомендуется следующее определение баллов:

Балл	**Расшифровка значения**
1	присваивается в случае, если в течение любых 30 последовательных календарных дней проверяемого периода нарушения отсутствовали
2	присваивается в случае, если в течение любых 30 последовательных календарных дней проверяемого периода выявлено не более 2 нарушений
3	присваивается в случае, если в течение любых 30 последовательных календарных дней проверяемого периода выявлено 3 и более нарушений

** Значение параметра самооценки определяется путём умножения веса показателя на балл.

*** Итоговое значение самооценки рассчитывается как сумма произведения веса на балл деленное на сумму весов указанных параметров самооценки.

Самооценку эффективности СУР платёжной системы рекомендуется определять в зависимости от значения соответствующего показателя на основании шкалы, приведенной ниже в таблице.

Шкала самооценки эффективности СУР платёжной системы

Хорошее	Удовлетворительное	Сомнительное	Неудовлетворительное
< 1,3	>=1.3 и 1.9<	>=1.9 и 2.2<	>=2.2

Приложение № 4
к Положение по УР и обеспечению БФПС

План обеспечения непрерывности деятельности и восстановления деятельности

№ пп	Причины нарушений	Действия	Срок
1.	Связанные с неблагоприятными событиями природного, техногенного и социального характера, при угрозе взрыва, обнаружении подозрительных предметов, похожих на взрывные устройства, при обнаружении очага пожара	Информирование соответствующих федеральных и региональных служб.	Незамедлительно
		Принятие мер к изоляции очага, вызванного неблагоприятным воздействием.	Незамедлительно
		Эвакуация сотрудников и клиентов в безопасное место.	В соответствии с планом эвакуации
		Оповещение Участников платежной системы о невозможности осуществления переводов.	В течение двух часов после обнаружения
		Проведение восстановительных работ.	В зависимости от очага повреждения
		Информирование Участников Платежной системы о предполагаемых сроках устранения.	В течение двух часов после обнаружения
		Возобновление работы.	В течение двух часов после устранения
2.	Связанные с деятельностью террористов и лиц, совершающих преступления и правонарушения. Информирование соответствующих федеральных и региональных служб, при угрозе взрыва, обнаружении подозрительных предметов, похожих на взрывные устройства, при обнаружении очага пожара, при вооруженном нападении	Информирование.	Незамедлительно
		Эвакуация сотрудников и клиентов в безопасное место.	В соответствии с планом эвакуации
		Принятие мер к защите информации и материальных ценностей.	Незамедлительно
		Оповещение Участников Платежной системы о невозможности осуществления переводов.	В течение двух часов после обнаружения
		Проведение восстановительных работ.	В зависимости от объема повреждения
		Информирование Участников платежной системы о сроках устранения.	В течение двух часов после обнаружения
		Возобновление работы.	В течение двух часов после устранения
3.	Связанные со сбоями, отказами программных и технических средств	Определение причин, вызывающих нарушение.	В течение трех часов
		Исправление или замена программных и технических средств.	Не более одного операционного дня

		В случае невозможности осуществления электронных переводов информирование Участников Платежной системы.	В течение одного операционного дня
		Возобновление работы.	В течение двух часов после устранения
4.	Связанные с деятельностью персонала	Выявление нарушений.	В режиме реального времени
		Проведение анализа причин возникновения нарушения.	В соответствии с регламентом работы комиссии по чрезвычайным ситуациям
		Принятие мер дисциплинарного или административного воздействия к нарушителям	В установленном законодательством порядке
		Принятие мер к недопущению повтора нарушений, установления причин.	Незамедлительно после
5.	Связанные с несоответствием требованиям надзорных и регулирующих органов действующему законодательству	Выявление нарушений.	В оперативном порядке
		Приведение в соответствие внутренних документов.	В течение пятнадцати календарных дней
		Информирование надзорных органов, о выполнении требований.	В соответствии с законодательными и нормативными актами

Приложение № 5
к Положение по УР и обеспечению БФПС

Методика
оценки рисков Участников ПС (кредитные организации).

1. Общие положения.

1.1. Методика оценки рисков кредитных организаций – участников ПС «ХЕЛЛО» (далее – Методика) разработана в соответствии с требованиями Положения Банка России от 28.06.2017 г. № 590-П «О порядке формирования кредитными организациями резервов на возможные потери по ссудам, ссудной и приравненной к ней задолженности», Положения Банка России от 23.10.2017 г. № 611-П «Положение о порядке формирования кредитными организациями резервов на возможные потери» и Инструкции Банка России от 28.06.2017 г. № 180-И «Об обязательных нормативах банков».

1.2. Методика содержит описание методов, правил и процедур, используемых при оценке финансового положения кредитных организаций (далее – КО) с целью оценки расчетного риска для Участников ПС. Заключительным этапом анализа является оценка кредитоспособности КО и оценка вероятности его дефолта (с учетом финансового положения, платежной дисциплины, а также иной информации о любых рисках КО и т.д.).

1.3. Источниками получения информации о контрагенте являются его правоустанавливающие документы, бухгалтерская, налоговая, статистическая и иная отчетность, публикации в средствах массовой информации и другие источники.

1.4. Данная Методика также используется при оценке основных расчётных банков, обслуживающих ПС «ХЕЛЛО».

2. Оценки включает несколько этапов:

2.1. Общая информация о КО:

- состав акционеров (участников) банка;
- срок деятельности и тип банка (вновь созданные банки, банки с участием государства, банки с участием иностранного капитала);
- место регистрации банка;
- участие банка в банковских группах, банковских сообществах и крупных холдингах;
- освещение работы банка в прессе и сети Интернет, в частности, наличие конфликтных и криминальных ситуаций вокруг банка;
- рейтинговая позиция банка по оценке международных рейтинговых агентств;
- другая информация о банке.

2.2. Оценка финансовых показателей.

2.2.1. Целью проводимой оценки финансового положения КО, является определение степени влияния риска и определение рейтинговой позиции рассматриваемого банка для принятия решений по возможности участия контрагента в Платежной системе «ХЕЛЛО».

2.2.2. На первом этапе проводится оценка финансового положения КО на основании анализа данных финансовой отчетности[7].

[7] а) при расчете используются несколько отчетных дат.

Расчет и анализ показателей базируется на основании данных, полученных из нижеуказанных форм отчетности, предоставляемых кредитными организациями в Банк России:

- «Оборотная ведомость по счетам бухгалтерского учета кредитной организации» - Форма №0409101;
- «Отчет о финансовых результатах» - Форма №0409102;
- «Расчет собственных средств (капитала)» - Форма №0409134;
- «Информация об обязательных нормативах и о других показателях деятельности кредитной организации» - Форма №0409135[8].

2.2.3. Пример агрегации основных финансовых балансовых показателей рассматриваемой КО выглядит следующим образом:

Финансовые показатели	**Дата**	**Дата**	***Изменение (%)***
АКТИВ			
1. Ликвидные активы 2. Размещенные средства в банках 3. Кредиты, векселя 4. Долговые обязательства и другие ценные бумаги с фиксированной процентной ставкой 5. Участие в капитале юридических лиц 7. Дебиторская задолженность 8. Обязательные резервы в Банке России 8. Основные средства 9. Средства в расчетах 10. Прочие активы			
Итого актив			
ПАССИВ 1. Обязательства перед банками 2. Обязательства перед клиентами 3. Прочие обязательства 4.Источники собственных средств Уставный капитал Фонды Добавочный капитал Финансовый результат Резервы 5. Кредиторская задолженность 6. Средства в расчетах			
Итого пассив			

2.2.4. На основании проведенного сравнительного анализа основных агрегированных статей баланса определяется динамика развития КО. С этой целью проводится сравнительный анализ основных агрегированных показателей баланса, проводимый с учетом нескольких отчетных дат. Анализ полученных динамических характеристик

б) Для банков-нерезидентов в качестве источника получения данной информации может служить «Годовой отчет» банка-контрагента или данные из «Banker`s Almanac».

[8] В случае постоянного нарушения КО нормативов ф. №0409135, не связанных со спецификой работы банка, данный банк не рассматривается как контрагент.

финансовой отчетности КО позволяет выявить отрицательную динамику роста финансовых показателей, на основании которого делается прогноз финансовой устойчивости КО.

2.2.5. Кроме анализа статистических показателей деятельности КО существенное влияние на формирование экспертного мнения на данном этапе оценки риска оказывает информация, позволяющая выявить качественные характеристики деятельности КО.

1. Наличие банка в списке кредитных организаций, отвечающих требованию Банка России по уровню рейтинга, предъявляемому для поручителей по кредитам Банка России в рейтинговом списке ЦБ и/или Ломбардном списке Банка России.
Рейтинговая оценка: Нет – 0 баллов, Да - 10 баллов
2. Выявлен факт нарушений требований законодательства и/или договора по проведению расчетных операций по кор/счету (в т.ч. наличие нарушений)
Рейтинговая оценка: Нет – 0 баллов, Да – (-20) баллов
3. Выявлен факт негативной информации (участие в судебных разбирательствах, жалобы клиентов, вызвавшие общественный резонанс, негативная информация в СМИ о собственниках, руководстве КО)
Рейтинговая оценка: Нет – 0 баллов, Да - (-10) баллов
4. Выявлен факт нахождения контрагента в регионе с нестабильной социально-экономической обстановкой
Рейтинговая оценка: Нет – 0 баллов, Да – (-15) баллов
5. Выявлен факт ареста корреспондентских счетов КО
Рейтинговая оценка: Нет – 0 баллов, Да – (-20) баллов
6. Выявлен факт наличия требований налоговых органов к КО
Рейтинговая оценка: Нет – 0 баллов, Да - (-20) баллов
7. Выявлен факт введения со стороны регулятора временной администрации
Рейтинговая оценка: Нет – 0 баллов, Да - 60 баллов

К качественным характеристикам можно отнести:

- информационная прозрачность;
- рейтинговая оценка;
- кредитная история и репутация банка;
- взаимоотношения с заинтересованными лицами (акционерами, сотрудниками, клиентами и др.).

2.2.6. Для присвоения рейтинговой позиции оценка выявленных количественных и качественных характеристик финансового положения производимая оценка рассматриваемой кредитной организации формализована следующим образом:

2.3. Помимо проводимой оценки финансового положения рассматриваемой КО проводится оценка рисков прочих качественных показателей**:**

Оценочный показатель	*Хорошее*	*Среднее*	*Плохое*
Сумма баллов	от 0 до 20 баллов	от (-20) до 0 баллов	менее (-20) баллов

2.4. На заключительном этапе в результате суммирования присвоенных баллов по каждому из параметров формируется итоговая сумма баллов. В зависимости от суммы баллов производится оценка финансового положения контрагента.

2.5. В зависимости от значения итогового балла, определяется оценочный показатель, который соответствует одному из трех интервалов значений. В соответствии с

присвоенной классификацией принимается решение о рассмотрении КО в качестве участника ПС.

2.6. Для возможности участия КО в Платежной системе «ХЕЛЛО» допускаются кредитные организации, если оценочный показатель, присвоенный КО *хороший* или *средний*.

Приложение № 6
к Положение по УР и обеспечению БФПС

Перечень регламентных работ, проводимых в ОЦ, по обеспечению бесперебойности функционирования ПС «ХЕЛЛО»

№ пп	Виды работ	Периодичность
1.	Профилактика и диагностика пропускной и охранной систем, системы видеонаблюдения	Один раз в три месяца
2.	Профилактика и диагностика пожарной сигнализации, систем пожаротушения	Один раз в три месяца
3.	Профилактика и диагностика систем резервного питания	Ежемесячно
4.	Профилактика и диагностика систем климат-контроля	Ежемесячно
5.	Резервирование каналов связи	Постоянно
6.	Резервирование сетевых аппаратных средств	Постоянно
7.	Профилактика сетевого оборудования, межсетевых экранов	Ежемесячно
8.	Зеркалирование или дублирование информации	В режиме реального времени
9.	Репликация баз данных	В режиме реального времени
10.	Резервное копирование ПО и данных	Ежедневно
11.	Администрирование и мониторинг серверов, каналов связи	В режиме реального времени
12.	Проверка системы резервного копирования и валидности хранящихся резервных копий информации	По мере ротации носителей
13.	Проверка алгоритмов и прав доступа в пропускной системе	Ежеквартально

Приложение № 7
к Положение по УР и обеспечению БФПС

Порядок информационного взаимодействия внутри Операционного центраПлатежной системы «ХЕЛЛО»

Порядок информационного взаимодействия внутри Операционного центра Платежной системы «ХЕЛЛО» (ОЦ «ХЕЛЛО») определяет действия для обеспечения бесперебойности функционирования Платежной системы «ХЕЛЛО» (ПС «ХЕЛЛО»).

Данный порядок разработан в соответствии с требованиями Законао НПС, Положения Банка России № 607-П, а также требований по обеспечению физическойлогической безопасности, предъявляемых Операционным центрам.

Данный порядок характеризует риски сбоев, возникающих в работе ОЦ «ХЕЛЛО», влияние их последствий на бесперебойность функционирования ПС «ХЕЛЛО».

Данным порядком, в том числе, определяются действия по оповещению внутри ОЦ «ХЕЛЛО» о возникновении угрозы нарушения бесперебойности функционирования ПС «ХЕЛЛО».

ЗПБ – Зона повышенной безопасности ОЦ «ХЕЛЛО».

Сбои в ОЦ «ХЕЛЛО» в целях оперативного оповещения можно условно разделить на 4 (Четыре) группы:

1. ***Локальные сбои*** – сбои оборудования или программных средств в ОЦ «ХЕЛЛО», не влияющие на работу устройств за пределами территории ОЦ «ХЕЛЛО». При таких сбоях обслуживание по картам не прерывается, информация о таких сбоях остается закрытой для посторонних. Локальный сбой характеризуется *Незначительным* уровнем риска нарушения бесперебойности функционирования ПС «ХЕЛЛО».

N п/п	**Наименование ресурса**	**Контроль работо-способности**	**Ответственные за восстановление**	**Длитель-ность отказа для оповещения**
1.	Копировальная техника	Персонал в процессе работы	Служба эксплуатации	0 минут (в раб. вр.)
2.	Печатающие устройства вне ЗПБ	Персонал в процессе работы	Служба эксплуатации	0 минут (в раб. вр.)
3.	Персональные компьютеры и терминалы вне ЗПБ	Персонал в процессе работы	Служба эксплуатации	0 минут (в раб. вр.)
4.	Отдельные телефонные аппараты	Персонал в процессе работы	Служба эксплуатации	0 минут (в раб. вр.)

5.	Система электроснабжения и освещения	Персонал в процессе работы	Энергетик по эксплуатации здания	0 минут
6.	Система кондиционирования и вентилирования помещений вне ЗПБ	Персонал в процессе работы	Управляющий зданием	0 минут (в раб. вр.)
7.	Система водоснабжения и канализации	Персонал в процессе работы	Управляющий зданием	0 минут (в раб. вр.)
8.	Внутренний файловый сервер	Персонал в процессе работы	Отдел системного администрирования	0 минут (в раб. вр.)
9.	Система бухгалтерского учета	Бухгалтерия в процессе работы	Нач. отдела системного администрирования	0 минут (в раб. вр.)
10.	Внутренние сервисные программы и системы, не влияющие на бесперебойность функционирования ПС «ХЕЛЛО»	Персонал в процессе работы	Отдел информационных технологий	0 минут (в раб. вр.)

Оповещение	Работник, обнаруживший Локальный сбой, обязан уведомить об этом своего непосредственного руководителя и обратиться в профильное структурное подразделение ОЦ «ХЕЛЛО» для принятия мер по устранениюсбоя.

2. ***Некритичные сбои*** – сбои оборудования или программных средств в ОЦ «ХЕЛЛО», следствием которых является неработоспособность отдельных устройств или подсистем ОЦ «ХЕЛЛО», не влекущие за собой существенные последствия для функционирования ПС «ХЕЛЛО» в целом. Некритичные сбои характеризуются ***Допустимым*** уровнем риска нарушения бесперебойности функционирования ПС «ХЕЛЛО». При таких сбоях может прерываться обслуживание по картам с использованием отдельных малозначимых сервисов ОЦ «ХЕЛЛО». Некритичные сбоине касаются подавляющего большинства держателей карт и не наносят большой ущерб репутации ПС «ХЕЛЛО». Такие сбои носят, как правило, кратковременный характер и быстро устраняются.

Оповещение	Работник, обнаруживший Некритичный сбой, обязан уведомить об этом своего непосредственного руководителя и обратиться в профильное подразделение ОЦ «ХЕЛЛО» для принятия мер по устранению сбоя.

3. ***Критичные сбои*** – сбои оборудования или программных средств в ОЦ «ХЕЛЛО», следствием которых является неработоспособность группы используемых в режиме on-line устройств или подсистем ОЦ «ХЕЛЛО», не влекущих за собой катастрофические последствия для функционирования ПС «ХЕЛЛО» в целом.

Критичные сбои характеризуются *Повышенным* или *Критическим* уровнем риска нарушения бесперебойности функционирования ПС «ХЕЛЛО». При таких сбоях прерывается обслуживание по картам с использованием отдельных сервисов или подсистем ОЦ «ХЕЛЛО». Такие сбои касаются отдельных категорий из числа держателей карт и могут нанести большой ущерб репутации ПС «ХЕЛЛО». Критичные сбои носят, как правило, длительный характер, и на их устранение требуется продолжительное время.

Оповещение	Работник, обнаруживший Критичный сбой, обязан уведомить об этом своего непосредственного руководителя, ответственного за восстановление системы, а также руководителя департамента информационных технологий или его заместителя (при его наличии). В случае неработоспособности ресурса более 1 часа руководитель департамента информационных технологий уведомляет об этом руководителей структурных подразделений ПС «ХЕЛЛО» согласно регламенту оповещения при Глобальном сбое.

4. ***Глобальные сбои*** – сбои оборудования или программных средств в ОЦ «ХЕЛЛО», неработоспособность которых может повлечь за собой катастрофические последствия для функционирования отдельных систем ОЦ «ХЕЛЛО» и ПС «ХЕЛЛО» вцелом. Глобальные сбои характеризуются *Катастрофическим* уровнем риска нарушения бесперебойности функционирования ПС «ХЕЛЛО». При таких сбоях полностью или почти полностью прерывается обслуживание по картам, информация о таких сбоях быстро распространяется среди держателей карт и наносит большой ущерб репутации ПС «ХЕЛЛО».

Оповещение	Работник, обнаруживший Глобальный сбой, обязан срочно уведомить об этом своего непосредственного руководителя, ответственного за восстановление системы, а также руководителя департамента информационных технологий или его заместителя.

Руководитель отдела информационных технологий, в свою очередь, информирует о происшествии для координации действий по устранению сбоя:

- генерального директора,
- руководителя отдела управления рисками.

Для принятия мер по устранению сбоя, формирования рабочей группы, если Глобальный сбой касается профиля этих подразделений, информация также доводится до сведения:

г) Руководителя отдела информационной безопасности,

д) Руководителей всех отделов Оператора по развитию партнерской сети РФ, стран СНГ (с соответствующим наименованием страны согласно внутренним

документам Оператора), иных стран (при наличии согласно внутренним документам Оператора),

е) Арендодателя,

ж) Главного бухгалтера.

Протокол устранения сбоя. Работник, обнаруживший *Критичный* или *Глобальный* сбой, заполняет Протокол устранения сбоя, где указываются обстоятельства его обнаружения: дата и время обнаружения, кто обнаружил, признаки сбоя, категория сбоя, подразделение, ответственное за восстановление ресурса, когда и кто был уведомлен о сбое. Протокол передается руководителю подразделения, ответственного за восстановление ресурса. Далее работник подразделения, занимавшийся устранением сбоя, заносит информацию о причине его возникновения, предпринятых действиях по устранению сбоя, времени неработоспособности ресурса, дате и времени полного устранения сбоя, мерах, предпринятых для предотвращения повторения такого сбоя, указывает Ф.И.О., ставит подпись. Протокол возвращается руководителю подразделения работника, обнаружившего сбой для анализа адекватности и достаточности предпринятых мер. Если руководитель решит, что предпринятые меры не смогут предотвратить в будущем повторениясложившейся ситуации, он может вынести обсуждение этого вопроса на повестку дня рабочего совещания руководителей подразделений ПС «ХЕЛЛО».

Протокол устранения сбоя

N п/п	**Параметр**	**Описание**
1.	Дата и время обнаружения сбоя	
2.	Сбой обнаружил (Фамилия И.О., подразделение, должность)	
3.	Подпись	
4.	Признаки сбоя	
5.	Наименование неработоспособного ресурса	
6.	Категория сбоя	
7.	Подразделение, ответственное за восстановление ресурса	
8.	Кто уведомлен о сбое (Фамилия И.О., подразделение, должность)	
9.	Дата и время уведомления	
10.	Причина возникновения	
11.	Предпринятые действия	
12.	Дата и время начала простоя	
13.	Дата и время полного восстановления	
14.	Длительность простоя	
15.	Меры по предотвращению повторения такого сбоя	

16.	Сбой устранил (Фамилия И.О., подразделение, должность)	
17.	Подпись	
18.	Руководитель (Фамилия И.О., подразделение, должность)	
19.	Подпись	

Приложение № 8
к Положение по УР и обеспечению БФПС

Порядок определения показателей БФПС

1. Показатель П1 рассчитывается по каждому из Операторов услуг платежной инфраструктуры и по каждому из инцидентов, повлекших приостановление оказания услуг платежной инфраструктуры, как период времени с момента приостановления оказания услуг платежной инфраструктуры вследствие инцидента, произошедшего у Оператора услуг платежной инфраструктуры, и до момента восстановления оказания услуг платежной инфраструктуры.

При возникновении инцидентов, повлекших приостановление оказания услуг платежной инфраструктуры одновременно двумя и более Операторами услуг платежной инфраструктуры, показатель П1 рассчитывается как период времени с момента приостановления оказания услуг платежной инфраструктуры в результате первого из возникших инцидентов и до момента восстановления оказания УПИ всеми операторами услуг платежной инфраструктуры, у которых возникли инциденты.

Показатель П1 рассчитывается в часах/минутах/секундах.

2. Показатель П2 рассчитывается по каждому из Операторов услуг платежной инфраструктуры при возникновении каждого из инцидентов, повлекших приостановление оказания услуг платежной инфраструктуры, как период времени между двумя последовательно произошедшими у Оператора услуг платежной инфраструктуры инцидентами, в результате которых приостанавливалось оказание услуг платежной инфраструктуры, с момента устранения первого инцидента и до момента возникновения следующего.

В платежных системах, в которых Оператор услуг платежной инфраструктуры оказывает более одного вида услуг платежной инфраструктуры одновременно, показатель П2 должен рассчитываться одновременно по всем видам услуг платежной инфраструктуры, оказываемым данным Оператором услуг платежной инфраструктуры.

Показатель П2 рассчитывается в часах/минутах/секундах.

3. Показатель П3 рассчитывается по каждому Оператору услуг платежной инфраструктуры.

Для ОЦ показатель П3 рассчитывается как отношение количества распоряженийУчастников ПС (их Клиентов), по которым в течение календарного месяца были оказаны операционные услуги без нарушения регламента выполнения процедур, к общему количеству распоряжений Участников ПС (их Клиентов), по которым были оказаны операционные услуги в течение календарного месяца, рассчитываемое по следующей формуле:

$$П3_{оц} = (N_{оц} / N_{оц}^{общ}) \times 100\%$$

где:

$N_{оц}$ - количество распоряжений Участников ПС (их Клиентов), по которым в течение календарного месяца были оказаны операционные услуги без нарушения регламента выполнения процедур,

$N_{оц}^{об\,щ}$ - общее количество распоряжений Участников ПС (их Клиентов), по которым были оказаны операционные услуги в течении календарного месяца.

Для ПКЦ показатель П3 рассчитывается как отношение количества распоряжений Участников ПС (их Клиентов), по которым в течение календарного месяца были оказаны

ПРи

услуги платежного клиринга без нарушения регламента выполнения процедур, к общему количеству распоряжений Участников ПС (их Клиентов), по которым были оказаны услуги платежного клиринга в течение календарного месяца, рассчитываемое по следующей формуле:

$$П3_{пкц} = (N_{пкц} / N^{общ}_{пкц}) \times 100\%$$

где:

$N_{пкц}$ - количество распоряжений Участников ПС (их Клиентов), по которым в течение календарного месяца были оказаны услуги платежного клиринга без нарушения регламента выполнения процедур

$N^{общ}_{пкц}$

- общее количество распоряжений Участников ПС (их клиентов), по которым были оказаны платежного клиринга в течении календарного месяц

Для РЦ показатель П3 рассчитывается как отношение количества распоряжений Участников ПС и (или) ПКЦ, по которым в течение календарного месяца были оказаны расчетные услуги без нарушения регламента выполнения процедур, к общему количеству распоряжений Участников ПС и (или) ПКЦ, по которым были оказаны расчетные услуги в течение календарного месяца, рассчитываемое по следующей формуле:

$$П3_{рц} = (N_{рц} / N^{общ}_{рц}) \times 100\%$$

где:

$N_{рц}$ – количество распоряжений Участников ПС и (или) ПКЦ, по которым в течении календарного месяца были оказаны расчетные услуги без нарушения регламента выполнения процедур

$N^{общ}_{рц}$

- общее количество распоряжений Участников ПС и (или) ПКЦ, по которым были оказаны расчетные услуги в течении календарного месяца.

Показатель П3 рассчитывается ежемесячно в процентах с точностью до двух знаков после запятой (с округлением по математическому методу).

Значение показателя П3 по ПС в целом принимается равным наименьшему из значений данного показателя, рассчитанных по всем Операторам услуг платежной инфраструктуры в отношении всех видов оказываемых ими услуг.

В платежных системах, в которых Оператор услуг платежной инфраструктуры оказывает более одного вида услуг платежной инфраструктуры одновременно, показатель П3 должен рассчитываться по данному Оператору услуг платежной инфраструктуры в отношении всех видов оказываемых им услуг.

4. Показатель П4 рассчитывается как среднее значение коэффициента доступности ОЦ ПС за календарный месяц, рассчитываемое 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 ПС в месяце,

D_i - общая продолжительность всех приостановлений оказания операционных услуг ОЦ ПС 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 временным регламентом функционирования ПС.

Показатель П4 рассчитывается ежемесячно в процентах с точностью до двух знаков после запятой (с округлением по математическому методу).

Для платежных систем с несколькими операционными центрами показатель П4 должен рассчитываться для каждого операционного центра платежной системы.

Значение показателя П4 по платежной системе в целом принимается равным наименьшему из значений данного показателя, рассчитанных по всем операционным центрам платежной системы.

5. Показатель П5 рассчитывается по ПС в целом и для каждого оператора услуг платежной инфраструктуры в отдельности как темп прироста среднедневного количества инцидентов за оцениваемый календарный месяц по отношению к среднедневному количеству инцидентов за предыдущие 12 календарных месяцев, включая оцениваемый календарный месяц, рассчитываемый по следующей формуле:

$$П5 = \left(\frac{\sum_{i=1}^{M} КИ_i / M}{\sum_{i=1}^{N} КИ_i / N} - 1 \right) \times 100\%$$

где:

$КИ_i$ – количество инцидентов в течении i-го рабочего дня платежной системы оцениваемого календарного месяца

M – количество рабочих дней платежной системы в оцениваемом календарном месяце

N – количество рабочих дней платежной системы за 12 предыдущих месяцев, включая оцениваемый месяц

Показатель П5 рассчитывается ежемесячно в процентах с точностью до одного знака после запятой (с округлением по математическому методу). В случае если за предыдущие 12 календарных месяцев, включая оцениваемый месяц, инцидентов не было, значение показателя признается равным нулю.

В платежных системах, в которых оператор услуг платежной инфраструктуры оказывает более одного вида услуг платежной инфраструктуры одновременно, показатель П5 должен рассчитываться по данному оператору услуг платежной инфраструктуры в отношении всех видов оказываемых им услуг.

Приложение № 9
к Положение по УР и обеспечению БФПС

Пороговые уровни показателей БФПС
Платежной системы «ХЕЛЛО»

Показатели		**Пороговые уровни показателей ПС «ХЕЛЛО»**
Показатель продолжительности восстановления оказания УПИ	**П1**	**не более 6 часов**
Показатель непрерывности оказания УПИ	**П2**	**не менее 12 часов**
Показатель соблюдения регламента	**П3**	**не менее 98,0% - ОЦ, ПКЦ** **не менее 99,0% - РЦ**
Показатель доступности Операционного центра платежной системы	**П4**	**не менее 96,0%**
Показатель изменения частоты инцидентов	**П5**	**не более 400,0% - если за предыдущий период было не более 10 инцидентов;** **не более 200,0% - если за предыдущий период было более 10 инцидентов.**

Приложение № 10
к Положение по УР и обеспечению БФПС

Бизнес-процессы Платежной системы «ХЕЛЛО»

Бизнес-процессы	Процедуры	Код
Операционные услуги	Получение и передача распоряжений Участников	001.1
	Получение и передача подтверждений об исполнении/извещений об отказе в исполнении распоряжений Участников	002.1
Услуги платежного клиринга	Прием к исполнению распоряжений Участников	001.2
	Процедуры контроля распоряжения: - проведение процедур удостоверения права распоряжения денежными средствами; - контроль целостности распоряжений; - структурный контроль распоряжений; - контроль дублирования распоряжений; - контроль значений реквизитов распоряжений; - контроль достаточности денежных средств	002.2
	Направление извещений об отказе в исполнении с указанием причин распоряжений Участников	003.2
Расчетные услуги	Исполнение распоряжений Участников	001.3
	Направление подтверждений об исполнении распоряжений	002.3

Приложение № 11
к Положение по УР и обеспечению БФПС

ПРОФИЛЬ РИСКА
(правового, операционного, расчетного, общего коммерческого, системного)

№	Профиль риска	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последсвий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1		1.1.							1.1.								

Далее указаны таблицы в разрезе рисков с перечнями риск-событий. Перечни риск-событий не являются исчерпывающими, могут быть дополнены и изменены. Таблицы заполняются в соответствии с Правилами ПС, данным Положением, в т.ч. Приложением № 1 данного Положения. Под уровнем риска в Приложении № 1 к настоящему положению для составления профилей риска понимается уровень присущего риска (до применения способов управления рисками) и уровень остаточного риска (после применения способов управления рисками).

ПРОФИЛЬ ПРАВОВОГО РИСКА

№	Профиль риска	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	**Правовой**	1.1. Претензии правового характера к Субъектам ПС со стороны государственных органов	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Несоблюдение Оператором ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участником(ами) требований законодательства, нормативных актов и заключенных договоров, внутренних документов, регламенти	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2 и/или 001.3 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	Средняя	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	1.1. Размер потерь – значительный	3	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2 и/или 001.3 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	>9	<=9	▪ -- Осуществление расчета в пределах предоставленных Участниками денежных средств; - Автоматизированное управление очередностью исполнения распоряжений Участников - по времени поступления распоряжений; ▪ - Осуществление расчета в Системе до конца рабочего дня;	<=9

				рующих их деятельность, а также наличие недостатков в внутренних документов							системы					▪ У-Установление предельных размеров (лимитов) обязательств в отношении Участников, открывших счета в привлеченном РЦ, с учетом уровня риска; иные способы управления рисками, в том числе: анализ и изучение финансовой отчетности, других сведений и документов Участников, ОУПИ (при их наличии), а также анализ и изучение информации в СМИ, отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС «ХЕЛЛО»). Также	

																рекомендации п.7.4 Приложения № 1 к настоящему Положению	
		1.2. Претензии правового характера к Субъектам ПС со стороны других Субъектов ПС, клиентов Участников ПС.	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Несоблюдение Оператором ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участником(ами) требований законодательства, нормативных актов и заключенных договоров, внутренних документов, регламентирующих их деятельность, а также наличие недостатков в внутренних документов	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2 и/или 001.3 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	Средняя	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Размер потерь - значительный	3	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2 и/или 001.3 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	>9	<=9	▪ -- Осуществление расчета в пределах предоставленных Участниками денежных средств; ▪ - Автоматизированное управление очередностью исполнения распоряжений Участников - по времени поступления распоряжений; ▪ - Осуществление расчета в Системе до конца рабочего дня; ▪ - Установление предельных размеров (лимитов) обязательств в отношении Участников, открывших счета в привлеченном РЦ, с учетом	<=9

																уровня риска; иные способы управления рисками, в том числе: анализ и изучение финансовой отчетности, других сведений и документов Участников, ОУПИ (при их наличии), а также анализ и изучение информации в СМИ, отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС «ХЕЛЛО»). Также рекомендации п.7.4 Приложения № 1 к настоящему Положению	

ПРОФИЛЬ ОПЕРАЦИОННОГО РИСКА

№	Профиль риска	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	**Операционный**	1.1. Нарушение функционирования ПС в результате нарушения работоспособности аппаратно-программных комплексов Субъектов ПС	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Нарушение работоспособности аппаратно-программных комплексов, ненадлежащие действия персонала	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2 и/или 001.3 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	Средняя	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	1.1.Размер потерь - допустимый	2	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2 и/или 001.3 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	>6	<=6	▪ -- Осуществление расчета в пределах предоставленных Участниками денежных средств; - Автоматизированное управление очередностью исполнения распоряжений Участников - по времени поступления распоряже	<=6

																ний; ▪ - Осуществление расчета в Системе до конца рабочего дня; ▪ Установление предельных размеров (лимитов) обязательств в отношении Участников, открывших счета в привлеченном РЦ, с учетом уровня риска; иные способы управления рисками, в том числе: анализ и изучение финансовой отчетности, других сведений и документов Участников, ОУПИ	

																(при их наличии), а также анализ и изучение информации в СМИ, отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС «ХЕЛЛО»). Также рекомендации п.7.4 Приложения № 1 к настоящему Положению	
		1.2. Нарушение функционирования ПС в	Метод индексов риска и элементы методик, основан	Нарушение работоспособности аппаратно-программных комплексов, ненадлежа	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2 и/или 001.3 и/или 002.3 (согласно Приложени	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или		Метод индексов риска и элементы методик, основанных на статистическом и	Размер потерь - допус		Метод индексов риска и элементы метод	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ			▪ -- Осуществление расчета в пределах предоставленных Участниками	

		резуль тате	ных на статист ическо	щие действия персонала	ю № 10 к настоящем у	Участник (и)	Средня я	сценарном анализе функциониро	тимы й	2	ик, основ анных	и/или 001.3 и/или	и/или Участн ик(и)	>6	<=6	денежных средств; ▪	<=6

		выполнения недопустимых операций или ошибочного выполнения операций в ПС	м и сценарном анализе функционирования системы		Положению)			вания системы			на статистическом и сценарном анализе функционирования системы	002.3 (согласно Приложению № 10 к настоящему Положению)				- Автоматизированное управление очередностью исполнения распоряжений Участников - по времени поступления распоряжений; ▪ - Осуществление расчета в Системе до конца рабочего дня; ▪ - Установление предельных размеров (лимитов) обязательств в отношении Участников, открывших счета в привлеченном РЦ, с учетом уровня риска;	

																иные способы управления рисками, в том числе: анализ и изучение финансовой отчетности, других сведений и документов Участников, ОУПИ (при их наличии), а также анализ и изучение информации в СМИ, отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС «ХЕЛЛО»). Также рекомендации п.7.4 Приложения № 1 к	

																настоящему Положению	

ПРОФИЛЬ РАСЧЕТНОГО РИСКА

№	Профиль риска	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	**Расчетный**	1.1. Несвоевременность проведения расчетов, задержка исполнения расчетных документов из-за отсутствия денежных средств на корреспондентских счетах	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Недостаточность (отсутствие) средств у Участника или нескольких Участников ПС для своевременного выполнения ими своих расчетных обязательств перед другими Участниками ПС, финансовая несостоятельность Участника ПС, концентрация	002.2 и/или 001.3 и/или (согласно Приложению № 10 к настоящему Положению)	ПКЦ и/или РЦ и/или Участник(и)	Минимальная	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	1.1. Размер потерь - незначительный	1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	002.1 и/или 003.2 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	>3	<=3	▪ - - Осуществление расчета в пределах предоставленных Участниками денежных средств; - Автоматизированное управление очередностью исполнения распоряжений Участников - по	<=3

		Участников ПС		значительного объема расчетных документов в определенные моменты и (или) периоды времени в течение дня												времени поступления распоряжений; ▪ - Осуществление расчета в Системе до конца рабочего дня; ▪ - Установление предельных размеров (лимитов) обязательств в отношении Участников, открывших счета в привлеченном РЦ, с учетом уровня риска; иные способы управления рисками, в том числе:	

																анализ и изучение финансовой отчетности, других сведений и документов Участников, ОУПИ (при их наличии), а также анализ и изучение информации в СМИ, отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС «ХЕЛЛО»). Также рекомендации п.7.4	

																Приложения № 1 к настоящему Положению	
		1.2. Несвоевременность проведения расчетов из-за невозможности использования имеющихся на этих счетах остатках денежных средств, невозможность испол	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Недостаточность (отсутствие) средств у Участника или нескольких Участников ПС для своевременного выполнения ими своих расчетных обязательств перед другими Участниками ПС, финансовая несостоятельность Участника ПС, концентрация значительного объема расчетных документов в определенные моменты и (или)	002.2 и/или 001.3 и/или (согласно Приложению № 10 к настоящему Положению)	ПКЦ и/или РЦ и/или Участник(и)	Минимальная	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Размер потерь - незначительный	1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	002.1 и/или 003.2 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	>3	<=3	▪ - Осуществление расчета в пределах предоставленных Участниками денежных средств; - Автоматизированное управление очередностью исполнения распоряжений Участников - по времени поступления распоряжений; ▪ - Осуществление	<=3

		нения Участником своих обязательств в ПС		периоды времени в течение дня												расчета в Системе до конца рабочего дня; ▪ - Установление предельных размеров (лимитов) обязательств в отношении Участников, открывших их счета в привлеченном РЦ, с учетом уровня риска; иные способы управления рисками, в том числе: анализ и изучение финансовой отчетности, других сведений и	

																	документов Участников, ОУПИ (при их наличии), а также анализ и изучение информации в СМИ, отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС «ХЕЛЛО»). Также рекомендации п.7.4 Приложения № 1 к настоящему Положению	

ПРОФИЛЬ ОБЩЕГО КОММЕРЧЕСКОГО РИСКА

№	Профиль риска	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последсвий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	**Общий коммерческий**	1.1. Сокращение количества Участников	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Наличие негативной информации об Операторе ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участнике(ах)	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2 и/или 001.3 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	Минимальная	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	1.1. Размер потерь - незначительный	1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционировании	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2 и/или 001.3 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	>3	<=3	▪ - Осуществление расчета в пределах предоставленных Участниками денежных средств; - Автоматизированное управление очередностью	<=3

											системы					исполнения распоряжений Участников - по времени поступления распоряжений; ▪ - Осуществление расчета в Системе до конца рабочего дня; ▪ - Установление предельных размеров (лимитов) обязательств в отношении Участников, открыв	

																ших счета в привле ченном РЦ, с учетом уровня риска; иные способ ы управл ения рискам и, в том числе: анализ и изучен ие финанс овой отчетн ости, других сведен ий и докуме нтов Участн иков, ОУПИ (при их наличи и), а также анализ и изучен ие инфор мации в СМИ,	

																	отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС «ХЕЛЛО»). Также рекомендации п.7.4 Приложения № 1 к настоящему Положению	
		1.2. Сокращение количества	Метод индексов риска и элементы методик, основан	Наличие негативной информации об Операторе ПС и/или ОЦ и/или	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2 и/или 001.3 и/или 002.3 (согласно Приложени	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и)	Минимальная	Метод индексов риска и элементы методик, основанных на статистическом и	Размер потерь - незначительный	1	Метод индексов риска и элементы метод	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или	>3	<=3	▪ - Осуществление расчета в пределах	<=3

		Клиентов	ных на статистическом и сценарном анализе функционирования системы	ПКЦ и/или РЦ и/или Участнике (ах)	ю № 10 к настоящему Положению)			сценарном анализе функционирования системы			ик, основанных на статистическом и сценарном анализе функционирования системы	003.2 и/или 001.3 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Участник(и)			предоставленных Участниками денежных средств; - Автоматизированное управление очередностью исполнения распоряжений Участников - по времени поступления распоряжений; ▪ - Осуществление расчета в Системе до конца рабочего дня; ▪	

																- Установление предельных размеров (лимитов) обязательств в отношении Участников, открывших счета в привлеченном РЦ, с учетом уровня риска; иные способы управления рисками, в том числе: анализ и изучение финансовой отчетности, других сведений и	

															документов Участников, ОУПИ (при их наличии), а также анализ и изучение информации в СМИ, отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС «ХЕЛЛО»). Также рекомендации п.7.4	

																Приложения № 1 к настоящему Положению	

ПРОФИЛЬ СИСТЕМНОГО РИСКА

№	Профиль риска	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	**Системный**	1.1. Распространение между Субъектами ПС последствий сочетания двух основных рисков, указанных в п.4 – п.7 Приложения №1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Реализация одновременно нескольких или всех рисков, указанных выше	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2 и/или 001.3 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	Минимальная	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	1.1. Размер потерь - незначительный	1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2 и/или 001.3 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	>18	<=18	▪ - - Осуществление расчета в пределах предоставленных Участниками денежных средств; - Автоматизированное управление очередностью исполнения распоряжений Участников - по времени	<=18

		к Положению по БФПС, вызывающих нарушения функционирования ПС.														поступления распоряжений; ▪ - Осуществление расчета в Системе до конца рабочего дня; ▪ - Установление предельных размеров (лимитов) обязательств в отношении Участников, открывших счета в привлеченном РЦ, с учетом уровня риска; иные способы управления рисками, в том числе: анализ и изучение финансовой	

																отчетности, других сведений и документов Участников, ОУПИ (при их наличии), а также анализ и изучение информации в СМИ, отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС «ХЕЛЛО»). Также рекомендации п.7.4 Приложения № 1 к настоящему Положению	

		1.2. Распространение между Субъектами ПС последствий сочетания нескольких основных рисков, указанных в п.4 – п.7 Приложения №1 к Положению по БФПС, вызывающих нарушения функционирования ПС.	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Реализация одновременно нескольких или всех рисков, указанных выше	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2 и/или 001.3 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	Минимальная	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Размер потерь - незначительный	1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	001.1 и/или 002.1 и/или 001.2 и/или 002.2 и/или 003.2 и/или 001.3 и/или 002.3 (согласно Приложению № 10 к настоящему Положению)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	>18	<=18	▪ - - Осуществление расчета в пределах предоставленных Участниками денежных средств; - Автоматизированное управление очередностью исполнения распоряжений Участников - по времени поступления распоряжений; ▪ - Осуществление расчета в Системе до конца рабочего дня; ▪ У - Установле	<=18

																ние предельных размеров (лимитов) обязательств в отношении Участников, открывших счета в привлеченном РЦ, с учетом уровня риска; иные способы управления рисками, в том числе: анализ и изучение финансовой отчетности, других сведений и документов Участников, ОУПИ (при их наличии), а также анализ и изучение информации в СМИ,	

																отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС «ХЕЛЛО»). Также рекомендации п.7.4 Приложения № 1 к настоящему Положению	

Приложение № 12
к Положение по УР и обеспечению БФПС

ПРОФИЛЬ РИСКА НАРУШЕНИЯ БФПС

№	Профили рисков	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последсвий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	**Профиль правового риска**	1.1.							1.1.								
2	**Профиль операционного риска**	2.1.							2.1.								

3	**Профиль расчетного риска**	3.1.							3.1.								
4	**Профиль общего коммерческого риска**	4.1.							4.1.								
5	**Профиль системного риска**	5.1.							5.1.								

Приложение № 8 к Правилам Платежной системы «ХЕЛЛО»

Наименование Субъекта Платежной Системы _____

Дата заполнения _____

АНКЕТА

Выполнение требований по обеспечению защиты информации			
	вопрос	**ответ (да/нет)**	**пояснение/ссылка на внутренний документ**
1	Субъектом ПС создано структурное подразделение/назначено должностное лицо, ответственное за организацию защиты информации		*указать наименование структурного подразделения/ФИО должностного лица*
2	В должностные обязанности работников Субъекта ПС, участвующих в обработке информации, включены обязанности по выполнению требований к обеспечению защиты информации		*указать перечень обязанностей*
3	При осуществлении переводов денежных средств обеспечена защита информации:		*указать наименование соответствующего документа*
3.1.	в собственных информационных системах		
3.2.	о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите		
3.3.	при использовании информационно-телекоммуникационных сетей общего пользования		
4	Субъектом ПС применяются средства защиты информации:		
4.1.	шифровальные (криптографические) средства		
4.2.	средства защиты информации от несанкционированного доступа		
4.3.	средства защиты от воздействия вредоносного кода		
4.4.	средства межсетевого экранирования		
4.5.	средства обнаружения и предотвращения вторжений		
4.6.	средства контроля (анализа) защищенности		
4.7.	другие средства защиты информации		*указать средства защиты*
5	Субъект ПС осуществляет коммуникацию с Банком России по выявленным инцидентам, связанным с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств		

Сотрудник, заполнивший Анкету _____

подпись ФИО

Приложение № 9 к Правилам Платежной системы «ХЕЛЛО»

Сведения о выявленных Инцидентах, связанных с нарушением бесперебойности функционирования Платежной системы

Дата:_____

Наименование Субъекта Платежной системы:_____

	Дата и время возникновения Инцидента		Краткое описание Инцидента	Наименование бизнес-процессов, в ходе которых произошел Инцидент	Наименование бизнес-процессов, на которых оказал влияние Инцидент	Наличие (отсутствие) факта приостановления (прекращения) оказания УПИ в результате Инцидента	Влияние Инцидента на БФПС	Степень влияния Инцидента на функционирование Платежной системы	Дата и время восстановления оказания УПИ, в случае приостановления		Мероприятия по устранению Инцидента и его последствий	Дата и время восстановления оказания УПИ, соответствующего требованиям оказания услуг		Неблагоприятные последствия			
	Время (чч.мм)	Дата (дд.мм.гг)							Время (чч.мм)	Дата (дд.мм.гг)		Время (чч.мм)	Дата (дд.мм.гг)	Сумма денежных средств, уплаченная и (или) взысканая с Оператора ПС	Сумма денежных средств, уплаченная и (или) взысканая с Оператора (Операторов) УПИ	Количество и суммы неисполненных и (или) несвоевременно исполненных и (или) ошибочно исполненных распоряжений	Продолжительность приостановления оказания УПИ
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

Руководитель Субъекта ПС _____/_____/

М.П.

Исполнитель: